

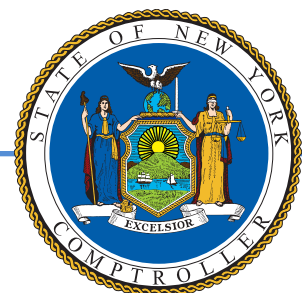
Department of Corrections and Community Supervision

Controls Over Tablet and Kiosk Usage by Incarcerated Individuals

Report 2022-S-8 | May 2023

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Division of State Government Accountability



Audit Highlights

Objectives

To determine whether the Department of Corrections and Community Supervision provides sufficient oversight to ensure that the independent network, kiosks, and tablets used by Incarcerated Individuals are secure, and whether secure messaging accessed by these individuals complies with Department Directives. The audit covered the period from February 2019 through August 2022.

About the Program

The Department of Corrections and Community Supervision (Department) is responsible for the confinement and rehabilitation of approximately 31,000 individuals in its custody at 44 facilities throughout the State. The Department has contracted with Securus and its subsidiary JPay Inc. (Provider) to provide Incarcerated Individuals (or Individuals) with access to tablets and kiosks (tablet program). Department Directives (or Directives) contain policies and procedures governing the tablet programs available to Incarcerated individuals. Through loaned tablets, general population Individuals have access to Department-approved educational material; the ability to purchase Department-approved music, videos, e-books, and other media; and the opportunity to communicate with family and friends using a fee-based secure messaging system through an account created on the Provider's website. Individuals in specialty populations are allowed limited access to two types of tablets: a law library tablet that contains access to law library material and a static content tablet that provides telephone access and Department-approved, preloaded applications, such as educational material, videos, e-books, music, and games. While the static and law library tablets used by the specialty populations receive periodic software updates through Wi-Fi, all other tablets are not Wi-Fi enabled, and must be synced to a kiosk to receive updates and to send or receive secure messages. All secure messages are subject to content screening by authorized facility staff. Upon release or transfer out of the Department's custody or when opting out of the tablet program, the Individual's assigned tablet shall be returned to the Provider, as outlined in Department Directives. Facility employees are responsible for inspecting the physical security and condition of kiosks daily, and must complete and note any damage or evidence of tampering on a daily safety checklist. The tablet program was implemented in 2019. During the audit period, the Department had 1,093 active kiosks and 26,563 active general population tablets.

According to the State's Information Security Policy, all State government entities, including their third parties (e.g., local governments, consultants, vendors, and contractors) are required to maintain systems at a vendor-supported level to ensure the accuracy and integrity of information.

Key Findings

- According to the Department, it is not responsible for the tablet program, which it describes as a relationship between the Provider and Individuals. This position has resulted in limited assurance of compliance with Department Directives.
- The Department does not know how many Individuals have opted in/out of the tablet program and does not internally monitor the number of active tablets at its facilities. Instead, the Department relies on the Provider to maintain these records at both the statewide and facility levels.
- The Department does not verify the identity of community members who are in correspondence with Individuals through secure messaging, and its secure message content screening process does not adequately capture all risks to Individuals and others.

-
- The Department is not adequately overseeing the security and configuration of certain assets, and does not ensure systems are maintained at vendor-supported levels required to preserve the accuracy and integrity of Department information.

Key Recommendations

- Strengthen the Department's responsibility and role in the relationship between the Provider and Individuals.
- Develop, implement, and adhere to an internal process to effectively monitor program participation and tablet inventory at both the facility and statewide levels.
- Implement a process to ensure that Individuals' correspondence with community members via secure messaging complies with Department Directives.
- Ensure that systems are maintained at vendor-supported levels. Until then, the Department should work with the Office of Information Technology Services to submit the required exception request form.
- Implement the remaining technical recommendations detailed in the preliminary report.



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

May 11, 2023

Anthony J. Annucci
Commissioner
Department of Corrections and Community Supervision
1220 Washington Avenue
State Campus Building 2
Albany, NY 12226

Dear Mr. Annucci:

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.

Following is a report of our audit entitled *Controls Over Tablet and Kiosk Usage by Incarcerated Individuals*. 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** **5**
- Background** **6**
- Audit Findings and Recommendations** **8**
 - Secure Messaging **8**
 - Physical Security **10**
 - Technical Controls **12**
 - Recommendations **12**
- Audit Scope, Objectives, and Methodology** **14**
- Statutory Requirements** **16**
 - Authority **16**
 - Reporting Requirements **16**
- Agency Comments and State Comptroller’s Comments** **17**
- Contributors to Report** **24**

Glossary of Terms

Term	Description	Identifier
Department	Department of Corrections and Community Supervision	<i>Auditee</i>
Checklist	Daily safety checklist used to document visual inspection of kiosks	<i>Key Term</i>
Directives	Department Directives	<i>Policy</i>
Individuals	Incarcerated Individuals	<i>Key Term</i>
ITS	Office of Information Technology Services	<i>Agency</i>
JPay Account	Account required to access the kiosks and secure messaging	<i>Key Term</i>
Provider	Securus and its subsidiary JPay Inc., with whom the Department contracted to provide Individuals with access to tablets, kiosks, and telephone	<i>Key Term</i>

Background

The mission of the Department of Corrections and Community Supervision (Department) is to improve public safety by providing continuity of appropriate treatment services in safe and secure facilities where the needs of the population are addressed, Incarcerated Individuals (or Individuals) in its custody are successfully prepared for release, and parolees under community supervision receive supportive services that facilitate a successful completion of their sentence. As of August 2022, the Department had responsibility for the confinement and rehabilitation of approximately 31,000 Individuals held in custody at its 44 State facilities.

To aid in addressing its mission and serve the needs of the Individuals under its custody, the Department has contracted with Securus and its subsidiary JPay Inc. (Provider) to provide Individuals with access to tablets and kiosks (hereafter referred to as the tablet program). Department Directives (or Directives) contain policies and procedures governing tablet programs available to Incarcerated Individuals. Through loaned tablets, Individuals in the general population can access Department-approved educational material; purchase Department-approved music, videos, e-books, and other media; and communicate with family and friends using a fee-based secure messaging system through an account (JPay Account). Individuals establish a JPay Account during tablet distribution that is used in conjunction with a kiosk to send secure messages, while community members create their JPay Account on the Provider's website. Individuals in specialty populations, such as the Special Housing Unit and Regional Mental Health Unit, are allowed limited access to two types of tablets: a law library tablet that contains law library material, such as legal books and journals, and a static content tablet that provides telephone access and Department-approved, pre-loaded applications, such as educational material, videos, e-books, music, and games. Additionally, these tablets are used at the four facilities where Individuals can enroll in a tablet-based college program with Ashland University.

General population tablets, which come with a protective case, earbuds, and a charger, are distributed to Individuals at one of three facilities that have a reception center. Reception center staff distribute the items and send weekly inventory email updates with the number of tablets on hand to the Department's Central Office. All facilities have a package room or mailroom responsible for collecting broken or returned tablets and/or accessories and shipping them back to the Provider. Upon release or transfer out of the Department's custody, or opting out of the tablet program, the Individual's assigned tablet shall be returned to the Provider, as outlined in Department Directives. Those who choose to opt out must sign an "Incarcerated Individual Tablet Program Opt Out" form.

The tablets used by specialty populations for telephone and law library access use Wi-Fi to receive periodic software updates. However, all other tablets are not Wi-Fi enabled and must be synced to a kiosk to receive periodic software and content updates. The tablets used by the general population must also be synced to a kiosk to send or receive secure messages from an Individual's JPay Account to a family member's or friend's account. Both tablets and kiosks require periodic software and application upgrades, which are performed by the Provider upon the Department's approval.

Department officials meet weekly with the Provider to discuss tablet program updates. Employees at each facility are responsible for conducting daily inspections of the physical security and condition of kiosks and the facility areas where kiosks have been installed. Any damage or evidence of tampering must be noted on a daily safety checklist form (Checklist) and must be immediately reported to the facility Watch Commander. The report is then sent to the facility maintenance office, which notifies the Provider to address the issues identified. All completed Checklists are sent to, and retained by, the Fire Safety Officer. In addition to visual inspections, all secure messages are subject to content screening by authorized staff.

The tablet program was implemented in 2019. During the audit period, the Department had 1,093 active kiosks and 26,563 active general population tablets.

According to the State's Information Security Policy, all State government entities, including their third parties (e.g., local governments, consultants, vendors, and contractors) are required to maintain systems at a vendor-supported level to ensure the accuracy and integrity of information.

Audit Findings and Recommendations

The Department does not internally monitor the number of active tablets in its facilities, nor does it know how many Individuals have opted in/out of the tablet program. The Department also does not verify that Individuals are corresponding with community members in accordance with Department Directives. As a result, there is limited assurance that the Department is able to detect inappropriate activity, such as tablets being removed from a facility or used by someone other than the Individual to whom it is assigned, nor can the Department be assured that Individuals are not messaging community members whom they are legally prohibited from corresponding with. In addition, the Department may be unaware of potentially dangerous activity exchanged in secure messages and would be unable to proactively address and prevent any threats to the safety, security, and well-being of the facility and Incarcerated Individuals, such as content that may negatively impact an Individual's mental health.

In addition, the Department is not adequately overseeing the security and configuration of certain assets. Until the Department implements a corrective action plan to appropriately identify, accept, and manage the associated risks, these systems will continue to present a risk to the operation of the Department's facilities.

According to Department officials, the tablet program is a relationship between the Provider and the Individual that is conducted at the Department's facilities, and the Department is not responsible for the tablets and kiosks – even though the contract, which is between the Department and the Provider, and Department Directives, which require certain security controls, suggest otherwise. The Department's position has resulted in limited assurance of compliance with Department Directives – which are overridden on an as-needed basis or are only enforced if a problem is identified at the facility.

Secure Messaging

Content Screening

The Department screens all Individuals' secure messages at its facilities for select content. Any inbound and outbound message that does not adhere to Department policies is captured by the screening mechanism for review by facility staff prior to delivery. To assess the effectiveness of the Department's current screening mechanism, we conducted secure message testing using a JPay Account created for audit testing purposes. We sent secure messages from our test JPay Account to a sample of 46 Individuals located at the 12 facilities we visited. The testing prevented the content from ultimately being delivered to the Individuals selected for testing. Based on the results of our testing, we discussed with the Department certain limitations in the design of its system, for which the Department accepted the risk due to its assessment of the cost benefit. The Department considers its screened content proprietary and confidential; thus, these concerns were discussed privately with the Department and are not reported here.

We found that all but three of the 46 messages containing Department-screened content were captured in the system for additional review as intended. According to

officials, the three messages – sent to Individuals at three separate facilities – with Department-screened content were not captured in the system because the content related to a mental health pilot program that is only screened at select facilities. Although requested, the Department was unable to provide documentation to support its mental health pilot program assertion. Furthermore, if the mental health content screening process is only conducted at select facilities, this represents a missed opportunity for the Department to monitor and address potential mental health issues at all facilities.

Additionally, we identified, and Department officials confirmed, certain issues regarding the Department’s secure messaging content screening mechanism. Due to their confidential nature, these issues were discussed with the Department privately. These limitations may create opportunities whereby the screening process could allow harmful messages to pass through.

Verification Checks

According to Department Directives, correspondence by an Individual to certain community members, such as unrelated minors or an Individual’s crime victim, requires special advance approval. Further, Individuals are generally prohibited from using secure messaging to communicate with: other Individuals; those who are civilly committed as a dangerous sex offender or are being evaluated for civil management as a detained sex offender; and any person listed on an active Court Order of Protection prohibiting such contact.

We determined, however, that any community member who creates a JPay Account can initiate contact with any Individual. According to Department officials, they have no way of determining or verifying the identity of those community members corresponding with Individuals via secure messaging and thus whether such correspondence adheres to its own Directives. Department officials stated they do not see the value of performing identity verification checks since contact via secure messaging must be initiated by the community member, and they are not concerned with who is contacting Individuals unless the Individual is involved in nefarious activities. When asked how they would identify correspondents who require special advance approval or are prohibited from but may be contacting Individuals via secure messaging, officials responded they would “find them eventually.”

In addition, according to Department Directives, whenever a recipient of an Individual’s correspondence indicates, in any manner, that further correspondence from an Individual is not desired, the appropriate Department officials and Individual shall be notified and the recipient’s name shall be added to a “negative correspondence/telephone list.” However, the Department has limited assurance that its Directives are being followed, as officials stated their secure message review process does not screen community members against the negative correspondence/telephone list. According to officials, the number of community members on this list is too minimal to waste the money and resources it would require, stating “it will be a lot of work with little return” and “the juice is not worth the squeeze.”

Lastly, the Department has the ability to place Individuals with a certain risk level on “mail watch,” which requires all communication, including secure messages, to be reviewed by the Department. Individuals placed on mail watch for secure messaging have a note in their JPay Account, which flags every incoming and outgoing message for review by the Department’s Central Intelligence Unit prior to delivery. However, the Department has only placed one individual on mail watch for secure messaging since the start of the tablet program in 2019.

Physical Security

The Department does not internally monitor the number of active tablets at its facilities or the population of Individuals who have opted in/out of the tablet program. Without knowing how many tablets have been assigned, and to whom, the Department is unable to enforce the policies and procedures outlined in its Directives. The Department does not consistently ensure compliance with the security controls outlined in its own Directives; rather, it relies on an “honor system” of the incarcerated population, without monitoring and enforcement of routine procedures and security controls. According to officials, the Directives are applied in a manner they likened to enforcement of a speed limit sign – used as a way to hold them accountable if violated, but not a guarantee asserting it will not happen.

Inventory Monitoring and Tablet Physical Security

During our site visits, we found the Department does not monitor the number of active tablets in its facilities and does not know how many Individuals have opted in/out of the tablet program. In order to provide the audit team with the total number of active tablets in its facilities, the Department had to request and obtain this information from the Provider. Further, the Provider was unable to give the Department the number of tablets used by specialty populations at each facility. The Provider stated that tablets used by specialty populations are considered community-based tablets that have no true ownership since they are handed out and collected daily; are only visible to the Provider’s network engineers if located within range of the wireless access points; and are in constant turnover – all factors that contribute to a difficult tracking process. Without knowing how many, to whom, or where the tablets are assigned, facility management and Department officials at Central Office are unable to enforce the controls put in place by their Directives.

The Department also does not monitor compliance with the Directive that prohibits the sharing of tablets and associated passwords or pin numbers between Individuals. Rather, Department officials stated they rely on an honor system of the incarcerated population. Although tablets are issued from the Provider with three different-colored cases based on their location of use in the facility (i.e., general population tablets in housing units, static content and law library tablets in special housing units), tablets assigned to Individuals are not labeled with the Individual’s name or Department identification number to identify ownership. In response, Department officials asserted that tablets are the property of the vendor and that an identification label would damage the tablets, yet conversely indicated that an identification label would

not assist in enforcing its Directives since an Individual could just peel the label off. We question the risk of identification labels causing damage to tablets if, as officials state, they could be easily peeled off. This issue notwithstanding, the labeling of tablets would provide some measure of oversight of the tablet program.

Kiosk Inventory

As part of our audit testing, we compared kiosks installed at the 12 facilities we visited with Department records to determine whether they were online, had a unique ID, and appeared to be working in accordance with Department Directives. We found irregularities related to five kiosks at three correctional facilities, as follows:

- At one facility, a kiosk listed in the Department's records was never installed or operational.
- For a second facility, the Department's records did not accurately reflect the location of two kiosks.
- At another facility, two kiosks had the same identification number listed on them and Department records only accounted for one of the kiosks. Department officials stated the second kiosk with the same identification number was associated with alternative kiosk records for a closed annex section of the facility.

Without accurate, complete records of all tablet program assets installed and located in Department facilities, officials are unable to sufficiently monitor whether assets are secure and functioning as intended.

Daily Safety Checklists

During our site visits to the 12 facilities, we requested and reviewed copies of all daily Checklists completed by facility staff for the preceding day and spot-checked a sample of Checklists in process on the day of our site visit. These Checklists are required by Department Directives. We assessed whether the Checklists were completed in accordance with the Directives, including a verification of the physical security and condition of the kiosks and the facility area where the kiosks are installed. Any damage or malfunction related to the kiosks must be noted on the Checklist, which is forwarded to facility maintenance, who then notifies the Provider for on-site repair. We found 40 instances at six facilities where employees did not complete a visual inspection of the kiosk during their shift and four instances at two facilities where the number of kiosks in the buildings were not properly documented and accounted for on the daily Checklist. Therefore, we were unable to determine whether these kiosks were inspected as required. Further, we found four facilities were using outdated Checklists – some dating back to 2012 and some that did not account for kiosk inspection. According to Department officials, they instructed facilities to use their existing supply of outdated Checklists to avoid waste. We question why Department officials did not also instruct facilities to amend the outdated forms to include a review of the kiosks for compliance with the Directives. Insufficient oversight of program assets may inhibit the timeliness of tablet

software updates performed through the kiosks, which are essential to mitigating vulnerabilities as well ensuring that tablets can be used as intended.

Technical Controls

The Department is not adequately overseeing the security and configuration of certain assets, and does not ensure they are maintained at vendor-supported levels required to preserve the accuracy and integrity of information and thus ensure that the tablet program functions as intended, including maintaining appropriate security. Further, the Department did not submit the required Office of Information Technology Services (ITS) exception request form to appropriately identify and accept the associated risks of the unsupported system. If not configured and secured appropriately, assets may pose a risk to the Department's systems and data.

According to the State's Information Security Policy, all State government entities, including their third parties (e.g., local governments, consultants, vendors, contractors), are required to maintain systems at a vendor-supported level to ensure the accuracy and integrity of information. The policy defines systems as including, but not limited to, servers, platforms, networks, communications, databases, and software applications. We determined that certain Provider systems used within the Department's facilities for the tablet program are not maintained at a vendor-supported level. Until systems are supported, or the Department implements a corrective action plan to appropriately identify, accept, and manage the associated risks, these systems will continue to present a risk to the operation of the Department's facilities. The Provider performed its own review of the system and, while acknowledging the potential vulnerabilities associated with the unsupported system, it contended that mitigating controls implemented reduced the risk of exploitation to an acceptable level.

Due to their confidential nature, we communicated the details of the unsupported system we identified to Department officials in a separate preliminary report and do not address those details in this report. To conduct these technical tests at the Department, a substantial effort in coordination between Central Office, the 12 facilities, and the Provider was needed. We appreciate the effort and support provided by the Department while conducting these tests.

Recommendations

1. Strengthen the Department's responsibility and role in the relationship between the Provider and Individuals for the tablet program.
2. Implement a process to ensure that Individuals' correspondence with community members via secure messaging complies with Department Directives.
3. Implement a process to ensure compliance with the negative correspondence/telephone list.
4. Ensure that all kiosks located at facilities are visually inspected in accordance

with Department Directives, and facilities are using updated daily Checklists to complete visual inspections of kiosks.

5. Develop, implement, and adhere to an internal process to effectively monitor program participation and tablet inventory at both the facility and statewide levels.
6. Ensure that systems are maintained at vendor-supported levels, including those under the vendor's responsibility. Until then, the Department should work with ITS to submit the required exception request form.
7. Implement the remaining technical recommendations detailed in the preliminary report.

Audit Scope, Objectives, and Methodology

The objectives of our audit were to determine whether the Department provides sufficient oversight to ensure that the independent network, kiosks, and tablets used by Incarcerated Individuals are secure, and whether secure messaging accessed by these Individuals complies with Department Directives. This audit covered the period from February 2019 through August 2022.

To accomplish our objectives and assess related internal controls, we interviewed Department officials at Central Office and the facilities, Provider officials, and ITS officials to discuss their roles and oversight responsibility related to the tablet program. We also reviewed applicable laws and regulations; Department policies, procedures, and Directives; ITS policies; and the Department's active contracts with the Provider. We obtained data concerning the Department's facilities, its master kiosk inventory per facility, and its secure messaging content screening process.

We judgmentally selected 12 correctional facilities based on the following factors: facilities' location within the State, reception center facilities, and facilities that use the Lantern educational application to access the Department's academic program and Ashland University distant learning program. At each facility, we conducted meetings with facility officials to discuss Individuals' use of tablets for education purposes and facility controls over Provider tablets. We conducted a walkthrough at each facility and visited each building where kiosks were located and the secured housing unit and infirmary where the Provider Wi-Fi-enabled tablets (static tablets and law library tablets) are held. We performed scans using OSC-provided testing equipment and software. We also reviewed a judgmental sample of Checklists in progress on the day of our site visits, based on the number of buildings and floors, and requested copies of all completed Checklists from the day preceding our site visit to assess whether they were completed in accordance with Department Directives. We visually counted and inspected all kiosks located in the facility and noted broken sync cables, non-functioning kiosks, and any evidence of tampering, and compared our count to the kiosk records provided by the Department.

We conducted secure messaging testing using a JPay account created for audit purposes to assess the Department's screening process. We sent test messages to a select population of Individuals in the secure housing unit at each of the 12 facilities visited. The day before each site visit, Department officials sent the Department identification number of up to five Individuals (pending current facility population in the secure housing unit) from which we selected up to five Individuals' JPay Accounts for testing at each facility using a random number generator. Forty-six JPay Accounts at 12 facilities each received two test messages.

We performed a count of the green law library tablets and gray static tablets and assessed how they are tracked at 10 of 12 facilities; audit staff availability limitations precluded this work at the remaining two facilities. We performed technical tests of tablet software based on Department-provided information. To determine whether the Department was maintaining its systems at vendor-supported levels, we viewed various settings and compared the system identified with the last supported date for those systems. We also tested housing restrictions placed on tablets by the Department at five facilities when we identified a risk during our testing by

connecting a tablet to a kiosk in another, non-assigned housing unit. None of the samples selected for our audit testing were projected or intended to be projected to a population as a whole.

Additionally, we verified the reliability of the data used to conduct our audit work that would be used as support for findings and found the data sets were sufficiently reliable for the purposes of our audit. We compared the master kiosk inventory list provided by the Department to the number of kiosks installed at the facilities according to the Provider's website. We assessed the reliability of the Department's secure message content screening process by using a random number generator tool to select a sample and found that the data sets were sufficiently reliable for the purposes of our audit.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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 the Department's oversight and administration of controls over tablet and kiosk usage by Incarcerated Individuals.

Reporting Requirements

We provided a draft copy of this report to Department officials for their review and formal comment. Their comments were considered in preparing this final report and are included in their entirety at the end of it. Department officials disagreed with our conclusions. Our responses to certain Department comments are embedded within the Department's response as State Comptroller's Comments.

Within 180 days after final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the Department of Corrections and Community Supervision 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 and State Comptroller's Comments



Corrections and Community Supervision

KATHY HOCHUL
Governor

ANTHONY J. ANNUCCI
Acting Commissioner

April 17, 2023

Nadine Morrell
Audit Director
Office of the State Comptroller
110 State Street, 11th Fl
Albany, NY 12236

RE: Report 2022-S-8 "Controls Over Tablet and Kiosk Usage by
Incarcerated Individuals"

Dear Audit Director Morrell:

The Department of Corrections and Community Supervision (DOCCS) has reviewed the Office of the State Comptroller's Draft Audit Report 2022-S-8, "Controls Over Tablet and Kiosk Usage by Incarcerated Individuals." In accordance with Section 170 of the Executive Law, please find attached the Department's reply.

We are complying with the provisions of the Budget Policy and Reporting Manual, Item L-100, by submitting a copy of this response to the Division of the Budget's Building a High Performance Government SharePoint site.

DOCCS would like to acknowledge the time and effort of all OSC employees who were involved with this audit and their desire to improve the Department's operation.

Sincerely,

A handwritten signature in black ink, appearing to read "Anthony J. Annucci".

Anthony J. Annucci
Acting Commissioner

Attachment

cc: Daniel F. Martuscello, Executive Deputy Commissioner
Anne Marie McGrath, Deputy Commissioner
Osbourne A. McKay, Deputy Commissioner
Cathy Sheehan, Deputy Commissioner and Counsel
Melissa Coolidge, Associate Commissioner
Lori C. Young, Director, Bureau of Internal Controls
Muhammad Zamir, Director, Internal Audit Unit



Corrections and Community Supervision

KATHY HOCHUL
Governor

ANTHONY J. ANNUCCI
Acting Commissioner

April 17, 2023

Ms. Nadine Morrell Audit Director
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, New York 12236

Dear Ms. Morrell:

This is in response to the draft audit report, 2022-S-8, "Controls Over Tablet and Kiosk Usage by Incarcerated Individuals", which looked at the Department's oversight of the incarcerated tablet program to ensure that the independent network, kiosks, and tablets used by the incarcerated population are secure and whether secure messaging accessed by these individuals complies with Department Directives.

We appreciate the opportunity to review the draft report, key findings, and recommendations. The following is an outline of inaccuracies in the draft report and responds to the key findings and proposed recommendations:

State Comptroller's Comment – DOCCS officials did not respond to any of our preliminary reports, which we routinely provide to our auditees as a means of encouraging and maintaining transparency and an open dialogue throughout the audit process. These written preliminary findings also give the audited entities an opportunity to correct any potential errors of fact. Had DOCCS officials responded to our preliminary reports at the outset, this would have allowed us to address any misunderstandings of the findings early on.

Key Findings

OSC: According to the Department, it is not responsible for the tablet program, which it describes as a relationship between the Provider and Individuals. This position has resulted in limited assurance of compliance with Department Directive.

DOCCS Response: This is an inaccurate representation of what was said during the multiple meetings OSC held with DOCCS' staff. DOCCS is responsible for the administration of the incarcerated tablet program, kiosks, infrastructure, and responsiveness of the vendor as described in our contract with the provider and as outlined in the Department Directive #4425, "Incarcerated Individual Tablet Program". DOCCS monitors overall trouble tickets submitted by the incarcerated individuals to ensure they are addressed/resolved by the vendor. DOCCS expressed to OSC that when an incarcerated individual purchases content or services via the contract from the vendor, the purchase is between the provider and the incarcerated individual.

State Comptroller's Comment – We disagree that it is an inaccurate representation of what DOCCS officials said. As noted on page 8 of the report, officials stated to us that the tablet program is a relationship between the Provider and the Individual that is conducted at DOCCS facilities, and DOCCS is not responsible for the tablets and kiosks. Further, this information was provided to DOCCS officials in our preliminary reports, which they declined to respond to, as indicated above.

OSC: The Department does not know how many individuals have opted in/out of the tablet program and does not internally monitor the number of active tablets at its facilities. Instead, the Department relies on the Provider to maintain these records at both the statewide and facility levels.

DOCCS Response: Upon the issuance or declination of a tablet at Reception, the incarcerated individual completes the appropriate form, which is maintained in the incarcerated individual's file. Due to the vast amount of movement between and within facilities, the inventory records that OSC is recommending DOCCS maintain would be immediately outdated, any attempt to maintain such a count would not be feasible for the Department and would be a duplication of effort. At a moment's notice, the Department can determine who has been assigned a tablet and if they are actively using such tablet through our provider. The utilization of the tablets and kiosks are monitored by several staff, whether it be the housing unit Correction Officers who are watching the individuals using the kiosk and completing the daily safety sheets, the Correction Lieutenants monitoring the secure messages, investigators from OSI, CIU, or maintenance staff.

State Comptroller's Comment – In its response, DOCCS states that it does not internally monitor the number of active tablets at its facilities or the population of Individuals who have opted in/out of the tablet program – which is the finding in the audit. However, DOCCS states it can obtain the inventory from the provider. Yet when asked, the Provider was unable to provide DOCCS with the number of tablets used by specialty populations at each facility as they are considered community-based tablets that have no true ownership. Without knowing how many tablets have been assigned and to whom, DOCCS is unable to enforce the policies and procedures outlined in its Directives. Therefore, it is unclear what point DOCCS is trying to make.

Additionally, the Department prohibits the sharing of passwords, however, like in the outside world, there is no practical way to proactively enforce such. When we find this happening, we take a progressive approach that ranges from counseling to the issuance of a misbehavior report. Furthermore, while the tablets are not engraved or affixed with labels indicating who has been assigned a particular tablet, each tablet is assigned within the software installed on the tablet and, when powered on, it displays the incarcerated individual's name and DIN, which allows staff to enforce our policy of not sharing tablets.

State Comptroller's Comment – The Directive prohibits the sharing of tablets and passwords. Individuals' usage of tablets in the housing units is not strictly monitored or supervised by facility staff; instead, DOCCS officials rely on an "honor system" among incarcerated individuals. In contrast, a proactive approach such as affixing identification labels to the tablets would allow staff to easily see who the assigned user is, without powering on, and readily recognize when tablets are being shared.

OSC: The Department does not verify the identity of community members who are in correspondence with individuals through secure messaging, and its secure message content screening process does not adequately capture all risks to individuals and others.

DOCCS Response: OSC inappropriately took sections of Directive #4422, "Incarcerated Individual Correspondence Program" and applied them to Directive #4425, "Incarcerated Individual Tablet Program" as this directive references the need to be in compliance with all **applicable** provisions as outlined in

Directive #4222, regarding mail, contraband, and incarcerated individual communication. After review of the section of Directive #4422 as referenced in the report, the Department asserts it was not our intent to make all sections listed applicable as referenced in Directive #4425. Furthermore, the section of Directive #4422 that is cited in the report deals only with outgoing correspondence from an incarcerated individual, not from members of the community, thus it would be inappropriate to place such requirements on community members who are corresponding via secure message. Equally important, an incarcerated individual cannot send a secure message to any community member and may only correspond to community members who initiate contact with them.

DOCCS has the ability to identify IP addresses through investigation when necessary. Additionally, there is a process to protect incarcerated individuals who do not wish to receive secure messages. The system allows the incarcerated individual to delete messages on the kiosk without opening or downloading them and also allows the incarcerated individual to remove any community member from their contact list. Once removed, the community member cannot message the incarcerated individual.

With regards to the correspondence with community members, as previously stated above, community members must initiate contact with the incarcerated individual in order for the incarcerated individual to correspond with the community member. If the community member does not initiate contact, the incarcerated individual cannot correspond with anyone they so choose. Lastly, the verification standard recommended by OSC is not realistic and could be circumvented by community members by having other individuals registering and then sharing access. The Department has put many safeguards in place to ensure the safety and security of our institutions, staff, the incarcerated population, and the public.

State Comptroller's Comment – We did not inappropriately apply the Directives. Directive #4425 states that Individuals and community members using secure messaging must adhere to all applicable provisions as outlined in Directive #4422 regarding mail, contraband, and Individual communication. Further, we met with DOCCS officials several times on this issue, and they never voiced their concerns regarding the Directives we were using as criteria in this area. Moreover, if DOCCS' intent was to exclude certain sections of Directive #4422 within Directive #4425, it should have specifically done so. Poorly written policies and procedures create compliance risk.

DOCCS has maintained adequate controls over the review and screening of secure messages based on the input of correctional professionals and as outlined in Department Directive #4425. DOCCS will continue to explore ways to enhance screening processes to mitigate any risk to staff, incarcerated individuals and the public.

Key Recommendations

OSC: Strengthen the Department's responsibility and role in the relationship between the Provider and Individuals.

DOCCS Response: The Department has several Central Office Executive Staff that are involved in the day-to-day administration of the Incarcerated Individual Tablet Program and the oversight of our contract with the provider, including participating in weekly calls with the Provider. In addition, as was clearly witnessed during the OSC site visits, DOCCS has over 420 Correction Lieutenants who are monitoring and screening secure messages across the State, over 200 investigative staff from the Office of Special Investigations, and in excess of 50 members of the Crisis Intervention Unit, along with facility Executive staff and maintenance staff at each institution who interact with the Provider and thousands of Correction Officers who perform the daily safety checklist inspections.

State Comptroller's Comment – As noted on page 8 of the report, officials stated to us that the tablet program is a relationship between the Provider and the Individual that is conducted at DOCCS facilities, and DOCCS is not responsible for the tablets and kiosks. DOCCS' day-to-day administration of the tablet program at the facility level is only to ensure compliance with DOCCS Directives – not the relationship between the Provider and Individuals.

OSC: Develop, implement, and adhere to an internal process to effectively monitor program participation and tablet inventory at both the facility and statewide levels.

DOCCS Response: Upon the issuance or declination of a tablet at Reception, the incarcerated individual completes the appropriate form, which is maintained in the incarcerated individual's file. Due to the vast amount of movement between and within facilities, the inventory records that OSC is recommending DOCCS maintain would be immediately outdated, any attempt to maintain such a count would not be feasible for the Department and would be a duplication of effort. At a moment's notice, the Department can determine who has been assigned a tablet and if they are actively using such tablet through our provider. The utilization of the tablets and kiosks are monitored by several staff, whether it be the housing unit Correction Officers who are watching the individuals using the kiosk and completing the daily safety sheets, the Correction Lieutenants monitoring the secure messages, investigators from OSI, CIU, or maintenance staff.

Additionally, the Department has the ability to verify when incarcerated individuals are accessing the kiosk, for how long and what transactions have occurred, along with detailed utilization records supplied by the Provider.

Lastly, the Department prohibits the sharing of passwords, however, like in the outside world, there is no practical way to proactively enforce such. When we find this is happening, we take a progressive approach that ranges from counseling to the issuance of a misbehavior report. Furthermore, while the tablets are not engraved or affixed with labels indicating who has been assigned a particular tablet, each tablet is assigned within the software installed on the tablet and, when powered on, it displays the incarcerated individuals name and DIN, which allows staff to enforce our policy of not sharing tablets.

State Comptroller's Comment – As noted on page 10 of the report, DOCCS does not internally monitor the number of active tablets at its facilities or the population of Individuals who have opted in/out of the tablet program. Further, the Provider was unable to provide DOCCS with the number of tablets used by specialty populations at each facility as they are considered community-based tablets that have no true ownership. Without knowing how many tablets have been assigned and to whom, DOCCS is unable to enforce the policies and procedures outlined in its Directives.

OSC: Implement a process to ensure that Individuals' correspondence with community members via secure messaging complies with Department Directive.

DOCCS Response: As noted above, OSC inappropriately took sections of Directive #4422, "Incarcerated Individual Correspondence Program" and applied them to Directive #4425, "Incarcerated Individual Tablet Program" as this directive references the need to be in compliance with all applicable provisions as outlined in Directive #4222, regarding mail, contraband, and incarcerated individual communication. After review of the section of Directive #4422 as referenced in the report, the Department asserts it was not our intent to make all sections listed applicable as referenced in Directive #4425. Furthermore, the section of Directive #4422 that is cited in the report deals only with outgoing correspondence from an incarcerated individual, not from members of the community, thus it would be inappropriate to place such requirements on community members who are corresponding via secure message. Equally important, an incarcerated

individual cannot send a secure message to any community member and may only correspond to community members who initiate contact with them.

DOCCS has the ability to identify IP addresses through investigation when necessary. Additionally, there is a process to protect incarcerated individuals who do not wish to receive secure messages. The system allows the incarcerated individual to delete messages on the kiosk without opening or downloading them and also allows the incarcerated individual to remove any community member from their contact list. Once removed, the community member cannot message the incarcerated individual.

With regards to the correspondence with community members, as previously stated above, community members must initiate contact with the incarcerated individual in order for the incarcerated individual to correspond with the community member. If the community member does not initiate contact, the incarcerated individual cannot correspond with anyone they so choose. Lastly, the verification standard recommended by OSC is not realistic and could be circumvented by community members by having other individuals registering and then sharing access. The Department has put many safeguards in place to ensure the safety and security of our institutions, staff, the incarcerated population and the public.

DOCCS has maintained adequate controls over the review and screening of secure messages based on the input of correctional professionals and as outlined in Department Directive #4425 . DOCCS will continue to explore ways to enhance screening processes to mitigate any risk to staff, incarcerated individuals and the public.

State Comptroller's Comment – Directive #4425 states that Individuals and community members using secure messaging must adhere to all applicable provisions as outlined in Directive #4422 regarding mail, contraband, and Individual communication. Further, we met with DOCCS officials several times on this issue, and they never voiced their concerns regarding the Directives we were using as criteria in this area. Moreover, if DOCCS' intent was to exclude certain sections of Directive #4422 within Directive #4425, it should have specifically done so. Poorly written policies and procedures create compliance risk.

OSC: Ensure that systems are maintained at vendor-supported levels. Until then, the Department should work with the Office of Information Technology Services to submit the required exception request form.

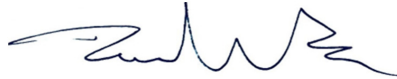
DOCCS Response: DOCCS does not believe that NYS-P13-001 is applicable to the Incarcerated Tablet Program as it operates on a Provider installed secure network and does not operate or interact with the DOCCS network, thus having no impact on DOCCS technical resources. Due to this configuration, DOCCS believes that a risk to the operation of the Department's facilities is properly mitigated. However, in an abundance of caution, DOCCS is currently working with the Provider to complete the appropriate Exception Request Form for submission to ITS in order to document the situation for the ITS Information Security Office.

OSC: Implement the remaining technical recommendations detailed in the preliminary report.

DOCCS Response: We appreciate OSC confirming that the tablets cannot connect to any wireless network other than the one that was installed by the Provider for this purpose. This confirms that the assessment conducted by ITS and the Provider prior to implementation was accurate when it specifically concluded that both the static content and the law library tablets could only connect to a signal originating from the Provider's wireless access points and that no other device can connect to those wireless access points. We will continue to implement additional protections to ensure the safety of staff, incarcerated individuals, and the overall institution.

The Department appreciates the opportunity to review and respond to the draft findings for report, 2022-S-8, "Controls Over Tablet and Kiosk Usage by Incarcerated Individuals."

Sincerely,



Daniel F. Martuscello III
Executive Deputy Commissioner

Contributors to Report

Executive Team

Andrea C. Miller - *Executive Deputy Comptroller*

Tina Kim - *Deputy Comptroller*

Stephen Lynch - *Assistant Comptroller*

Audit Team

Nadine Morrell, CIA, CISM - *Audit Director*

Bob Mainello, CPA - *Audit Manager*

Holly Thornton, CFE, CISA - *Audit Supervisor*

Amy Tedesco - *Examiner-in-Charge*

Karen Corbin - *Senior Examiner*

Inza Kone - *Senior Examiner*

Justin Dasenbrock, CISA, ITIL - *IT Audit Supervisor*

Christopher Bott - *IT Examiner-in-Charge*

Nicole Cappiello - *Senior IT Examiner*

Jonathan Julca - *Senior IT Examiner*

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



Like us on Facebook at facebook.com/nyscomptroller

Follow us on Twitter @nyscomptroller

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