Thomas P. DiNapoli
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

September 26, 2012

Ms. Gladys Carrión, Esq.
Commissioner
Office of Children and Family Services
52 Washington Street
Rensselaer, NY 12144

Re: Report 2012-F-24

Dear Ms. Carrión:

According 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 followed up on the actions taken by officials of the Office of Children and Family Services (Office) to implement the recommendations contained in our audit report, *Mobile Devices with Sensitive Information are not Secure* (Report 2010-S-19).

Background, Scope and Objective

The Office provides a system of family support, juvenile justice, child care, and child welfare services that promotes the safety and well being of children and adults. The Office funds and supervises 59 Local Districts that provide these services.

Local District staff use a variety of mobile devices to help complete their job duties, whether in or away from the office. These allow staff to record confidential information such as casework information and progress notes, and store pictures related to investigations, files related to court petitions, and medical requests. In addition, staff can use these devices to access the Office's child welfare application, CONNECTIONS, as well as other Office network resources.

According the Social Services Law, information relating to public assistance and care, children, and children's protective services held by public agencies is deemed to be confidential and protected by law. Further, the Office has regulations which specifically set forth procedures for safeguarding this confidential information maintained by the Office, Local Districts and other authorized agencies.

In 2007, the New York State Office of Cyber Security established encryption standards for protecting State data stored on laptops. State agencies were required to implement these Standards by December 31, 2008. Further, the Office of Cyber Security's Cyber Security Policy (Security Policy) states that agencies should take steps to adequately secure data whenever

laptop computers are used. The Security Policy applies to State entities, staff and all users who have access to or manage State information, including outsourced third parties.

Our initial audit, which was issued on August 22, 2011, examined whether security controls over mobile devices protect sensitive child welfare data from unauthorized access. The objective of our follow up was to assess the extent of implementation as of September 10, 2012, of the six recommendations included in our initial report.

Summary Conclusions and Status of Audit Recommendations

We found that officials have made significant progress in improving controls over mobile devices. Of the six prior audit recommendations to the Office and the Local Districts, five were implemented and one is no longer applicable. They have also taken additional steps to ensure that mobile devices are properly managed and secured, both at the Office and at the Local Districts.

Follow-up Observations

Office Recommendation 1

Regularly communicate with and train staff at Local Districts on securing mobile devices used for child welfare activities.

Status - Implemented

Agency Action - The Office has done a significant amount of work to ensure that information regarding the security of mobile devices, and the training for how to secure such devices, is communicated to the staff at Local Districts.

As a result of the previous audit, the Office conducted training sessions with Local Districts that stated they had not received any guidance from the Office regarding the security over mobile devices. They also instituted initiative 11-OCFS-ADM-08 which addressed Local District responsibilities and requirements related to the maintenance, custody, inventory and security of Office-issued equipment, and safeguarding personal, private, and sensitive information. The Office indicated to all Local District Commissioners that compliance with this initiative is mandatory and sent follow-up memos to Commissioners who had not sent inventory levels to the Office to ensure full Local District participation.

The Office has also been regularly communicating training and educational information regarding the use and security of mobile devices to Local District staff. For example:

- resources are accessible on their intranet page, for all Local District staff, regarding information security and the use of mobile devices,
- information related to security is presented in Monthly Awareness Messages and CONNECTIONS weekly messages,

- security training materials are currently being presented to Office staff, with Fall 2012 as a target to provide this information to Local Districts, and
- multiple memorandums have been distributed to Local District Commissioners prohibiting the use of QuickPads and AlpaSmart devices in the field as they do not support encryption. Additionally, memos have been distributed regarding the use of agency maintained databases.

Office Recommendation 2

Develop a mobile device security policy to be followed by all staff (Office, Local District, and others) that have access to or manage child welfare information.

Status - Implemented

Agency Action - The Office is in the process of finalizing a formal Administrative Directive on Portable Device Security. The expected approval date for this policy is Fall 2012. Once approved, the policy will be distributed to all users of portable devices. The purpose of the policy is to provide information about required technical, administrative, and physical measures to protect the security of portable devices issued by the Office, and requirements when users remotely access Office applications from a non-State owned or personally owned device.

Office Recommendation 3

Ensure all mobile devices provided by the Office are encrypted. Develop procedures for ensuring mobile devices purchased by Local Districts are encrypted.

Status - Implemented

Agency Action - All equipment purchase requests, including those using Local District funds, must go through the Office's review and approval process. The Office prohibits the purchasing of equipment that does not support encryption capabilities, unless there is a business need and compensating controls have been approved (specifically physical security controls). The Office has been working with the Local Districts to recover all QuickPads, which do not have encryption capabilities. To date, all but ten devices have been recovered or certified as securely disposed. All newly-purchased IT equipment, with a few minor exceptions, must be shipped directly to the Office, where it is logged into the inventory database and, where applicable, configured with encryption software.

Based upon encryption reports provided by the Office, we found 99 percent of the laptops were encrypted. Office Information Security staff are following up with the Local Districts on the remaining unencrypted laptops.

Office Recommendation 4

Amend current regulations relating to safeguarding of confidential information to address the use of computer systems to store such information and direct Local Districts to adopt appropriate security measures to protect such information.

Status - No Longer Applicable

Agency Action - The Office has taken numerous remediation steps to safeguard confidential information, including establishing and implementing various policies and administrative directives, as noted previously. Therefore, the amendment of regulations is no longer necessary.

Local Districts Recommendation 1

Keep an accurate inventory of mobile devices used for child welfare activities.

Status - Implemented

Agency Action - Office staff maintain an inventory database to record all IT equipment, including mobile devices used at the Local Districts. Office Asset Management staff have been working with the Local Districts since our initial audit to reconcile the number of mobile devices they are aware of to the number of mobile devices listed in the inventory database. The Office plans to conduct this reconciliation process annually once the initial reconciliation is complete.

Local Districts Recommendation 2

Encrypt or otherwise properly secure all mobile devices.

Status - Implemented

Agency Action - Since our initial audit, Office Information Security staff have been working to reconcile Office inventory reports with the State Office of Information Technology Services' encryption reports. This reconciliation has been occurring at least monthly, and more frequently as needed. As of August 2012, 99 percent of all Local District laptops active on the Human Services Network were encrypted. Where unencrypted laptops are still outstanding, the Office has contacted the relevant Local Districts to resolve the issue.

In addition, the Office now prohibits the purchasing of equipment that does not support encryption capabilities, unless there is a business need and compensating controls have been approved. All IT equipment purchases, including those using Local District funds, must go through the Office's review and approval process. This equipment, with a few minor exceptions, must be shipped directly to the Office, where it is configured with the base Office image, which includes encryption software.

Major contributors to this report were Nadine Morrell, Jennifer VanTassel, and Jared Hoffman.

We thank Office of Children and Family Services management and staff for the courtesies and cooperation extended to our auditors during this follow-up review.

Yours truly,

Brian Reilly
Audit Manager

cc: Thomas Lukacs, Division of the Budget
Kevin Mahar, Office of Children and Family Services