

Office of Children and Family Services

Access Controls Over Selected Critical Systems

Report 2017-S-56 | March 2019

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

Division of State Government Accountability



Audit Highlights

Objective

To determine whether access controls over selected Office of Children and Family Services (OCFS) systems are sufficient to prevent unauthorized or inappropriate access to those systems. The audit covers the period August 1, 2016 through December 10, 2018.

About the Program

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; and juvenile justice. OCFS owns approximately 60 computer systems, which are used to support its activities. OCFS' system infrastructure is maintained by the Office of Information Technology Services. OCFS' systems contain a broad range of sensitive information that is considered confidential but is necessary to support the programs and services that OCFS provides to vulnerable populations. To ensure that only authorized users are allowed to access this information, agencies, such as OCFS, must follow New York State Information Technology (NYS IT) security policy and standards related to security and account management and access controls.

Key Findings

- Access controls over six OCFS systems containing confidential information were insufficient to prevent unnecessary or inappropriate access to those systems.
- We identified 367 user accounts with access to six OCFS systems that were inappropriate because OCFS had not performed the required annual reviews of user accounts. This included 35 active user accounts on four systems containing confidential information for individuals who no longer worked for OCFS.
- OCFS did not keep accurate records of those individuals authorized to approve or manage access to its systems, maintain an accurate inventory of systems, or classify the data on those systems, as required by NYS IT policy and standards.
- We encountered significant delays during our audit due to a lack of cooperation and timely access to information necessary to complete our work. As a result, our work in certain areas was limited.

Key Recommendations

- 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.
 - 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

March 21, 2019

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

Dear Commissioner Poole:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage government resources efficiently and effectively and, by doing so, providing accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit entitled *Access Controls Over Selected Critical Systems*. 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.

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** **7**
 - Inappropriate or Unnecessary Account Access **8**
 - Account Administrator Discrepancies **11**
 - Inaccurate System Inventory **12**
 - Data Classification Non-Compliance **13**
 - Lack of Cooperation **13**
 - Recommendations **14**
- Audit Scope, Objective, and Methodology** **15**
- Statutory Requirements** **16**
 - Authority **16**
 - Reporting Requirements **16**
- Agency Comments and State Comptroller’s Comments** **18**
- Contributors to Report** **27**

Glossary of Terms

Abbreviation	Description	Identifier
ISO	Information Security Officer	<i>Key Term</i>
NYS IT	New York State Information Technology	<i>Policy/Standard</i>
ITS	Office of Information Technology Services	<i>Agency</i>
OCFS	Office of Children and Family Services	<i>Auditee</i>

Background

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 (ITS).

As these systems contain a broad range of sensitive information that are considered confidential for a variety of social services programs, including foster care and adoption, child and vulnerable adult protective services, and juvenile justice, 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;
- For each system, assign an employee or group to be responsible for account management, and document and maintain a list of authorized users in these roles; and
- Classify systems data based on confidentiality, integrity, and availability characteristics.

Audit Findings and Recommendations

We determined access controls over six OCFS systems were insufficient to prevent unnecessary or inappropriate access to those systems. Each of these six systems contained confidential information. OCFS has not implemented centralized policies and procedures to govern access to its systems. Rather, each division within OCFS has its own procedures for managing access to the systems they use. Furthermore, during our audit period, OCFS did not have an information security officer (ISO) or similar official who was responsible for centrally monitoring the patchwork of procedures relating to user access controls and ensuring compliance with NYS IT policies and standards. Lacking centralized access policies and procedures, OCFS cannot be confident that its systems – and the data within – are protected against unauthorized or inappropriate access. As a result of our review, we found:

- OCFS had not performed the required annual reviews of user accounts, and consequently failed to identify 367 user accounts with unnecessary or otherwise inappropriate access to six OCFS systems. This included 35 active user accounts on four systems for individuals who no longer worked (i.e., through transfer, retirement, or resignation) for OCFS.
- OCFS did not maintain an accurate listing of authorized users in the key roles involved with account management and access control. Of 44 individuals listed as administrators by OCFS, 33 (75 percent) did not have a user account (administrative or otherwise) for the systems they were designated to administer.
- OCFS could not provide auditors with a clear and accurate inventory of its systems and had to consult with ITS to assemble it.
- OCFS did not complete the required data classifications until well after our audit was underway.

Notably – and as discussed in greater detail in the following sections – for each of the above aspects of our audit, OCFS officials imposed significant delays in providing requested materials and/or restricted auditors' access, which suggests either a lack of complete and organized materials readily on hand or an intention to withhold certain information essential to our audit. Additionally, if the information was intentionally withheld from the auditors, this compromises OCFS' transparency and accountability. As a result of the delays and restrictions, our work in certain areas was limited.

In response to the engagement of our audit, OCFS took actions to address user access controls, such as performing formal data classifications and reviewing user account access. OCFS also filled its ISO position. These efforts notwithstanding, OCFS needs to further implement controls to reduce the likelihood of unauthorized or inappropriate access.

Inappropriate or Unnecessary Account Access

According to NYS IT standards, agencies must review the appropriateness of user account access to their systems at least annually, and take immediate steps to remove those individuals whose circumstances change and who no longer need access. We found that, generally, OCFS did not perform annual reviews of user access to its systems as required, but began this activity after the commencement of our audit. In its review of four systems, OCFS identified 70 user accounts that were inappropriate or unnecessary and should be removed. Our testing of user accounts for a sample of seven systems, including the four reviewed by OCFS, identified an additional 367 user accounts on six systems that should be considered for removal. This includes 51 additional user accounts not identified by OCFS for three of the four systems it reviewed and 316 accounts on the remaining three systems in our sample.

The user accounts we identified as unnecessary or inappropriate included those that: had never been used to log on to a system, had not been used to log on to a system recently (nine or more months for the purposes of our audit), or were associated with individuals who no longer worked for OCFS. For example, as of September 2018:

- 228 of the 367 user accounts we identified had not been used to log on to certain OCFS systems since prior to January 2018 (nine or more months). One account had not been used to log on to the designated OCFS system since January 2008 – more than ten years at the time of our testing in September 2018.
- Another 104 user accounts were never used to log on to the associated OCFS systems at all. More than half of these user accounts (59 of the 104) were for a system that is used to record sensitive data. We maintain that user accounts that have never been used or that have not been used for a long period are unnecessary, and should be removed in accordance with NYS IT standards.

We also compared user accounts for OCFS employees for our sample of seven systems with OSC payroll information. We identified 35 individuals, across four systems containing confidential information, who continued to have active user accounts after their separation (i.e., transfer, retirement, or resignation) from OCFS employment. This includes three individuals who separated from OCFS in 2013, but still had active accounts at the time of our review in September 2018 – over five years later.

When we provided OCFS officials with details of the 367 user accounts

we identified during our testing, they disagreed that the accounts should be considered for removal but did not provide evidence to support their position. Table 1 provides a summary of user accounts with inappropriate or unnecessary access for the seven systems we reviewed.

Table 1 – Summary of User Accounts With Inappropriate or Unnecessary Access

System	Number of User Accounts			
	Identified by OSC	Assigned to Individuals Who Had Separated	Never Used to Log On to Systems	Not Recently Used to Log On to Systems
A	256	11	59	186
B	40	0	22	18
C*	0	0	–	–
D	20	0	9	11
E*	22	1	12	9
F*	7	1	2	4
G*	22	22	–	–
Totals	367	35	104	228

Note: “–” indicates the audit team was unable to conclude or conduct testing based on the data provided.

*System reviewed by OCFS.

OCFS officials noted that, during our audit period, the agency’s ISO position was vacant and there was no one responsible for ensuring the agency complied with applicable NYS IT standards regarding user access reviews. As a result, the reviews had not been performed, and unnecessary or inappropriate accounts were left active, creating a risk for unauthorized access to OCFS systems containing confidential information. OCFS has since filled its ISO position.

We encountered significant delays in performing our work related to user access. To better understand and assess the controls over each application, we requested meetings with the relevant program officials in the divisions responsible for each system in our review. Between January 2018 and August 2018, we made 20 requests for these meetings. However, OCFS repeatedly failed to schedule the meetings in a timely manner. With the exception of a meeting in May 2018 and a follow-up meeting in June 2018 covering two systems, we were not permitted to meet with program personnel for the remaining systems until July, August, or September 2018. We found that, during the period we were delayed, each of the applicable divisions had

started reviews of user access to their respective systems. We are left to conclude that OCFS purposefully refused to schedule the meetings to allow the divisions time to start user access reviews, which they had not performed prior to the commencement of our audit.

Our testing of user accounts was also limited to the scenarios outlined in Table 1. Although we sought to perform additional testing, information necessary to conduct further testing was either unavailable or restricted from the audit team by OCFS. For example, OCFS officials cited user IDs as confidential and declined to provide them, despite our written confidentiality agreement with OCFS outlining how information would be shared and protected. While we were able to conduct certain high-level tests described previously, user IDs are a key field in following up and determining, with certainty, which users had unnecessary or inappropriate access to OCFS systems.

Additionally, key records were unavailable, which prevented the audit team from performing certain tests. For example, we were unable to analyze when user accounts were last used to access these systems. Further, in some cases, user accounts that were identified as no longer active or had roles deleted from the accounts were not included in the data provided and were therefore unavailable for testing.

We also encountered protracted time frames for OCFS to coordinate our information requests related to user data. Although OCFS is the system data owner, under its current structure, OCFS must coordinate with ITS, which maintained the OCFS systems in our sample population. Consequently, OCFS referred us to ITS for technical questions and requests for information such as user lists or administrative logs showing changes to user accounts for certain systems. We made initial requests for user data for certain systems in June 2018 and ultimately received the information in August 2018 – two months after it was requested.

In light of the delays imposed on our audit, we limited our testing to what we could accomplish using the available information and within the allotted time frames for the seven systems. However, given the results of our limited testing and the lack of centralized oversight of user account access, we conclude the results could be representative of similar issues on other systems housing sensitive OCFS program information.

Account Administrator Discrepancies

According to NYS IT policy and standards, all systems must have an individual employee or group assigned to be responsible for account management, and a listing of authorized users in these roles must be documented and maintained. We found that OCFS did not maintain a complete and accurate listing of authorized users in the key roles involved with account management and access control. We compared a list of administrators provided by OCFS with system user data for seven systems, and determined that 33 of 44 (75 percent) individuals listed as administrators by OCFS did not have any type of user account (administrative or otherwise) for the systems they were designated to administer (see Table 2).

We also compared individuals who were identified as administrators in the system user data for five of the seven systems with the list of administrators provided by OCFS, and found 22 individuals with administrator accounts who were not on OCFS' list of administrators (see Table 2). We could not test user accounts for the remaining two systems because the user data provided did not identify whether an individual was an administrator. However, our limited testing demonstrates OCFS did not keep sufficient lists of those individuals charged with managing access to its systems.

Table 2 – Account Administrator Discrepancies Identified by OSC

System	Administrators on OCFS List	Administrators on OCFS List Without a User Account	Additional Administrators in User Data But Not on OCFS List
A	13	9	N/A
B	10	10	2
C	2	0	6
D	11	9	N/A
E	1	1	5
F	5	4	5
G	2	0	4
Totals	44	33	22

Note: N/A indicates the user data for this system did not identify administrative accounts, so this particular test could not be completed.

NYS IT policy also states that users of privileged (administrator) accounts must use a separate, non-privileged (regular) account when performing normal business transactions. We reviewed the user data for five systems, and identified a total of 14 administrators assigned to four different systems who did not have two separate accounts as required.

As with user account access, we again encountered significant delays as we sought to obtain the data necessary to accomplish our testing related to account administration. Between January 2018 and August 2018, we made 15 requests for a complete list of system administrators designated by OCFS. The list that was finally provided and used in our testing ultimately proved to contain the discrepancies noted in this section because OCFS officials did not ensure NYS IT policies are followed. OCFS officials agreed they did not maintain an accurate list of authorized users involved with account management and access control processes, citing the lack of an ISO, who would have been responsible for such tasks. Additionally, they indicated that the newly hired ISO is now in the process of working with ITS officials to create such a listing.

Inaccurate System Inventory

NYS IT policy states agencies must maintain an inventory of all assets at a level that enables tracking and reporting. We determined that OCFS did not maintain a clear and accurate inventory of its systems as required. Instead, OCFS relied on ITS to maintain a listing of its systems. We initially requested a list of systems from OCFS in July 2017. OCFS consulted with ITS to assemble the list, which was ultimately provided in January 2018. The delay of more than five months suggested OCFS did not have an inventory of its systems readily available.

Additionally, we question the accuracy of the inventory provided during the audit. In response to questions about three systems in our sample, OCFS repeatedly provided conflicting information, indicating a lack of familiarity with them. For example, in one instance, we inquired about a system in our sample that, among other things, houses confidential information for children. Between January 2018 and December 2018, OCFS provided us with no fewer than seven different explanations regarding basic characteristics of the system. In this case, rather than clarifying prior information about the system in question, each subsequent explanation only served to further confuse the issue. In the case of other systems, OCFS officials cited the timing of our questions as a reason for their conflicting explanations or claimed the explanations they provided were accurate.

OCFS officials insisted the conflicting answers were not meant to mislead auditors. Their claim notwithstanding, these examples highlight the importance of maintaining an accurate inventory, without which OCFS may be unaware of the status of certain systems. If OCFS cannot readily identify and determine the status of the systems it uses, there is a risk that it has not implemented the necessary access controls for those systems.

Data Classification Non-Compliance

Information must be classified on an ongoing basis, based on its confidentiality, integrity, and availability characteristics according to the NYS IT policy. We found that OCFS completed the required data classifications, but not until well after our audit was underway and after our repeated requests for documentation supporting the classifications. We made 20 requests for documentation to support data classifications performed for the 16 systems in our sample between July 2017 and June 2018, and ultimately issued written preliminary findings in June 2018 reporting that the classifications had not been completed. OCFS eventually conducted classifications for 14 of the 16 systems late in June 2018, following the issuance of our preliminary report – and nearly a year after our audit was engaged and we began requesting supporting documentation. We appreciate that OCFS officials took action to comply with NYS IT policy as a result of our audit. However, if OCFS does not review and classify the data on its systems on an ongoing basis as required, it will be unable to ensure that controls, including those over access, are appropriate and commensurate with the data’s classification.

Lack of Cooperation

OCFS has a responsibility to the public to provide access to information and to ensure access to its systems is monitored according to applicable standards. As discussed throughout this report, however, OCFS officials hindered auditors’ progress, not only by delaying access to pertinent individuals and information but also by presenting us with contradictory information, which ultimately caused us to limit our audit work and, therefore, our conclusions.

It is important to note that this particular audit experience is not an isolated incident; rather, following similar OCFS responses to previous audits, it constitutes a pattern of poor cooperation by OCFS and a disregard for transparency and accountability. Our report entitled *Oversight of Residential Domestic Violence Programs (2017-S-16)* highlights instances where OCFS officials delayed and/or restricted information, which affected OSC auditors’ ability to draw conclusions. Transparency and accountability are two cornerstones of good government. Insufficient internal controls provide less assurance that objectives, such as controlling user account access to systems with sensitive data, are being accomplished efficiently and effectively.

Recommendations

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

Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether access controls over selected OCFS systems are sufficient to prevent unauthorized or inappropriate access to the systems. Our audit covered the period August 1, 2016 through December 10, 2018.

To accomplish our objective and assess relevant internal controls, we met with officials from OCFS and ITS and reviewed relevant OCFS and NYS IT policies and standards related to access controls. We selected a judgmental sample of 16 systems for review during our audit based on the system descriptions and the descriptions of confidential data contained therein. We met with officials from the divisions within OCFS responsible for the systems in our sample. We also judgmentally selected 7 of the 16 systems based on number of users (size), authentication method, and OCFS divisions that utilized each system, and analyzed user data to identify certain types of user accounts at risk for unauthorized or inappropriate access, such as accounts that were never used to log on to a system or that had not been used to log on recently (nine or more months for the purposes of our audit). We also compared the user data with OSC payroll information to identify user accounts associated with individuals who no longer worked for OCFS. Administrator accounts were identified in the user data for five of the seven systems, which we compared with an OCFS listing of administrators to determine the accuracy of the list.

Statutory Requirements

Authority

We conducted our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions, and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

This audit was performed pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article 11, Section 8 of the State Finance Law.

Reporting Requirements

We provided a draft copy of this report to OCFS officials for their review and formal written comment. We considered their comments in preparing this final report. We are disappointed in OCFS' failure to address the report's recommendations. Rather than consider the recommendations as an improvement opportunity in their oversight of very sensitive information, OCFS officials expressed nearly universal disagreement with the audit conclusions and recommendations. We urge OCFS to reconsider its position relating to the audit's findings and recommendations, and take needed steps to enhance their controls.

We also note that OCFS' response includes multiple misleading and/or inaccurate statements. Our responses to those comments are included as State Comptroller's Comments, which are embedded in OCFS' response.

Within 90 days of the final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the Office of Children and Family Services shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where the recommendations were not implemented, the reasons why.

Agency Comments and State Comptroller's Comments



Office of Children and Family Services

ANDREW M. CUOMO
Governor

SHEILA J. POOLE
Acting Commissioner

March 1, 2019

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

Re: *Audit 2017-S-56 Report: Access Controls Over Selected Critical Systems*

Dear Mr. Reilly:

This letter constitutes the Office of Children and Family Services' (OCFS) response to Draft Report 2017-S-56 summarizing the audit conducted by the Office of the State Comptroller (OSC) on Access Controls over Selected Critical Systems. The objective of this audit was to determine whether access controls over selected OCFS systems are sufficient to prevent unauthorized or inappropriate access to those systems. The audit covered the period August 1, 2016 through December 10, 2018.

Account Access

For the systems under audit, OSC concluded that OCFS must review annually all user accounts for systems containing critical or sensitive information and remove accounts for users who no longer require access. OSC also claims that OCFS prevented OSC from conducting additional testing as they were not provided the required information. OCFS has implemented a schedule to review user accounts of critical systems on an annual basis; however, OCFS takes exception to OSC's claims regarding OCFS' failure to provide information for additional testing since OCFS does not release confidential user IDs as recommended by New York State Information Technology Services (ITS).

State Comptroller's Comment 1 - We maintain our position that, had OCFS provided all the requested data – not only user IDs but other key records as well – we would have been able to perform additional testing. OCFS' withholding of information prevented the audit team from performing certain tests on some systems, such as analyzing when user accounts were last used to access systems. Further, as noted on page 10, we had a written confidentiality agreement with OCFS outlining how information would be shared and protected to ensure confidential information would be handled in an agreed-upon manner.

Annual Reviews

OSC Finding: OSC concluded that OCFS did not perform annual reviews of user accounts to its systems but began this activity after the commencement of our audit. As part of OSC's testing of user accounts for a sample of systems, OSC identified 367 user accounts on six systems that OSC considers inappropriate or unnecessary and should be considered for removal. OSC's asserts that certain accounts for OCFS employees who had not logged on for a 9-month period should be considered for removal.

OCFS Response: Although we agree with OSC's review of user accounts as part of this audit and agree that the user accounts for systems under review for this audit should be reviewed annually, we disagree with the conclusion that all 367 user accounts identified are inappropriate or unnecessary and should be considered for removal.

State Comptroller's Comment 2 - We disagree with OCFS' statement. We provided detailed information regarding the 367 users to OCFS on November 27, 2018. In fact, while OCFS officials disagreed with our findings, they acknowledged they needed additional time to review the 367 accounts. At the time this final report was prepared, OCFS still had not provided OSC with any documentation or explanations justifying why these user accounts are appropriate and necessary and should continue to have access. Therefore, all 367 user accounts should be considered for removal.

Further, OSC's claim of 9-month review of inactive account seems arbitrary as OSC does not provide a basis for a 9-month period of time, which is less than the recommended annual review by ITS. As such, OCFS has implemented a schedule to review annually user accounts on all OCFS systems to confirm the continued need for all user accounts.

State Comptroller's Comment 3 - The nine-month time frame was based on the length of time it took OCFS to provide the auditors with the information. However, agencies that set a time frame related to deactivating inactive accounts, which is commonly accepted as a best practice and required by federal standards, generally use a much shorter time frame. For instance, the Payment Card Industry Standard requirement is 90 days, which is also the standard used by many federal agencies.

OCFS' lack of understanding and recognition of the risks associated with inactive accounts is of concern. It is a well-established IT principle that accounts that are not used regularly are often the target of attack since it is less likely that any changes (such as a changed password) will be noticed. The more appropriate question that OCFS should be asking is why it allowed so many individuals access to this highly sensitive data for so long, especially when, based on usage, they did not need this access.

Additional Testing

OSC Finding: OSC states that although they sought to perform additional testing, information necessary to conduct further testing was either unavailable or restricted from

the audit team by OCFS. For example, OCFS officials cited user IDs as confidential and declined to provide them, despite our written confidentiality agreement with OCFS outlining how information would be shared and protected.

OCFS Response: During the audit, OCFS advised OSC that the decision to not release user IDs was based on New York State Office of Information Technology Services' (ITS) recommended practice, which advises against the release of user IDs because of the security risks associated with that practice. As the entity that provides statewide IT strategic direction, directs IT policy and delivers centralized IT products and services that support the mission of the State, OCFS appropriately relied on ITS' recommendations.

State Comptroller's Comment 4 - We maintain our position that, had OCFS provided all the requested data – not only user IDs but other key records as well – we would have been able to perform additional required testing. OCFS' withholding of information prevented the audit team from performing certain tests on some systems, such as analyzing when user accounts were last used to access systems. Further, as noted on page 10, we had a written confidentiality agreement with OCFS outlining how information would be protected to ensure confidential information would be handled in an agreed-upon manner. Also refer to Comment 1.

Account Administrator Discrepancies

Pursuant to NYS IT policy, all systems must have an employee or group assigned to be responsible for account management. For the systems under review, OCFS provided to OSC a list of OCFS and NYS ITS individuals who review and approve system access and complete the technical process of provisioning and deprovisioning accounts. OSC's audit findings fail to recognize this process and incorrectly assumes that OCFS employees who evaluate account access must also have system administrator accounts.

OSC Finding: OCFS did not maintain a complete and accurate listing of authorized users in the key roles involved with account management and access control.

OCFS Response: Although OCFS agrees with OSC's review of administrative accounts as part of this audit, OCFS disagrees with the assessment of whether or not the individuals listed as administrators performed their responsibilities because the individual identified did not have any type of user account for those systems.

As a general matter, account administration takes place both by OCFS and ITS. OCFS' processes for account management, including administrator accounts, are consistent with New York State Information Technology Policy NYS-P03-002 Information Security in that all OCFS applications have an individual person or unit responsible for the management and access control of each application. Additionally, the process of account management involves at least two components: the business review for whether an account request is appropriate and the technical administration of creating the account or granting access. For most applications under review, OCFS "administrators" review the request and determine whether access is appropriate. No system account is necessary for this determination. Separate and apart from the business analysis, ITS manages account creation with administrative accounts. As such, OSC's finding does not consider the practice by which

OCFS and ITS provision and deprovision accounts. Although OCFS expressed this distinction throughout the audit, OSC's findings do not take the above into account. Nonetheless, OCFS has created and filled the position of OCFS ISO whose duties include formalizing a process and scheduling periodic review of OCFS accounts with each system owner.

State Comptroller's Comment 5 - As noted in our report, the lists of administrators were not accurate, and many of those individuals listed as administrators did not have user accounts for the systems they were charged with administering. We provided detailed information regarding the administrative users to OCFS on November 27, 2018, and OCFS provided no documentation or explanations regarding these administrators' specific roles (business vs. technical). We based our conclusion on the information provided during the audit, and we were unable to distinguish the specific roles of the administrators and whether they were responsible for a business review or technical administration. As such, we acknowledge that individuals listed as administrators, but without a user account, may have only performed business reviews. We made changes to the report based upon this OCFS response.

This review of accounts process, including a review by the application owner or designee for account need, has been completed for the systems under review by OSC and will be completed for the remaining OCFS systems. These reviews include review of administrative accounts for OCFS personnel.

Inaccurate System Inventory

NYS ITS policy requires that agencies must maintain an inventory of assets. OSC requested a list of all OCFS systems, which was beyond the scope of this audit of "critical" systems.

State Comptroller's Comment 6 - We take exception to OCFS' assertion that our request for a list of all OCFS systems was beyond the scope of the audit. The objective of our audit, as noted on pages 1 and 15 of the report, was to determine whether access controls over selected OCFS systems are sufficient to prevent unauthorized or inappropriate access to those systems. In fact, OCFS requested a copy of our audit objective in writing in August 2017 after our opening conference, which OSC promptly provided. As is typical during the course of an audit, OSC requests data to assess controls related to our audit objective. To meet standards, OSC must understand the full population of systems in order to select systems to concentrate on. As such, it is not up to OCFS to determine what the scope of an OSC audit should be. Further, this action demonstrates OCFS' efforts to obstruct, limit, and influence our audit objective and process.

Contrary to OSC's report, at all times OCFS maintained various inventories of computer systems for the purpose of disaster recovery, budgeting, and operations.

State Comptroller's Comment 7 - We disagree. As OCFS itself notes, NYS IT policy requires that agencies must maintain an inventory of assets. OCFS could not

provide auditors with an inventory of its systems and instead relied on ITS to maintain this listing. Further, if OCFS had these inventories of systems for the purposes it describes, it should have provided them to OSC when requested rather than five months later.

OSC Finding: OSC determined that OCFS did not maintain an accurate inventory of its systems. OSC found that instead, OCFS relied on ITS to maintain a listing of its systems.

OCFS Response: During the initial stages of the audit, there was considerable ambiguity regarding OSC's request for a list of all "systems that process and/or store sensitive data" and how OSC defined "systems." OSC declined to provide a definition of "system" or "critical" for this audit. As a result, on or about January 18, 2018, OCFS and OSC met to discuss the scope of the audit and to discuss specific criteria to define the list of systems responsive to OSC's request. Based on those discussions, both parties agreed that OCFS would provide a list of systems supported by ITS. OCFS provided that list of systems and explicitly advised that the list was not a comprehensive list of OCFS systems for the above-mentioned reasons.

State Comptroller's Comment 8 - We believe our request for a list of "systems that store and/or process sensitive data," as part of an information technology audit, was sufficiently clear. OCFS' perplexity regarding systems and the need for a "definition" as it related to our requests can only be construed as further evidence of its obstructive intentions to influence and limit our audit scope.

Data Classification

NYS ITS policy requires that information must be classified based on the data's level of confidentiality, integrity, and availability. OSC incorrectly asserts in its report that OCFS had not classified its data. OCFS, through NYS ITS ISO, had classified its system data on an ongoing basis and NYS ITS provided said classifications for the systems under review.

OSC Finding: OSC found that OCFS completed the required data classifications, but not until well after our audit was underway and after repeated requests for documentation supporting the classifications. OCFS eventually conducted classifications for 14 of the 16 systems in late June 2018 following the issuance of our preliminary report.

OCFS Response: OCFS disagrees with this finding. The ITS Human Services Information Security Office representative submitted to OSC on April 9, 2018, on behalf of OCFS, a statement advising that for the OCFS systems under review, the data contained in said systems was classified as "federal medium."

OSC rejected that classification, citing NYS Information Technology Policy NYS-P03-002, on the basis that as the owner of the data OCFS is responsible for its data classification. OSC provided no further evidence to support its conclusions. OCFS submits that it complied with NYS-P03-002, and specifically the section of the policy entitled *ITS Information Classification IT standard*, through the classification performed by the ITS ISO Team and provided on April 9, 2018.

State Comptroller's Comment 9 - We disagree. OCFS, in its response, has omitted pertinent information regarding the data classification finding. We did not reject OCFS' classification based on NYS IT Policy NYS-P03-002, nor did we provide "no further evidence" to support our conclusion. Our preliminary report to OCFS officials clearly stated the criteria we used to evaluate OCFS' data classification, and this included ITS' Information Classification Standard (NYS-S14-002). This standard states that an information classification must include an identification of information assets; classification of information assets by confidentiality, integrity, and availability; and determination of controls based on the classification. Each of these principles must be individually rated as low, moderate, or high and the information owner must answer questions in the information classification worksheet to determine the classification of their information assets and resulting controls that should be implemented. However, as OCFS admits, officials only provided a statement from an ITS official that simply asserted the data contained in the systems was classified as "federal medium"; there was no evidence provided to support the conclusions of that assessment. Further, in response to our preliminary finding, OCFS admitted that "a classification of OCFS had not been completed in accordance with 'the letter' of NYS information technology standards per NYS-S14-002." Officials also stated that, when OSC rejected OCFS' data classification statement, it completed, in conformance with state information classification standards, the data classification of those systems in our audit.

More specifically, New York State *Information Technology Policy NYS-P03-002, Information Security* Section 4.1(a)(2) allows a state entity's (SE) information security function to "be fulfilled by the Enterprise Information Security Office (EISO) and Cluster Security Services Teams" for those "SEs that receive ITS services as a member of one of the clusters within ITS." Here, OCFS is a member of the ITS Human Services Cluster and, as such, the information security function has been fulfilled by the ITS Cluster Security Services Team who worked in conjunction with OCFS data owners, or representatives, to classify the data housed within OCFS's systems.

Additionally, prior to the commencement of this audit, OCFS had taken steps to create and fill the position of OCFS Information Security Officer, whose duties would include formally documenting the classification of OCFS data. As such, in response to OSC's decision to reject the statement provided by the ITS EISO classifying the data as federal rating of medium, once the agency's ISO was hired, OCFS began and completed a formal documentation of 14 of the 16 systems under review as part of this audit. For the remaining two systems selected by OSC, one system was never utilized and does not contain any stored data or content, and the other system is accessible to OCFS users only through another one of the systems for which the data classification was completed. Thus, OCFS made the decision that the content and controls of the system through which access is obtained is sufficiently documented.

Lack of Cooperation

Contrary to OSC's findings, OCFS cooperated with OSC's audit team and responded to OSC's requests throughout the duration of this audit. The computer systems under review are

supported by NYS ITS. OSC failed to consider that both the technical nature of the requests and reliance on another NYS agency would add significant time to the process of gathering information and responding to OSC's request. On multiple occasions, OCFS endeavored to provide additional information or clarification, which OSC wholly ignored.

State Comptroller's Comment 10 - We fervently disagree. As noted on page 9 of the report, OCFS did not cooperate with the audit team; rather, OCFS delayed meetings with program officials for six to eight months. These meetings needed no coordination with ITS. In fact, we made 20 requests for these meetings between January 2018 and August 2018. Finally, it is important to note that this particular audit experience is not isolated to just this audit. OCFS has delayed responses to previous audits, which fully supports a pattern of poor cooperation by OCFS and a disregard for transparency and accountability.

We also disagree that OSC "wholly ignored" any information made available during the audit. OSC reviewed and considered all the information that OCFS provided during the audit. Information that supported OCFS' position was recognized and information that was not adequate was not accepted.

OSC Finding: OCFS officials hindered auditors' progress, not only by delaying access to pertinent individuals and information but also by presenting us with contradictory information, which ultimately caused OSC to limit our audit work and, therefore, our conclusions.

OCFS Response: OCFS disagrees with this finding. The complexity of this audit, the dense nature of the information requested, and OCFS's reliance on ITS for assistance in gathering much of the information contributed to the time invested in an effort to provide OSC with complete and accurate information.

State Comptroller's Comment 11 - We disagree with OCFS' characterization of our audit as complex or dense in nature. This was designed as a routine audit of access controls over computer systems. However, OCFS officials challenged the audit's scope, delayed meetings with program officials, and delayed providing requested information, thereby making the audit far more difficult and complex.

In an effort to hasten the flow of information, OSC made a request on June 21, 2018 to OCFS and ITS "to have the ability to follow up directly with ITS personnel for items related to [OSC's] access control audit including meetings, data, table layouts, user lists, etc. [OSC] would still [copy] OCFS on the requests so they are aware of what [OSC is] asking for, but [expressed that] a more direct approach to follow up on information would be helpful." OCFS granted that request to reduce the number of requests that OCFS internal audit would be responsible for, eliminated the additional step of having OCFS send requests to ITS on behalf of OSC, reduce the risk for misunderstanding or miscommunication, and allowed OSC to receive information directly from the source providing it.

State Comptroller's Comment 12 - OCFS' response is a mischaracterization. Although we agree that OCFS eventually allowed us direct access to ITS, from the

beginning, OCFS continually obstructed the audit by requiring that all meeting and documentation requests go through OCFS Internal Audit. For example, as noted on page 9, it took OCFS eight months to schedule meetings with program officials. In addition, as noted on page 12, during that same eight-month period, OSC made 15 requests to OCFS for a complete list of system administrators before it was finally provided to us. It is OSC's policy to always request direct access to sources of necessary information, and this would include ITS officials. OCFS' protracted time frame for providing the requested information – which should otherwise have been readily available – causes us to question whether the information existed at the time of our request.

As previously stated, OCFS has repeatedly attempted to provide clarity in response to what OSC called "conflicting information." As we explained during the course of the audit, OSC conducted interviews with various OCFS and ITS staff regarding the identified systems and received answers from individuals that included various terms and description from individuals who answered OSC's questions from their individual perspective. When OCFS attempted to clarify the various terms and definitions, OSC insisted they had been provided conflicting information when, in fact, they had not.

OCFS Coordination with New York State Office of Information Technology Services

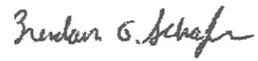
OSC Finding: The draft report indicates that OSC encountered protracted time frames for OCFS to coordinate information requests related to user data. Although OCFS is the system data owner, under the current NYS enterprise wide structure, OCFS must coordinate with ITS for such data. ITS maintains nearly all of the OCFS systems under review in this audit. Consequently, OCFS referred OSC to ITS for technical questions and requests for information such as user lists and logs showing changes to user accounts.

OCFS Response: As explained to OSC during the course of the audit, ITS provides statewide IT strategic direction, directs IT policy and delivers centralized IT products and services that support the mission of the State, including OCFS. As a result, OCFS referred OSC to ITS for technical questions and requests for information such as user lists. Furthermore, OCFS relied on ITS for certain technical information necessary to respond to OSC's inquiry. ITS supported OCFS throughout the audit. The complexity of the technical systems, lack of common terminology, and multi-party relationship resulted in delays in responding to OSC that were outside of OCFS's control.

State Comptroller's Comment 13 - Again, we strongly disagree with this characterization. As noted on page 9 of the report, OCFS delayed meetings with relevant program officials for six to eight months – these meetings needed no coordination with ITS. In fact, we made 20 requests for these meetings between January 2018 and August 2018. OCFS introduced continuous delays in the audit by requiring that all meeting and documentation requests go through OCFS Internal Audit. It is OSC's policy to always request direct access to sources of necessary information, and this would include ITS officials.

Should you have any questions or concerns, please contact Bonnie Hahn at Bonnie.Hahn@ocfs.ny.gov or by phone at (518) 402-3985.

Sincerely,



Brendan G. Schaefer, CPA
Audit Director
Office of Audit and Quality Control

Contributors to Report

Executive Team

Andrew A. SanFilippo - *Executive Deputy Comptroller*

Tina Kim - *Deputy Comptroller*

Ken Shulman - *Assistant Comptroller*

Audit Team

Brian Reilly, CFE, CGFM - *Audit Director*

Nadine Morrell, CIA, CISM - *Audit Manager*

Brian Krawiecki - *Audit Supervisor*

Holly Thornton, CISA, CFE - *Examiner-in-Charge*

Jared Hoffman, OSCP, GPEN, GWAPT - *Information Technology Specialist*

Christopher Bott - *Senior Examiner*

Mary McCoy - *Supervising 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



Like us on Facebook at facebook.com/nyscomptroller

Follow us on Twitter @[nyscomptroller](https://twitter.com/nyscomptroller)

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