Office of Information Technology Services

Inventory Controls

Report 2023-S-17 | February 2025

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Division of State Government Accountability

Audit Highlights

Objective

To determine whether the Office of Information Technology Services has adequate controls to ensure the accuracy and completeness of inventory records, accountability for inventory transactions, and safeguarding of inventory. The audit covered the period from March 2020 through August 2024.

About the Program

The Office of Information Technology Services (ITS) was created in 2012 and is the lead agency for State IT services and technology solutions, including the procurement, distribution, and maintenance of technical equipment for State employees. Additionally, ITS is responsible for maintaining an accurate inventory of all information assets, including all workstations (desktop and laptop computers), virtual desktops, printers, scanners, mobile devices, and additional specialized equipment, as well as any digital programs or systems needed to support various job functions. To manage the vast inventory, ITS utilizes the Information Technology Service Management (ITSM) software as its centralized system of record.

ITS supports 108 State entities and operates 83 stockroom locations statewide. Stockroom personnel are required to receive inventory shipments and scan the devices into ITSM. Next, in-stock devices are available to be assigned to users and distributed for either onboarding or refreshing an outdated device. As devices are assigned to users and distributed, ITS' Asset Management team updates the record within ITSM to reflect the changes.

As of January 2023, stockroom managers are required to complete quarterly inventory audits to ensure devices are being tracked in ITSM effectively, as well as to ensure stockrooms always have adequate inventory on hand.

Key Findings

ITS does not have the necessary controls in place to accurately and completely account for all workstations and other hardware assets for which it is responsible. We found significant weaknesses related to ITSM accuracy, as well as missing devices, and a lack of security over equipment and the information stored on devices at ITS stockrooms. Further, this general lack of accurate inventory information has resulted in overspending and government waste. For example:

- ITSM data is neither accurate nor complete as it pertains to technology equipment. ITSM contains many errors, including missing devices, with 17,887 devices categorized as absent after they could not be located; duplicate data; and blank serial numbers in the system so that devices cannot be identified. Absent devices are ITS workstations, such as desktops and laptops, that are no longer in ITS' possession but still exist in ITSM.
- Stockrooms throughout the State were not able to accurately reconcile items with ITSM records. We found devices listed in ITSM that were not present in the stockrooms and devices in stockrooms that were not listed in ITSM. We were unable to reconcile 58 of 606 (9.6%) sampled workstations from our 23 stockroom visits with the ITSM information. Further, we found 96 devices present in stockrooms but not listed in ITSM.
- We observed unsecured workstations and the unsecured storage of hard drives that potentially contain confidential data. For example, we saw 36 pallets of used equipment—including

workstations, hard drives, monitors, and keyboards—kept in a shared storage area within the building, easily accessible to employees from other entities. We also saw three boxes of hard drives that had been removed from devices and stored behind an ITS employee's desk—kept in a manner that makes them inappropriately accessible to other individuals with access to the floor.

- We found over 924 lightly used or new devices (e.g., desktop and laptop computers) that were set to be destroyed, with an estimated value between $530,000 and $660,000. New, unused, and lightly used equipment was, in the past, sometimes donated or sold at State auctions; however, due to the additional processes necessary to donate or sell workstation equipment, ITS currently elects to destroy all discarded equipment, even equipment in new or like-new condition.

Further, we identified areas where stronger oversight is needed over stockroom and agency operations and additional training is needed for ITS stockroom personnel. ITS has not provided stockroom personnel with the proper knowledge and skills to competently and effectively use ITSM. We found that ITS stockroom employees at several locations were unable to adequately navigate ITSM to provide reports to the audit team or search the ITSM database for devices by serial number. We also found that 13 of the 23 (57%) stockrooms we visited have not completed all quarterly physical inventory audits as required. Additionally, some State entities have been circumventing appropriate protocols by purchasing their own equipment, putting their own equipment on ITS networks, and keeping equipment that should have been returned to ITS, posing potential security risks to the network and compromising data integrity.

We also identified weaknesses in technical controls that need to be corrected to ensure the selected information systems, and their associated data, are not at risk.

For 7 months, during the beginning stages of our audit, ITS officials imposed scope limitations on the audit team. They placed unwarranted restrictions on access to records, officials, and other individuals needed to fully address our audit objective. When the necessary information was eventually provided, we found instances where the underlying information had been changed, specifically ITSM workstation inventory data. Despite these changes, we found the data to be unreliable, as discussed in the body of the report. After we issued a preliminary findings report on this issue, we saw substantial improvement regarding the availability of information with ITS, and for the remainder of the audit, there was an adequate exchange of information between ITS and OSC.

Key Recommendations

- Conduct a comprehensive review and cleanup of ITSM data to ensure accuracy and completeness, and implement ongoing quality reviews of ITSM data to maintain integrity.
- Improve oversight and monitoring of stockrooms.
- Maintain an accurate and complete inventory of workstations and other equipment available to ensure efficient use of resources and prevent waste of equipment and taxpayer money.
- Formally evaluate the current practice of destroying new and lightly used equipment, and determine if these devices could be resold or donated.
- Implement the recommendation detailed in our preliminary findings to strengthen technical controls over the selected systems reviewed.
- Continue to improve the timeliness of cooperation with authorized State oversight inquiries to ensure transparent and accountable agency operations.

Office of the New York State Comptroller
Division of State Government Accountability

February 14, 2025

Dru Rai
Chief Information Officer
Office of Information Technology Services
Empire State Plaza
P.O. Box 2062
Albany, NY 12220

Dear Mr. Rai:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage their resources efficiently and effectively. By so doing, it provides accountability for the 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.

The following is a report of our audit entitled *Inventory Controls*. 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,

Division of State Government Accountability

Contents

Glossary of Terms

Term	Description	Identifier
ITS	Office of Information Technology Services	*Auditee*
ITSM	Information Technology Service Management system	*Key Term*
State Technology Law	State Technology Law, Section 103, Chapter 57-A of the Consolidated Laws of New York	*Law*

Background

The Office of Information Technology Services (ITS) was created in 2012 to centralize IT services and develop cutting-edge technology solutions that enable State government to serve New Yorkers in a better, smarter, and more cost-effective way. The State Technology Law, Section 103, Chapter 57-A of the Consolidated Laws of New York (State Technology Law), charges ITS with maintaining and updating its inventory of hardware and software periodically. The agency is also responsible for protecting and securing State information resources and data.

ITS provides New York State employees with equipment based on their job functions. This can include workstations (a desktop or a laptop computer), a virtual desktop, standard printers or multi-functional printer/copier/scanners, mobile devices, and additional or specialized equipment. Between March 1, 2020 and March 31, 2024, ITS spent approximately $61.7 million on workstations and associated equipment, including $31.1 million to accommodate the COVID-19 work-from-home initiative. ITS also oversees the State's Information Technology Asset Management process. ITS fully supports 57 State entities, while providing partial support to 51.

To track its inventory of information assets, or workstations, ITS utilizes Information Technology Service Management (ITSM) software to manage its centralized system of record. Previously, ITS had used a different software application to coordinate its stockroom manager inventory responsibilities, while using ITSM to coordinate its back-end data collection and management. The prior software application was discontinued on June 30, 2021, and the ITSM mobile application was implemented for stockroom manager data entry. ITSM pulls data from several automated systems used to identify assets on the ITS network and to compile its centralized inventory listing. Also included in the data are manual entries created by ITS personnel.

ITS' Workplace Device Computing policy requires ITS to maintain an accurate inventory of all information technology assets, including all workstations. ITS' Asset Management team is responsible for tracking these devices throughout their life cycle—from the time they are ordered until they are retired and destroyed. ITS begins its tracking of workstations in ITSM when it orders devices from its vendors. It then tracks devices when stock is transferred between stockrooms, when devices are deployed to users, when devices are reclaimed from users, and finally, through devices' destruction. Once the vendor destroys and disposes of workstations, ITS receives a Certificate of Destruction for each device, certifying that decommissioned devices have been sufficiently destroyed. When ITS receives Certificates of Destruction, it sets devices to a state of "Retired" with a substate of "Disposed."

The ITS policy on Information Security requires information processing and storage facilities to have a defined security perimeter and appropriate security barriers and access controls. Information technology equipment must be physically protected from security threats and environmental hazards. All information technology equipment and information media must be secured and concealed to the extent possible to prevent a compromise of confidentiality, integrity, or availability.

ITS operates 83 stockroom locations across the State. Each stockroom is responsible for various State entities and/or geographical locations. Stockroom managers are responsible for the oversight of equipment contained in their stockrooms and are required to keep their ITSM information up to date, including an accurate listing of all workstations (desktops and laptops) in their stockrooms. In addition, stockroom managers are responsible for completing the onboarding and offboarding processes for employees of the State entities they service. The ITS Policy on Workplace Device Computing states that State entities are primarily responsible for offboarding their users upon separation from the State entity. Whether the user leaves State service or simply transfers to a new agency, the State entity must promptly complete and submit an Employee Offboarding request through ITSM.

Audit Findings and Recommendations

ITS does not have the necessary controls in place to accurately and completely account for all workstations and other hardware assets it is responsible for. We found significant weaknesses related to ITSM accuracy, including absent devices, an inability to reconcile ITSM with inventory in ITS stockrooms, and a lack of security over equipment and the information stored on devices. Further, this general lack of accurate inventory information has resulted in overspending and government waste. For example:

- ITSM data is neither accurate nor complete as it pertains to technology equipment. ITSM contains many errors, including missing devices, with 17,887 devices categorized as absent after they could not be located; duplicate data; and blank serial numbers in the system.
- When the audit team compared devices on hand to ITSM, stockrooms throughout the State were unable to accurately reconcile stockroom inventory with ITSM. We found both devices listed in ITSM that were not present in the stockrooms and devices at stockrooms that were not listed in ITSM. For example, we were unable to reconcile 58 of 606 (9.6%) workstations listed in ITSM. Further, we found 96 devices present in stockrooms but not listed in ITSM.
- We observed unsecured workstations and the unsecured storage of hard drives that potentially contain confidential data. We saw 36 pallets of used equipment—including workstations, hard drives, monitors, and keyboards —kept in a shared storage area within the building, easily accessible to employees from other State entities. We also found three boxes of hard drives that were removed from devices and stored behind an ITS employee's desk—kept in a manner that makes them inappropriately accessible to other individuals with access to the floor.
- We found over 924 lightly used or new devices (e.g., desktop and laptop computers) that were set to be destroyed, with an estimated value between $530,000 and $660,000. New, unused, and lightly used equipment was, in the past, sometimes donated or sold at State auctions; however, due to the additional processes necessary to donate or sell workstation equipment, ITS currently elects to destroy all discarded equipment, even equipment in new or like-new condition.

We also identified additional areas where stronger oversight is needed over stockroom and agency operations and additional training is needed for ITS stockroom personnel. ITS has not provided its stockroom personnel with the proper knowledge and skills to competently and effectively use ITSM. We found that ITS stockroom employees at several locations were unable to adequately navigate ITSM to provide reports to the audit team or search the ITSM database for devices by serial number. We also found that 13 of the 23 (57%) stockrooms we visited have not completed all quarterly physical inventory audits as required.

Further, State entities have been circumventing appropriate protocols by purchasing their own equipment and keeping equipment that should have been returned to ITS. Also, in some cases, State entities have put their own equipment on the ITS network outside of the central device management process, posing potential security risks to the network and compromising data integrity.

For 7 months, during the beginning stages of our audit, ITS officials imposed scope limitations on the audit team. They placed unwarranted restrictions on access to records, officials, and other individuals needed to fully address our audit objective. When the necessary information was eventually provided, we found instances where the underlying information had been changed, specifically ITSM workstation inventory data. After we issued a preliminary findings report on this issue, we saw substantial improvement regarding the availability of information with ITS, and for the remainder of the audit, there was an adequate exchange of information between ITS and OSC.

ITSM Data Analysis

After 7 months of delays, ITS provided workstation (e.g., desktop and laptop computers) inventory data from its ITSM system, as of December 2023. The inventory list contained 341,931 workstation records, categorized by Install States (used to categorize the status of device installations), as shown in Table 1.

Table 1 – ITS Workstation Inventory Records

Install State	Quantity
Absent	17,887
In Maintenance	69
In Stock	63,503
Installed	200,992
On Order	504
Pending Decommission	30
Pending Install	105
Pending Repair	47
Retired	58,778
Stolen	15
Under Construction	1
Total	**341,931**

The audit team reviewed ITSM data to identify findings and potential areas of risk, focusing on absent devices, duplicate entries in ITSM data, and workstation records containing blank serial numbers. We also reviewed server device data.

Absent Devices

Absent devices are ITS workstations, such as desktops and laptops, that are no longer in ITS' possession but still exist in ITSM. We analyzed ITSM data and identified a total of 17,887 workstations categorized as absent. Of those devices, 14,694 (82%) records did not contain the location where the device should have been. The remaining 3,193 absent devices' records contained the location where the device should be located and were used to select a sample of absent devices at 14 of the 23 stockrooms we visited. During the 14 stockroom visits, we used

ITSM data provided in December 2023 to select judgmental samples of 102 of 448 absent devices to review with ITS personnel associated with stockrooms we visited. ITS stockroom personnel were unable to locate 94 devices (92%). We located the remaining eight absent devices from our sample—seven were detected by ITS personnel searching their network and determining the device to be active, and one device was physically located in a stockroom, designated to be decommissioned and destroyed.

In addition, we identified distinct trends in how devices' Install States were changed to absent. Asset Management officials stated that there was an initiative to change the status of approximately 11,000 devices in ITSM that were deemed missing to a state of absent. In essence, ITS undertook a significant data cleanup within ITSM during our scope, reclassifying devices that were previously marked under other Install States such as In-stock and Installed (e.g., assigned to a user) as absent. These changes occurred between our initial request for ITSM data on May 15, 2023 and when we received ITSM data on December 28, 2023. According to ITS officials, stockrooms were instructed to find the missing unscanned devices from the first quarterly physical inventory audit. In October and November 2023, any devices not found were marked absent in ITSM. As a result, ITS has identified a significant number of workstations that have likely gone missing due to inadequate controls over workstation inventory. ITS should have policies and processes in place to ensure devices are adequately accounted for throughout their life cycle.

Duplicate Entries

During our review of ITSM data, we noted 931 unique duplicates in the serial number entries, four of which had invalid serial numbers. The four duplicates without actual serial numbers are shown in Table 2:

Table 2 – Duplicate ITSM Data

Serial Number	Number of Times Duplicated in Data
Virtual	6
123456789012345	5
123456789	3
0	3

We determined the reasons for some duplicates were the scanning of the wrong bar code and manual entries. For example, certain devices do not scan properly using the mobile ITSM application and, therefore, must be input manually into ITSM. ITS stockroom personnel stated that inputting devices manually can cause issues if the incorrect serial number is entered, or entries could potentially be duplicated if the ITS employee does not check to see if the device already exists in ITSM. During our analysis of ITSM data, we identified 532 of 927 (57%) duplicate entries were from manual entries. As a result, there is a significant risk that scanning incorrect bar codes or manually entering records into ITSM can cause inaccuracies in ITS' inventory. ITS should automate the input and update of device records in ITSM to the extent possible to avoid data entry errors and/or duplication of records.

Blank Serial Numbers

We identified 1,582 entries in the workstation ITSM listing where the serial number entry was blank. Of these, 589 (37%) did not contain a physical address where the devices were located, making it impossible for ITS to know if these records represent actual workstations. Consequently, ITSM contains workstation device records that are potentially incomplete and may not reflect actual ITS workstations. Moreover, without the serial number, it cannot be determined if an item at that location is the correct item. ITS should ensure that appropriate controls are in place to ensure workstation device records in ITSM are accurate and complete.

Incomplete Server Data

ITS does not have complete ITSM server data. We reviewed a judgmental sample of 50 servers out of 492, to test the accuracy and completeness of the data provided. We were not able to reconcile 11 of 50 servers we sampled. For these 11, we were able to locate the devices but were unable to reconcile them with the ITSM server listing.

During audit testing, ITS personnel were utilizing a separate Excel spreadsheet, outside of ITSM to assist with locating devices. ITS personnel stated that they have experienced issues with ITSM and entering server locations into the system —sometimes, the data is overwritten by automated processes. ITS should ensure that the automated processes it employs do not compromise the accuracy and completeness of the information in ITSM.

In response to our audit findings, ITS began a concentrated effort to improve the ITSM data to maintain its integrity and purchased the Hardware Asset Management module in the software. This module is anticipated to be fully integrated into the system by March 2025 and, according to ITS officials, will provide a more integrated process and improve the tracking of assets.

Stockroom Site Visits

Several ITS stockrooms do not possess the technical and physical inventory controls required to maintain an accurate and complete inventory listing, particularly for workstations. ITS has instituted some controls related to ITSM and stockrooms; however, these controls are not sufficient to ensure the accuracy and completeness of inventory records, accountability for inventory transactions, and safeguarding of inventory.

Quarterly Physical Inventory Audits

In January 2023, ITS Workplace Services instituted a quarterly physical inventory audit procedure across all ITS stockrooms. Per ITS guidance, all stockrooms must take a physical inventory of all equipment at least once each quarter. During our stockroom visits and through documentation provided by ITS, we learned that 13 of the 23 stockrooms we visited had not completed all quarterly physical inventory audits, as required. At the time of our review, each stockroom should have completed six quarterly stockroom audits; however, we found that six of the 23 stockrooms we visited (26%) had completed three or fewer. While implementing the physical inventory audit requirement strengthens ITS' controls over its stockrooms, it has not exercised adequate monitoring over the process and has not ensured that the stockrooms have completed all required quarterly physical inventory audits. As a result, ITS cannot be assured that all stockroom workstation equipment is accurately accounted for.

ITS has not instituted effective controls over stockroom operations, nor has it adequately communicated the policies, procedures, and guidance in place to stockroom employees. Prior to January 2023, ITS did not conduct physical inventories of stockrooms, which led to inaccuracies between ITSM and actual inventory on hand. As a result of the physical inventory audits conducted by stockrooms, ITS identified a significant number of devices that have been lost due to lack of proper internal controls over workstation inventory. Additionally, ITS has not standardized the operations of its stockrooms. Each stockroom has its own set of unwritten procedures that it employs to maintain the stockroom; however, there is very little consistency among stockrooms. While ITS makes its policies and procedures available on its own external-facing website and through internal training articles, we found that employees at some stockrooms are often unaware of the guidance available to them.

In response to our audit findings, ITS stated that quarterly audits are now being completed by all stockrooms. The Asset Management team will review the reconciliation results to ensure that audits are being completed and discrepancies are being addressed.

Stockroom Inventory

We visited 23 ITS stockroom locations used to store a significant number of workstations. We reviewed 606 workstations ready for deployment out of 17,444 located in ITS stockrooms, listed in ITSM as In-stock, Available. However, we were unable to reconcile 58 (9.6%) workstations with the ITSM information generated from the system.

- 14 devices were unable to be physically located.
- 11 devices were listed as In-stock, Available, but were assigned to a user.
- 4 devices were found in stockrooms but were assigned to users in ITSM.
- 21 devices were found to have the incorrect status.
- 7 devices were not in ITSM.
- 1 device was found to be a duplicate ITSM record.

We also identified several workstations that were not included in the ITSM workstation inventory record. For example, at various stockrooms throughout the State, we found:

- 41 desktop computers not recorded in ITSM.
- 55 laptops that were ready for destruction and had not been recorded into ITSM. ITS stockroom personnel stated that they would be scanned into ITSM when they have time to dispose of the laptops, and inadequate staffing at this location was the cause for the delay.
- 25 devices identified by Asset Management using procurement records and historical data that should have been, but were not, included in the stockroom's ITSM inventory listing. ITS staff were not able to locate these 25 workstations. This number is down from the approximately 130 workstations they were unable to locate before undertaking a major cleanup of this stockroom (this effort coincided with the timing of our audit).
- 143 workstations (105 laptops and 38 desktops) that they stated were incorrectly listed as In-stock, Available in ITSM when they should have been changed to a state of In-stock, Pending Disposal.

Furthermore, ITS staff at a distribution center (central stockroom where purchased workstations are received) stated there is an issue with stockrooms receiving assets from their location and scanning those devices into their stockrooms. Stockrooms are supposed to scan equipment into their stockrooms upon receipt. ITS staff stated that approximately 2,500 assets were shipped from the ITS Distribution Center to stockrooms that remain in an In-transit state, including approximately 600 assets shipped from this location during calendar year 2024. The devices were shipped to destination stockrooms across the State; however, no confirmation of receipt has been obtained by the ITS Distribution Center for those devices.

Managed control of all ITS assets plays a critical role in security monitoring, incident response, system backup, and recovery. Without an accurate and complete inventory of information assets, ITS cannot adequately safeguard its networks and serve its customers.

Security Over Equipment

ITS has not sufficiently monitored security controls over stockrooms and has not conducted stockroom inspections to determine the adequacy of storage for assets. Of the 23 stockroom locations we visited, we found storage inadequacies at five, including the presence of unsecured workstations and the unsecured storage of hard drives that potentially contain confidential data. For example, we found the following at the five stockroom locations:

- Location 1: We found 36 pallets of used equipment—including workstations, hard drives, monitors, and keyboards—kept in a shared storage area within a building, easily accessible to employees from other State entities (see Figure 1). In addition to ease of access, auditors observed a large water leak in the corner of the storage area near some of the equipment stored by ITS. ITS stockroom personnel stated that all used equipment stored in this area, some of which is data bearing, is to be destroyed. ITS stockroom personnel cited that low staffing levels and the inability to effectively move equipment through the building's freight elevator make properly discarding of old equipment challenging. In November 2023, auditors requested a listing of devices stored on the 36 pallets observed during our site visit; however, ITS was unable to provide this information. ITS cannot ensure security over this data-bearing equipment, nor does it know the contents of the 36 pallets of old equipment at this location.

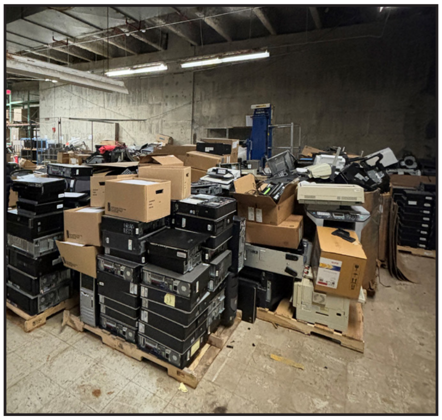


Figure 1 – Approximately 25 of the 36 pallets of devices awaiting disposal

- Location 2: We found equipment stored inadequately. We observed that some equipment was kept in a small closet and in locked cabinets, while other equipment was out in the open, stacked on push carts. Equipment kept on push carts at this location is accessible to anyone with building access. In August 2023, the ITS stockroom regional manager submitted a request to obtain additional storage units, with an estimated completion of March 2024; however, during a subsequent conversation with the stockroom manager, we learned new storage had not been installed as of June 2024. As a result, these workstations, pending setup and deployment, are not properly safeguarded from theft and inappropriate use.
- Location 3: We found unsecured workstation equipment. One side of the storage room required secure key card access; however, on the other side, there was an unlocked door leading to other agency offices. ITS stockroom personnel stated that there was little they could do to rectify this issue. They explained that they are provided with space by their host State entity and are often moved around to different locations within the building depending on the State entity's needs for space, which does not always include adequate equipment storage.
- Location 4: We found workstations in a shared storage room with no additional security measures. This storage room provides employees of other State agencies with offices in the same building access to potentially data-bearing workstations.
- Location 5: We found three boxes of hard drives that had been removed from devices and were stored behind an ITS employee's desk. These devices were kept in a manner that made them inappropriately accessible to other individuals with access to the floor (see Figure 2). ITS staff cited the reason that these hard drives were being kept outside of the secure stockroom was that they were awaiting pickup for destruction. Due to this agency's responsibilities and confidential information, proper controls over data-bearing devices are paramount. ITS cannot be assured that equipment is properly safeguarded if stockroom employees are not following policies instituted by ITS.

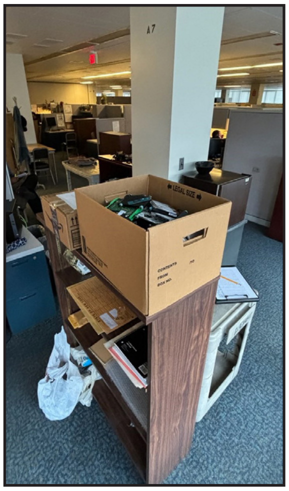


Figure 2 – Unsecured hard drives

In response to our findings, ITS officials stated that they have begun taking steps to improve stockroom security. This includes working with client agencies to ensure physical locations are secure and safe for all personnel. A lock will be added to the rear door of the unsecured stockroom identified, and additional secure storage has been made available for the stockrooms previously lacking it. ITS will conduct site visits to other locations and work with client agencies' landlords to address any identified problems.

Destruction of New or Lightly Used Workstations

During our stockroom site visits, we identified 924 new in-box or lightly used devices that ITS stockroom staff stated were designated to be destroyed or likely to be destroyed. At one stockroom location, we identified 175 unused laptops that were stacked on a pallet labeled for destruction (see Figure 3).

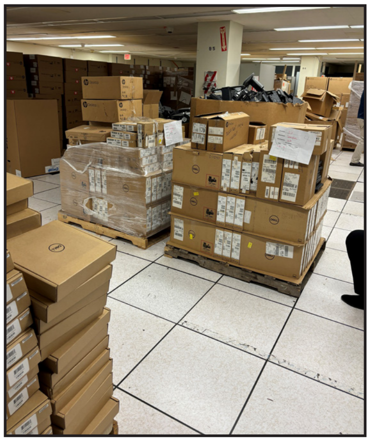


Figure 3 – New and lightly used devices to be destroyed

Also at the same stockroom, we identified 162 desktops with a warranty expiration date of March 2025. ITS personnel stated that, while these desktops could still potentially be deployed, it is unlikely that they will be due to the proximity of the warranty expiring.

At another stockroom, we identified 435 laptops that will be destroyed—170 of those laptops were marked as "break-fix" because their batteries have died due to sitting for too long. ITS personnel stated that they could be fixed, but, due to their age, they will likely be destroyed (see Figure 4). In addition, we identified 265 New York Response COVID-19 vaccination site laptops still in-box that were unused or lightly used during the pandemic.

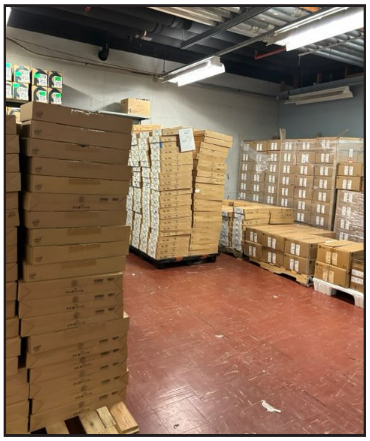


Figure 4 – New, lightly used, and "break-fix" devices to be destroyed

Additionally, at the ITS Distribution Center, we identified 77 laptops and 16 desktop workstations on pallets marked for disposal. Of the 77 laptops, 31 were designated as parts machines, to be used to replace parts for other broken laptops; however, ITS personnel stated that those were likely to be destroyed due to their age. In addition, we identified 54 high-end laptops that are deployed by special request only. These were stated to be stagnant stock that is not deployed frequently and were at risk of being destroyed. In total, we found 924 new or lightly used devices that were marked for disposal. We estimate the value of these devices ranges between $530,000 and $660,000.

ITS stockroom personnel stated workstations are destroyed when decommissioned, even in cases where new, unused equipment is discarded. In the past, new, unused, and lightly used equipment was sometimes donated or sold at State auctions; however, due to the additional processes necessary to donate or sell workstation equipment, ITS currently elects to destroy all discarded equipment, even equipment in new or like-new condition.

Generally, ITS' Asset Management team is responsible for the procurement of workstations. Each year, Asset Management executes a forecast of workstations needed based on the previous year's needs and current year refresh initiatives to provide new devices for onboarding State employees. During the COVID-19 pandemic, typical workstation purchasing controls were overridden to accommodate the work-from-home initiative. ITS Executive Management headed the purchasing of workstations during the pandemic, while ITS' Asset Management team was not involved in procurement. Pandemic-era purchases occurred prior to the institution of the physical inventory requirement, which would have made it impossible for Executive Management to know actual workstation counts available at each stockroom. As a result, there is a risk that ITS over-purchased workstations during the pandemic, which could have led to the workstation waste we observed. ITS should establish an emergency preparedness plan related to the purchasing of workstations during pandemics, natural disasters, or other crises to mitigate over-purchasing of workstation equipment.

In response to the finding, ITS stated the COVID-19 pandemic was an unprecedented public health emergency that presented unique challenges for many State agencies, including ITS. Among those challenges, ITS was tasked with supporting New York State's transition to a largely remote workforce. This required ITS' shift to providing remote-compatible workstations (laptops). The State implemented emergency procurement procedures and the federal government relaxed cost allocation requirements for certain funding streams. The State Division of Budget, through Budget Bulletin H-0503, coordinated and administered COVID-19-related reimbursements to ensure funding was used appropriately. ITS used its normal internal processes to identify aggregate needs and source hardware from vendors that were able to deliver items for the best value. When assets were no longer needed for COVID-19 response activities, the devices were redeployed for other State business needs or taken to be securely disposed. ITS noted it is committed to serving its client agencies, and, having already largely transitioned from desktop to laptop workstations, it better supports remote work capabilities. ITS will continue to ensure that future emergency procurement procedures meet agencies' needs, while following State and federal guidelines.

Additionally, in response to our audit findings, ITS stated that the Hardware Asset Management module will address most of the inventory discrepancies by March 2025. This will provide timely feedback on any future discrepancies that may occur during stock transfer, deployment, and offboarding. The movement and deployment of hardware devices within ITS is a complex undertaking. ITSM is currently leveraged to support approximately 8,000 user equipment refreshes annually as well as thousands of onboardings, offboardings, and repairs each year.

ITS Stockroom Employee Use of ITSM

ITS has not provided stockroom employees with the proper knowledge and skills to competently and effectively use ITSM. We found that ITS stockroom employees at several locations were unable to adequately navigate ITSM to provide reports to the audit team or search the ITSM database for devices by serial number. For example, some stockroom employees were unable to pull a report from ITSM displaying all their In-stock, Available workstations. The ITS audit liaison instead reached out to two other stockroom employees to have them pull the reports for us. While generating inventory reports from ITSM is not a direct responsibility of stockroom employees, the ability to do so allows them to better track and reconcile inventory on hand with ITSM.

We observed that stockrooms generally have a “learn on the fly” approach when it comes to utilizing ITSM and that no comprehensive ITSM training has been offered to stockroom employees, even though stockroom employees we interviewed stated that it would be helpful. Without providing stockroom employees with adequate training on the use of ITSM, ITS cannot be assured that those employees are able to effectively utilize and navigate the system. Without being able to utilize ITSM in a competent and effective manner, it is difficult to maintain accountability over stockroom inventory.

In addition to inadequate knowledge and skills in ITSM, we found ITS personnel at four of the stockrooms we visited reported maintaining their own internal spreadsheets outside of ITSM to track their stockroom inventory. Employees of these stockrooms exhibited a sense of mistrust in the reliability of data in ITSM, and as a result, believed it necessary to maintain their own documentation outside ITS’ requirements.

In response to our audit findings, ITS stated that the Hardware Asset Management module will make it easier for staff to follow policies and procedures for inventory management, and that training manuals will also be updated. Additionally, ITS established an Asset Management team to better enforce asset management tracking procedures. Further, officials noted training and instructions are available through the ITSM Knowledge Management Center and ITS will improve the cyclical review of training programs and update the materials. Additionally, management will highlight the availability of the training materials to stockroom staff to ensure all staff are properly trained.

State Entity Employee Offboarding

ITS is not effectively managing State entity employee offboarding and is allowing State entities to not follow protocols, specifically the reclaiming of equipment after employee separations. We found that State entities can deselect the checkbox in ITSM indicating there is equipment to be returned to ITS and thereby keep the equipment. ITS stockroom personnel and Asset Management stated that this is a known issue and they requested a change in ITSM to prohibit entities from deselecting the offboarding equipment checkbox. In addition, in a July 2024 meeting with ITS officials, ITS stated it has modified the ITSM offboarding service request form and removed the ability for State entities to uncheck the box for hardware return. ITS stockroom personnel will be notified any time staff are offboarded and will search ITSM to determine what assets need to be recovered.

Furthermore, ITS stockroom personnel stated that employee offboarding notifications related to reclaiming equipment from State entity employees do not contain itemized listings of equipment that needs to be recovered, making it difficult for ITS to determine if all equipment is retrieved. Ultimately, ITS is responsible for reclaiming equipment and cannot effectively do so if stockroom employees are not provided with an accurate listing of equipment to be reclaimed and/or State entities are able to inappropriately alter the Employee Offboarding request form.

State Entities Independently Purchasing Devices

ITS stockroom personnel notified us of instances where State entities have purchased their own equipment, and, in some cases, put their own equipment on ITS networks. At one stockroom, we learned of five workstations procured by a State entity that were potentially put on the network, outside of authorized ITS protocols. Those five devices, which were not standard ITS-issued devices, were discovered by the stockroom by manually identifying the make and model of the devices. According to stockroom personnel, they began noticing these devices approximately 1 year prior to our site visit. ITS stockroom personnel stated that they informed their internal ITS liaison of this issue; however, during our audit, it had not been resolved.

ITS Cooperation

For 7 months, during the beginning stages of the audit, the audit team had difficulties obtaining information from ITS. Requests for information would take months to complete, and the documents were often redacted to the point where they were not useful. Additionally, the audit team was often asked to come on-site at ITS to review and scribe documents, rather than ITS sending the documents to the audit team via a secure document transfer. This caused many issues and impaired the audit team’s ability to perform audit duties in accordance with generally accepted government auditing standards. Due to the difficulties receiving information, the audit team issued a scope impairment preliminary report for access to data and key personnel to ITS on December 15, 2023. After we issued the preliminary, we saw substantial improvement regarding the availability of information with ITS, and for the remainder of the audit, there was an adequate exchange of information between ITS and OSC.

Weaknesses in Technical Controls

During our testing, we identified systems not maintained at vendor-supported levels and weaknesses in technical controls that need to be corrected to ensure the selected information systems and their associated data are not at risk. Due to their confidential nature, we disclosed these matters to ITS officials in a separate report and, consequently, do not address them in detail in this report. In response to our findings, ITS officials stated that the Hardware Asset Management module will help address the issues we identified.

Recommendations

1. Conduct a comprehensive review and cleanup of ITSM data to ensure accuracy and completeness, and implement ongoing quality reviews of ITSM data to maintain integrity.
2. Improve oversight and monitoring of stockrooms, which may include, but not be limited to:
   - Developing and implementing standardized stockroom policies and procedures to ensure consistent operations and compliance.
   - Enforcing ITSM asset-tracking procedures to maintain accurate and complete inventory records.
   - Conducting periodic security control reviews of all stockrooms to assess their effectiveness, and coordinating with the host entity to correct security deficiencies identified.
   - Developing an ITSM training curriculum that addresses the specific needs of employees using the system and providing ongoing training and updates to employees as ITSM features and processes evolve.
   - Ensuring compliance with timely completion of quarterly physical inventory audits of stockrooms.
   - Performing a thorough network review to identify and remove unauthorized or unknown devices, and implementing ongoing network monitoring and internal controls to detect and mitigate future anomalies.
3. Maintain an accurate and complete inventory of workstations and other equipment available to ensure efficient use of resources and prevent waste of equipment and taxpayer money.
4. Conduct a comprehensive review of the effectiveness of COVID-19-related workstation purchases including decision-making processes and develop a clear set of guidelines for future emergency workstation procurement.
5. Formally evaluate the current practice of destroying new and lightly used equipment and determine if these devices could be resold or donated.
6. Conduct a review of all offboarding procedures, including equipment recovery, to identify and address deficiencies.
7. Continue to improve the timeliness of cooperation with authorized State oversight inquiries to ensure transparent and accountable agency operations.
8. Implement the recommendation detailed in our preliminary findings to strengthen technical controls over the selected systems reviewed.

Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether ITS has adequate controls to ensure the accuracy and completeness of inventory records, accountability for inventory transactions, and safeguarding of inventory. The audit covered the period from March 2020 through August 2024.

To accomplish our objective and assess related internal controls, we interviewed ITS officials and ITS stockroom staff and reviewed relevant laws as well as ITS policies and procedures related to inventory management. We became familiar with and assessed ITS' internal controls as they related to our audit objective, namely, controls over inventory management to ensure that State entities' needs are being met and that ITS is delivering its services as required. In addition, we conducted visits to 23 ITS inventory stockrooms to determine compliance with ITS guidance and gain a better understanding of the day-to-day operations of a stockroom.

We used a non-statistical sampling approach to provide conclusions on our audit objective and to test internal controls and compliance. We selected judgmental samples. However, because we used a non-statistical sampling approach for our tests, we cannot project the results to the respective stockroom population. Our samples, which are discussed in detail in the body of our report, included:

- A judgmental sample of 23 out of 83 stockrooms was selected based on geographical area, the number of available devices reported to be located at stockrooms, and the number of devices pending disposal at each location to test for any absent devices or bad inventory data in ITSM.
- A judgmental sample of 606 out of 17,444 In-stock, Available workstations was selected at the 23 stockrooms we visited. To ensure a variety of device selections, we considered device make and model, whether the device was a laptop or desktop, the location of the device within the facility, and whether the device was new or used to test for accuracy and completeness of ITSM.
- A judgmental sample of absent devices at 14 of the 23 stockrooms we visited. We used ITSM data provided from December 2023 to select the sample. Only site visits conducted on or after January 16, 2024 were included in this sample due to our analysis not being completed for visits prior to this date. During our visits to the 14 stockrooms selected, we asked staff to locate the absent devices. We used this information to better form our conclusion on the completeness and accuracy of ITSM.
- A judgmental sample of 102 of 448 absent devices was selected at 14 stockrooms we visited. At four of the stockroom locations, we selected the entire population of absent devices because the populations were less than 10. At five of the stockrooms, we selected our absent device sample based on discovery dates, discovery sources, and types of devices. At another five stockrooms, we selected our absent device sample based solely on most recent discovery dates due to lack of information available for devices with older discovery dates.

- A judgmental sample of 50 servers out of 492 was selected to test the accuracy and completeness of the ITSM server data provided. We selected physical servers on a specific domain at one location. Each server must have been in production and in use at the time of our site visit. In addition, our selections needed to have a variety of discovery sources and include different types of servers.

We obtained data from ITSM and assessed the reliability of that data by reviewing existing information, interviewing officials knowledgeable about the system, performing electronic testing, and tracing to and from source data. We determined that the data from this system was not reliable; however, we did not have any other source to obtain the data from. Certain other data in our report was used to provide background information. Data that we used for this purpose was obtained from the best available sources, which were identified in the report. Generally accepted government auditing standards do not require us to complete a data reliability assessment for data used for this purpose.

Statutory Requirements

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.

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. These duties could be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our professional judgment, these duties do not affect our ability to conduct this independent performance audit of ITS' oversight and administration of inventory controls.

Reporting Requirements

We provided a draft copy of this report to ITS officials for their review and formal written comments. We considered their response in preparing this final report and have included it in its entirety at the end of the report. ITS officials generally agreed with the recommendations and have indicated actions they will take to address them.

Within 180 days after 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 recommendations were not implemented, the reasons why.

Agency Comments

NEW YORK STATE | Office of Information Technology Services

KATHY HOCHUL
Governor

DRU RAI
NYS Chief Information Officer

Charles Lansburg
State Program Examiner 2
Office of the State Comptroller
110 State Street
Albany, NY 12236

January 22, 2025

RE: Revised Audit Report 2023-S-017

Dear Mr. Lansburg:

Thank you for the opportunity to review and respond to the draft report from the OSC audit of ITS Inventory Controls.

As you will see from our response below, ITS takes the OSC findings very seriously and is actively working to implement the report recommendations. ITS has recently established an IT Asset Management ("ITAM") team who will be tasked with ensuring assets are accounted for throughout the asset lifecycle: deployment, maintenance, upgrade, and disposal. ITS believes the ITAM team is critical to implement the recommendations in this draft report. The ITAM team implemented a new Asset Management Policy ITS-P24-004, that will be periodically updated to reflect the constantly evolving asset environment that we support and manage. Among other issues, this Policy addresses:

- Potentially unauthorized devices connected to the State network.
- Inactive devices which may be lost or subject to reassignment; and
- Regular device verification.

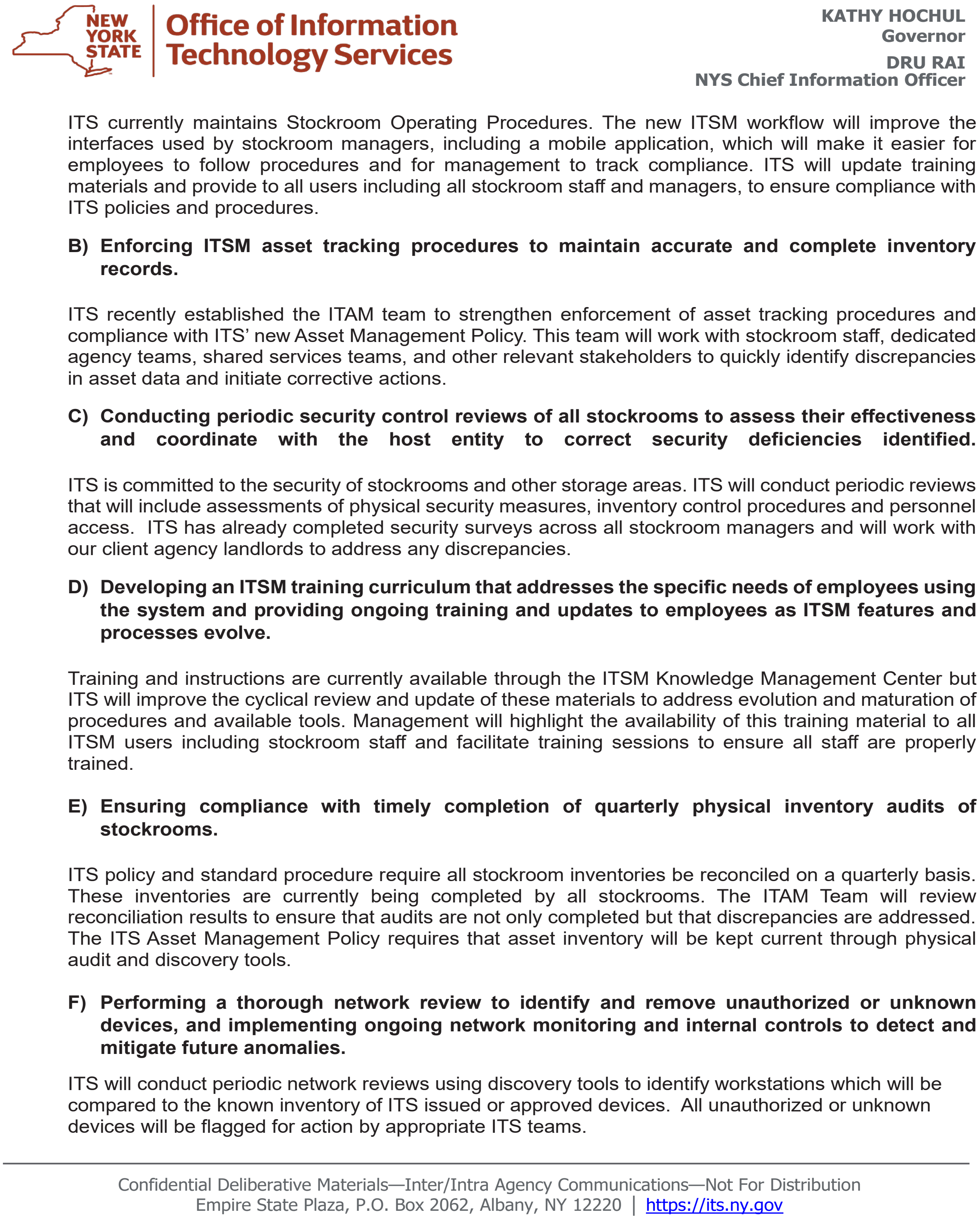
Please find the ITS responses to your recommendations below:

Recommendation 1: Conduct a comprehensive review and cleanup of ITSM data to ensure accuracy and completeness and implement ongoing quality reviews of ITSM data to maintain integrity.

Over the past several months, ITS has been reviewing and remediating ITSM data to correct data quality issues that resulted from automated legacy data integrations and manual data entry errors, such as a barcode for a single asset being mistakenly scanned multiple times. ITS has taken steps to improve monitoring going forward and will continue regular data quality and process reviews to reduce errors and improve data quality. ITS uses and is continuing to develop an asset management system within ITSM. ITS anticipates the updated asset management workflows will be fully integrated into ITS' processes by March 2025. This workflow will provide better tracking of assets throughout their lifecycle.

Recommendation 2: Improve oversight and monitoring of stockrooms, which may include but not be limited to:

A) Developing and implementing standardized stockroom policies and procedures to ensure consistent operations and compliance.



ITS currently maintains Stockroom Operating Procedures. The new ITSM workflow will improve the interfaces used by stockroom managers, including a mobile application, which will make it easier for employees to follow procedures and for management to track compliance. ITS will update training materials and provide to all users including all stockroom staff and managers, to ensure compliance with ITS policies and procedures.

B) Enforcing ITSM asset tracking procedures to maintain accurate and complete inventory records.

ITS recently established the ITAM team to strengthen enforcement of asset tracking procedures and compliance with ITS' new Asset Management Policy. This team will work with stockroom staff, dedicated agency teams, shared services teams, and other relevant stakeholders to quickly identify discrepancies in asset data and initiate corrective actions.

C) Conducting periodic security control reviews of all stockrooms to assess their effectiveness and coordinate with the host entity to correct security deficiencies identified.

ITS is committed to the security of stockrooms and other storage areas. ITS will conduct periodic reviews that will include assessments of physical security measures, inventory control procedures and personnel access. ITS has already completed security surveys across all stockroom managers and will work with our client agency landlords to address any discrepancies.

D) Developing an ITSM training curriculum that addresses the specific needs of employees using the system and providing ongoing training and updates to employees as ITSM features and processes evolve.

Training and instructions are currently available through the ITSM Knowledge Management Center but ITS will improve the cyclical review and update of these materials to address evolution and maturation of procedures and available tools. Management will highlight the availability of this training material to all ITSM users including stockroom staff and facilitate training sessions to ensure all staff are properly trained.

E) Ensuring compliance with timely completion of quarterly physical inventory audits of stockrooms.

ITS policy and standard procedure require all stockroom inventories be reconciled on a quarterly basis. These inventories are currently being completed by all stockrooms. The ITAM Team will review reconciliation results to ensure that audits are not only completed but that discrepancies are addressed. The ITS Asset Management Policy requires that asset inventory will be kept current through physical audit and discovery tools.

F) Performing a thorough network review to identify and remove unauthorized or unknown devices, and implementing ongoing network monitoring and internal controls to detect and mitigate future anomalies.

ITS will conduct periodic network reviews using discovery tools to identify workstations which will be compared to the known inventory of ITS issued or approved devices. All unauthorized or unknown devices will be flagged for action by appropriate ITS teams.

Recommendation 3: Maintain an accurate and complete inventory of workstations and other equipment available to ensure efficient use of resources and prevent waste of equipment and taxpayer money.

The implementation of the new ITSM workflow will address most of the existing inventory discrepancies with workstations by March 2025 and will provide ITS with timely feedback of any future inventory discrepancies which may occur during stock transfer, deployment and offboarding. ITS currently maximizes taxpayer funding by leveraging economies of scale for both hardware and software. The movement and deployment of thousands of hardware devices in a distributed environment of over 100,000 users is a complex undertaking. This process is managed at a variety of levels to save taxpayer dollars while providing employees with robust hardware meeting cybersecurity standards. ITSM reporting will enhance this existing process and further maximize taxpayer dollars.

Recommendation 4: Conduct a comprehensive review of the effectiveness of COVID-19 related workstation purchases including decision making processes and develop a clear set of guidelines for future emergency workstation procurement.

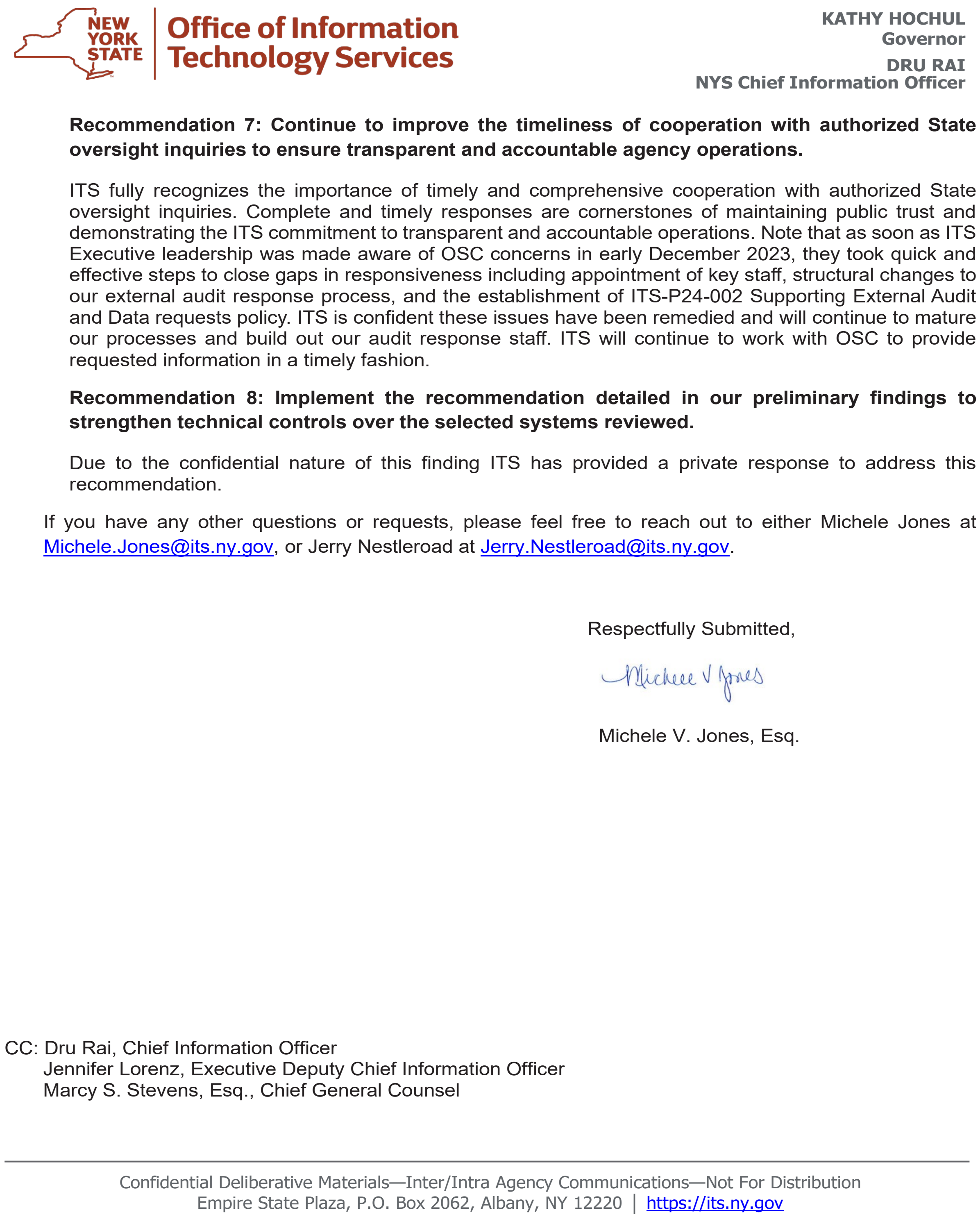
ITS reviewed all workstation procurement during the COVID-19 pandemic and concluded all purchasing was done within State and Federal guidelines. ITS will continue to properly procure equipment to satisfy agency needs within acceptable guidelines. ITS believes the processes in place are effective and will continue to ensure that future emergency procurement procedures meet agency needs while following State and Federal guidelines.

Recommendation 5: Formally evaluate the current practice of destroying new and lightly used equipment and determine if these devices could be resold or donated.

ITS prioritizes data security while disposing of assets in accordance with NYS-S13-003 Sanitization/Secure Disposal standard and relevant regulatory guidelines, as well as State Finance Law Sections 167 and 168. Due to the sensitive nature of the data on some devices, reselling or donation may not always be feasible. Where possible, ITS will explore opportunities for device donation or other means of disposal on a case-by-case basis. ITS has identified donation opportunities through the New York State Education Department's Computer Recycling for Education and Technology Enhancement (CREATE) ACT but reserves the right to pursue any future viable donation program. Resale of devices is carefully evaluated by taking into consideration security risks posed to the agency and associated costs to resell which generally make this solution prohibitive. Regardless of final disposition, all devices are tracked within ITSM.

Recommendation 6: Conduct a review of all offboarding procedures, including equipment recovery to identify and address deficiencies.

ITS modified the ITSM offboarding service request to remove the ability to uncheck the box for hardware return. Due to this modification, local ITS support staff will now be notified anytime staff are offboarded and will search ITSM to determine assets that need to be recovered. These staff will work with supervisors and Agency Dedicated Teams to recover all assets.



NEW YORK STATE | Office of Information Technology Services

KATHY HOCHUL
Governor

DRU RAI
NYS Chief Information Officer

Recommendation 7: Continue to improve the timeliness of cooperation with authorized State oversight inquiries to ensure transparent and accountable agency operations.

ITS fully recognizes the importance of timely and comprehensive cooperation with authorized State oversight inquiries. Complete and timely responses are cornerstones of maintaining public trust and demonstrating the ITS commitment to transparent and accountable operations. Note that as soon as ITS Executive leadership was made aware of OSC concerns in early December 2023, they took quick and effective steps to close gaps in responsiveness including appointment of key staff, structural changes to our external audit response process, and the establishment of ITS-P24-002 Supporting External Audit and Data requests policy. ITS is confident these issues have been remedied and will continue to mature our processes and build out our audit response staff. ITS will continue to work with OSC to provide requested information in a timely fashion.

Recommendation 8: Implement the recommendation detailed in our preliminary findings to strengthen technical controls over the selected systems reviewed.

Due to the confidential nature of this finding ITS has provided a private response to address this recommendation.

If you have any other questions or requests, please feel free to reach out to either Michele Jones at Michele.Jones@its.ny.gov, or Jerry Nestleroad at Jerry.Nestleroad@its.ny.gov.

Respectfully Submitted,

Michele V Jones

Michele V. Jones, Esq.

CC: Dru Rai, Chief Information Officer
Jennifer Lorenz, Executive Deputy Chief Information Officer
Marcy S. Stevens, Esq., Chief General Counsel

Contributors to Report

Executive Team

Andrea C. Miller - *Executive Deputy Comptroller*
Tina Kim - *Deputy Comptroller*
Stephen C. Lynch - *Assistant Comptroller*

Audit Team

Nadine Morrell, CIA, CISM - *Audit Director*
Amanda Eveleth, CFE - *Audit Manager*
Justin Dasenbrock, CISA, ITIL, CC - *IT Audit Manager*
Daniel Raczynski - *IT Audit Manager*
Charles Lansburg - *Examiner-in-Charge*
Logan Frese - *Information Systems Auditor*
Alma Pleasant - *Senior Examiner*
Rachel Moore - *Senior Editor*

Contact Information
(518) 474-3271
StateGovernmentAccountability@osc.ny.gov
Office of the New York State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

For more audits or information, please visit: www.osc.state.ny.us/state-agencies/audits