December 29, 2020

Ms. Sheila J. Poole
Commissioner
Office of Children and Family Services
52 Washington Street
Rensselaer, NY 12144

<div align="right">

Re: Access Controls Over Selected
Critical Systems
Report 2020-F-11

</div>

Dear Commissioner Poole:

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 have followed up on the actions taken by officials of the Office of Children and Family Services to implement the recommendations contained in our audit report *Access Controls Over Selected Critical Systems* (Report 2017-S-56).

Background, Scope, and Objective

The Office of Children and Family Services (OCFS) is charged with promoting the safety, permanency, and well-being of children, youth, families, and vulnerable populations in New York State. Its responsibilities encompass a wide range of social services programs, including: foster care and adoption; child and vulnerable adult protective services; preventive services for children and families; and juvenile justice. OCFS owns approximately 60 computer systems, which are used by the various divisions within OCFS to support its activities, including internal administration and program administration. Certain OCFS systems are also used by external entities, such as local departments of social services, voluntary agencies, and other third-party organizations that provide services on behalf of OCFS. OCFS' system infrastructure is maintained by the Office of Information Technology Services.

As these systems contain a broad range of sensitive information that is considered confidential for a variety of social services programs, controls over access to these systems are especially important. To ensure that only authorized users are allowed to access information stored on systems, agencies, such as OCFS, must follow New York State Information Technology (NYS IT) security policies and standards related to security and account management and access controls. Pursuant to NYS IT security policy and standards, among other provisions, agencies are required to:

• Perform annual reviews of user accounts to ensure only appropriate individuals have access;

• Maintain an inventory of all assets at a level that enables tracking and reporting;

- Assign an employee or group to be responsible for account management for each system, and document and maintain a list of authorized users in these roles; and

- Classify systems data based on confidentiality, integrity, and availability characteristics.

Our initial audit report, issued on March 21, 2019, determined whether access controls over selected OCFS systems were sufficient to prevent unauthorized or inappropriate access to those systems. Our audit covered the period August 1, 2016 through December 10, 2018. We found that access controls over six OCFS systems containing confidential information were insufficient to prevent unnecessary or inappropriate access to those systems. Specifically, we identified user accounts with inappropriate access to OCFS systems because OCFS hadn't performed required annual user reviews. We also found OCFS did not keep accurate records of those individuals authorized to approve or manage access to its systems, maintain accurate inventory of systems, or classify the data on those systems, as required by NYS IT policy and standards. Further, the audit team encountered significant delays during the audit due to lack of cooperation and timely access to information necessary to complete our work, which limited the amount of testing we were able to perform.

The objective of our follow-up was to assess the extent of implementation, as of November 3, 2020, of the two recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

We found that OCFS implemented one recommendation and did not implement the other recommendation from our initial audit.

Follow-Up Observations

Recommendation 1

Develop a program to ensure controls over user access to OCFS systems meet the applicable NYS IT requirements, including:

- *Maintaining and regularly reviewing user lists for each application;*

- *Developing and maintaining an up-to-date list of administrators for each application;*

- *Developing and maintaining an up-to-date inventory of systems; and*

- *Formally classifying all information assets.*

Status – Implemented

Agency Action – OCFS officials have developed a program to ensure controls over user access to OCFS systems meet the applicable NYS IT requirements. In January 2020, OCFS issued an Account and Access Management Policy that established the rules and processes for the oversight of user accounts and access to OCFS applications and resources, and mandates compliance with applicable State policies and standards regarding the management of user access. In addition, OCFS developed an inventory of its systems that tracks key information related to the oversight of user access. For example, for each system, the inventory captures user review dates. However, according to the inventory records for a sample of 15 systems, none of the 15 were reviewed annually as required by OCFS' Account and Access Management Policy. The time

between user reviews for the 15 systems averaged 581 days. In addition, 13 of the 15 user reviews were completed after OCFS had received the engagement letter notifying them of this follow-up review. We encourage OCFS officials to monitor the information they are capturing in their system inventory to ensure user reviews are completed within the time frames specified in their policy. The inventory also captures information on system administrators, allowing OCFS to maintain and monitor administrator names and the dates the administrator information was reviewed in a central location. Finally, OCFS conducted formal data classifications for each of its systems and recorded the dates of the classifications in the system inventory.

Recommendation 2

Improve the timeliness of cooperation with authorized State oversight inquiries to ensure transparent and accountable agency operations.

Status – Not Implemented

Agency Action – OCFS has not improved the timeliness of its cooperation, but instead continued a pattern of responding slowly to auditor requests and providing incomplete information during our review. For example, it initially took OCFS officials over a month to provide system inventory information that was repeatedly requested by auditors. When OCFS officials finally provided the information in response to those requests, they provided only a partial inventory of systems that had many relevant fields redacted. It took an additional 83 days and at least five more requests from auditors for OCFS officials to make the remaining system inventory information available. Further, OCFS would only make the additional information available via in-person review with OCFS officials present. Claiming confidentiality issues, OCFS officials refused to share the actual documentation despite having a signed confidentiality agreement in place with the Office of the State Comptroller. While this arrangement ultimately provided some assurance for auditors to draw their conclusions, it was an unnecessarily burdensome way to conduct the testing. We continue to encourage OCFS to improve its timeliness of cooperation with authorized State oversight inquiries.

Major contributors to this report were Nadine Morrell, Brian Krawiecki, Christopher Bott, Philip Boyd, and Nicole Cappiello.

We would appreciate your response to this report within 30 days, indicating any actions planned to address the unresolved issues discussed in this report. We thank the management and staff of the Office of Children and Family Services for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Brian Reilly, CFE
Audit Director

cc: Brendan Schaefer, OCFS