Thomas P. DiNapoli
COMPTROLLER

OFFICE OF THE
NEW YORK STATE COMPTROLLER

DIVISION OF STATE
GOVERNMENT ACCOUNTABILITY

OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE

NATIONAL DIRECTORY OF NEW HIRES DATA SECURITY

Report 2008-S-49

AUDIT OBJECTIVE

Did the Office of Temporary and Disability Assistance (Office) meet Federal requirements for securing National Directory of New Hires (Directory) data?

AUDIT RESULTS - SUMMARY

We found the Office met a majority of the Federal Security Requirements. However, there are a few requirements that were only partially implemented or not implemented, putting the Directory data at risk. While only five people were authorized to have access to Directory data, we found an additional 138 individuals had access to the data. All of these employees had administrative access to the server where Directory data is stored, allowing them to access information such as social security numbers and other Directory data. Further, various state agency staff could access Directory data while it was stored.

We found the Office's Security Plan does not address certain important risks to the Directory data. Also, while the Plan documented the system that the Office planned to use to handle Directory data, however, the Plan does not accurately represent the current processes or systems in use for protecting the data.

Our report contains three recommendations to improve security over Directory data. Office officials agreed with our recommendations and have implemented the necessary technical steps to secure the Directory data. The Office should implement our recommendations to meet Federal Security requirements and minimize the risks of unauthorized access to Directory data.

This report, dated June 25, 2008, is available on our website at: http://www.osc.state.ny.us.
Add or update your mailing list address by contacting us at: (518) 474-3271 or
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

BACKGROUND

The Federal Office of Child Support Enforcement (Child Support Enforcement) operates the Directory database. The purpose of the Directory is to provide a national database of employment and unemployment insurance information. The Directory contains employment, unemployment insurance, and wage data from state and Federal agencies.

Certain state agencies can submit a list of names to Child Support Enforcement to see if there are matches with the Directory. When agencies want to do this, they must enter into a written Computer Matching Agreement (Agreement) with Child Support Enforcement. The Agreement includes security requirements for the administrative, physical and technical safeguarding of the Directory data once it is given to the agencies. Further, the Agreement requires agencies to comply with the February 2007 Security Requirements for Receiving Federal Parent Locator Service Data (Security Requirements).

Since May 2006, the Office has been requesting matches between its database of New York Adult Temporary Assistance for Needy Families benefit recipients and the Directory. The matches help the Office identify recipients with unreported employment and income when it is verifying their eligibility for benefits.

Once Child Support Enforcement matches the Office's list of names to the Directory, it returns the match results as a text file to the New York State Department of Taxation and Finance, which is the designated New York State agency with a secure connection. This text file contains personal information about recipients such as their social security numbers.

When the Office started getting matches from Child Support Enforcement, it created the following process:

- The Office for Technology receives the text file, stores it on a mainframe and backs up the information.
- The file is then retrieved by the Office, which puts the text file on a different mainframe before moving it to a folder on an Office server. This server is connected to the Human Services Enterprise Network (Network), managed by the Office for Technology.
- The text file is then loaded into a database table, but is also kept on the Office server.

At the request of Office officials, we performed an independent security assessment of how the Office handles and secures Directory data, as outlined in the Security Requirements. We reviewed the security of both the Directory text files and the database table containing the Directory data.

AUDIT FINDINGS AND RECOMMENDATIONS

Security Requirements

The Office's Agreement with Child Support Enforcement requires it to comply with 36 Security Requirements when receiving Directory data. This includes updating a System Security Plan (Plan), identifying risks associated with the data, ensuring only those with authorization have access to Directory data, and ensuring that data is secured during transmission. We found that the Office fully complied with 25 of the 36 requirements, partially complied with nine and did not comply with two (we believe the risk is low for one of the non-compliant requirements). Further, we determined that some of the requirements that the Office only partially complied with and the one requirement that the Office did not comply with resulted in the Office not having an updated Plan, not identifying all risks and not implementing certain necessary access controls to prevent unauthorized access.

The Security Requirements indicate that States should implement risk-management programs that define responsibilities and processes for all personnel, systems, networks, data, and facilities that handle any Federal Parent Locator Service Data, including Directory data. The Security Requirements also indicate that States should develop Plans which specifically define how systems and networks handle this data.

Child Support Enforcement strongly encourages States to use the National Institute of Standards and Technology (NIST) Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," when establishing their Plans. This publication indicates that Plans are living documents that require periodic review, modification, and milestones for implementing security controls. Further, the publication indicates that a Plan should describe the technical system it covers, along with any environmental or technical factors that raise special security concerns, including risks associated with stand alone or enterprise networks.

The Plan has not been updated to accurately represent the current processes the Office uses for Directory data. In particular, the Plan does not address potential security problems with data stored on a server and accessible to other agencies and various Office staff. As a result, the Plan's indication that the risk to Directory data is low may not be accurate. The Plan should have been updated to define the existing technical environment over Directory data, as required. However, we found it was not.

In addition, the Office has not done a comprehensive risk analysis and does not have a program to continuously identify and manage significant risks to the Directory data. Therefore, the Office has not addressed all security risks and has not implemented an adequate risk-management program related to the Directory data.

Office management stated that the updated Agreement did not require that they submit a revised Plan. We disagree with Office management because, as mentioned earlier, the NIST publication requires periodic review and modification. Moreover, in the absence of comprehensive risk analysis, at least 138 individuals (119 Office for Technology network administrators, 11 Office network staff, and 8 Office Finance employees) had access to Directory data when only 5 people needed to access this data.

To determine whether Directory data was secure, we examined how it was handled and who had access. We found that the database tables were secure. However, we found the following additional security risks to the Directory text files:

- Office for Technology staff can access files on the production mainframe.

- Staff at the Office, the New York State Department of Health, and the Office for Technology could access files on the development mainframe. During the course of our audit, we alerted Office officials to this finding and they changed the process so Directory data is transmitted directly from the production mainframe to an Office server, without going to the development mainframe.

- The server is not routinely or thoroughly checked for weaknesses. Therefore, the server could have weaknesses that allow someone to take control of it and gain access to its data. Present controls do not prevent a Network user from using such weaknesses to gain access to the Directory text files on the Office server.

To secure Directory data, the Office should update their Plan and implement a risk management program that meets Federal Security requirements. Further, the Office should implement the technical recommendations in our preliminary report which address the above findings. These recommendations are omitted from this report for confidentiality purposes.

Recommendations

1. Update the Plan using NIST Special Publication 800-18 as guidance.

2. Implement a risk management program, including defining responsibilities and processes for all personnel, systems, networks, data, and facilities that handle Directory data.

3. Implement the technical recommendations contained in our preliminary audit report.

AUDIT SCOPE AND METHODOLOGY

We did our performance audit according to generally accepted government auditing standards. We audited security controls over Directory data for the period January 1, 2008 through May 2, 2008. We audited whether the Office meets Security Requirements for securing Directory data.

As part of our audit, we reviewed relevant Federal, Office, and Office for Technology policies and procedures. In addition, we interviewed staff responsible for securing Directory data. We also examined Office records and reports related to our audit scope. Further, we examined how Directory data is transmitted from Child Support Enforcement to the Office and the process for backing-up the data.

We reviewed security over the matched Directory text files from Child Support Enforcement and the database where these text files are maintained. As such, we did not review security over the entire Network. Also, we did not use automated software tools to identify any threats to Directory data.

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.

AUTHORITY

The audit was performed 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.

REPORTING REQUIREMENTS

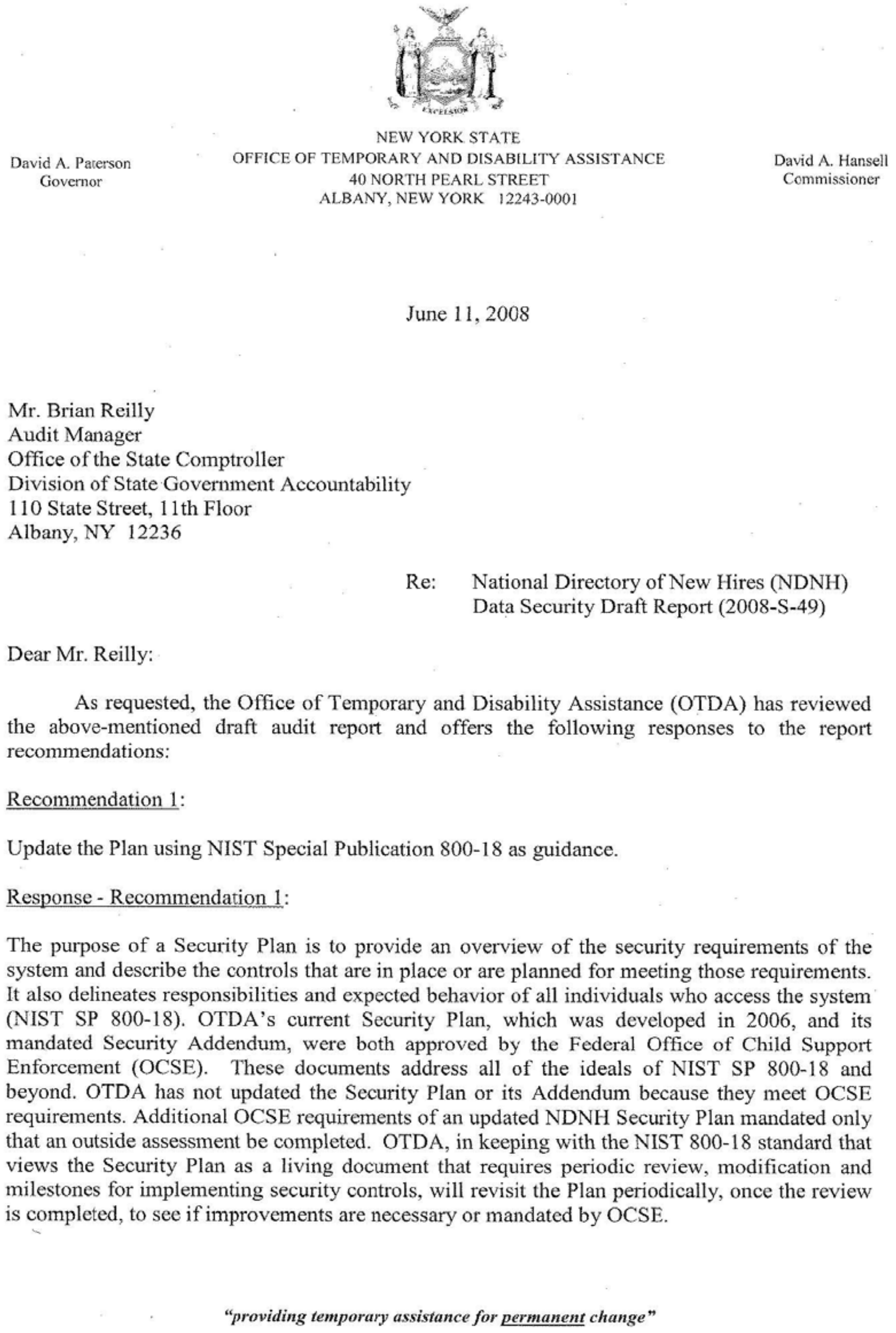
Draft copies of this report were provided to Office officials for their review and comment. Their comments were considered in preparing this report, and are attached as Appendix A. Office officials agreed with our recommendations and have already taken actions to improve security over Directory data. Our response to the Office's comments is presented in Appendix B.

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 Temporary and Disability Assistance 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 therefor.

CONTRIBUTORS TO THE REPORT

Major contributors to this report include Dave Hancox, Brian Reilly, Nadine Morrell, Mark Ren, Corey Harrell, Jennifer Van Tassel, and Sue Gold.

APPENDIX A - AUDITEE RESPONSE



NEW YORK STATE
OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE
40 NORTH PEARL STREET
ALBANY, NEW YORK 12243-0001

David A. Paterson
Governor

David A. Hansell
Commissioner

June 11, 2008

Mr. Brian Reilly
Audit Manager
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

Re: National Directory of New Hires (NDNH)
Data Security Draft Report (2008-S-49)

Dear Mr. Reilly:

As requested, the Office of Temporary and Disability Assistance (OTDA) has reviewed the above-mentioned draft audit report and offers the following responses to the report recommendations:

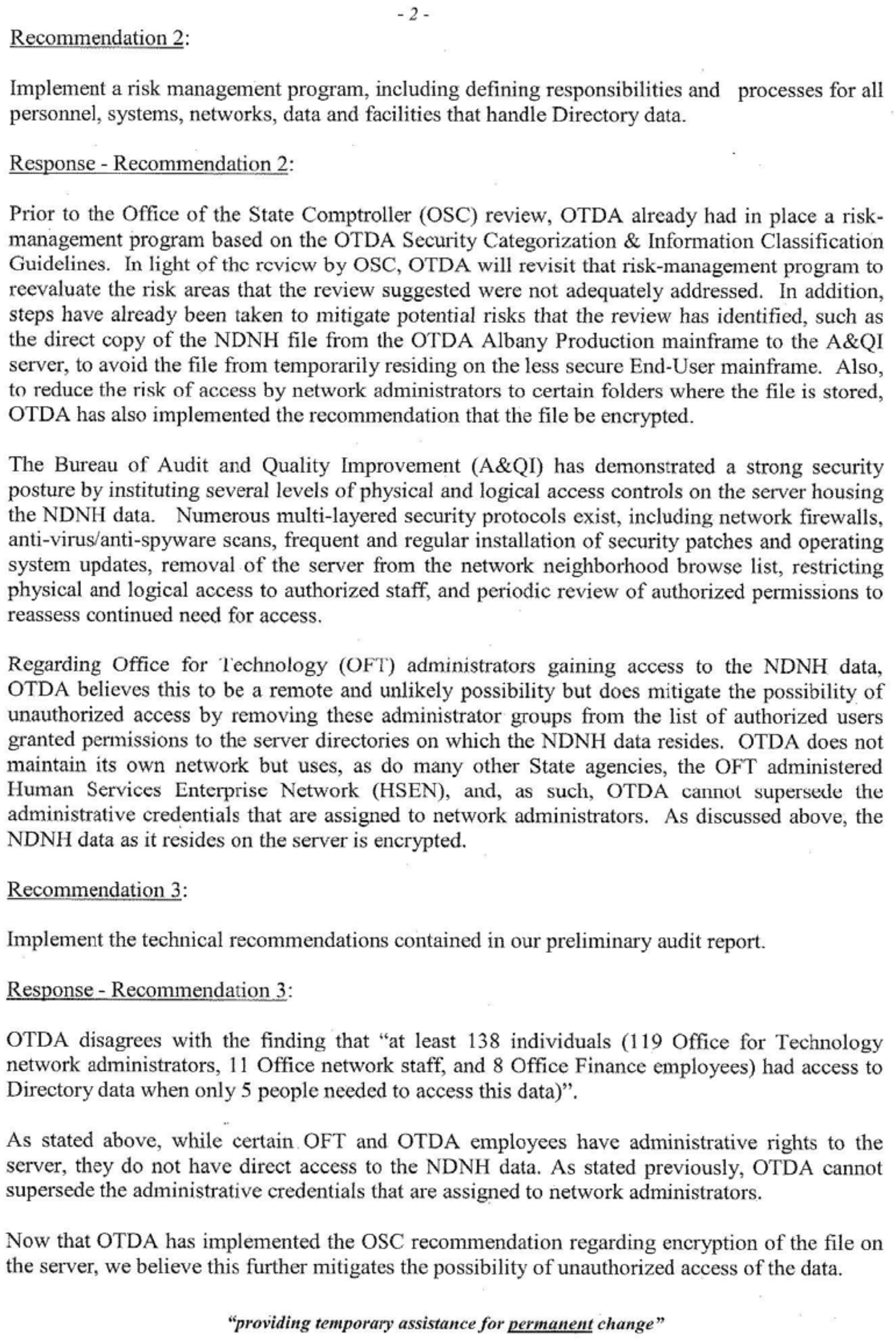
Recommendation 1:

Update the Plan using NIST Special Publication 800-18 as guidance.

Response - Recommendation 1:

The purpose of a Security Plan is to provide an overview of the security requirements of the system and describe the controls that are in place or are planned for meeting those requirements. It also delineates responsibilities and expected behavior of all individuals who access the system (NIST SP 800-18). OTDA's current Security Plan, which was developed in 2006, and its mandated Security Addendum, were both approved by the Federal Office of Child Support Enforcement (OCSE). These documents address all of the ideals of NIST SP 800-18 and beyond. OTDA has not updated the Security Plan or its Addendum because they meet OCSE requirements. Additional OCSE requirements of an updated NDNH Security Plan mandated only that an outside assessment be completed. OTDA, in keeping with the NIST 800-18 standard that views the Security Plan as a living document that requires periodic review, modification and milestones for implementing security controls, will revisit the Plan periodically, once the review is completed, to see if improvements are necessary or mandated by OCSE.

"providing temporary assistance for permanent change"



Recommendation 2:

Implement a risk management program, including defining responsibilities and processes for all personnel, systems, networks, data and facilities that handle Directory data.

Response - Recommendation 2:

Prior to the Office of the State Comptroller (OSC) review, OTDA already had in place a risk-management program based on the OTDA Security Categorization & Information Classification Guidelines. In light of the review by OSC, OTDA will revisit that risk-management program to reevaluate the risk areas that the review suggested were not adequately addressed. In addition, steps have already been taken to mitigate potential risks that the review has identified, such as the direct copy of the NDNH file from the OTDA Albany Production mainframe to the A&QI server, to avoid the file from temporarily residing on the less secure End-User mainframe. Also, to reduce the risk of access by network administrators to certain folders where the file is stored, OTDA has also implemented the recommendation that the file be encrypted.

The Bureau of Audit and Quality Improvement (A&QI) has demonstrated a strong security posture by instituting several levels of physical and logical access controls on the server housing the NDNH data. Numerous multi-layered security protocols exist, including network firewalls, anti-virus/anti-spyware scans, frequent and regular installation of security patches and operating system updates, removal of the server from the network neighborhood browse list, restricting physical and logical access to authorized staff, and periodic review of authorized permissions to reassess continued need for access.

Regarding Office for Technology (OFT) administrators gaining access to the NDNH data, OTDA believes this to be a remote and unlikely possibility but does mitigate the possibility of unauthorized access by removing these administrator groups from the list of authorized users granted permissions to the server directories on which the NDNH data resides. OTDA does not maintain its own network but uses, as do many other State agencies, the OFT administered Human Services Enterprise Network (HSEN), and, as such, OTDA cannot supersede the administrative credentials that are assigned to network administrators. As discussed above, the NDNH data as it resides on the server is encrypted.

Recommendation 3:

Implement the technical recommendations contained in our preliminary audit report.

Response - Recommendation 3:

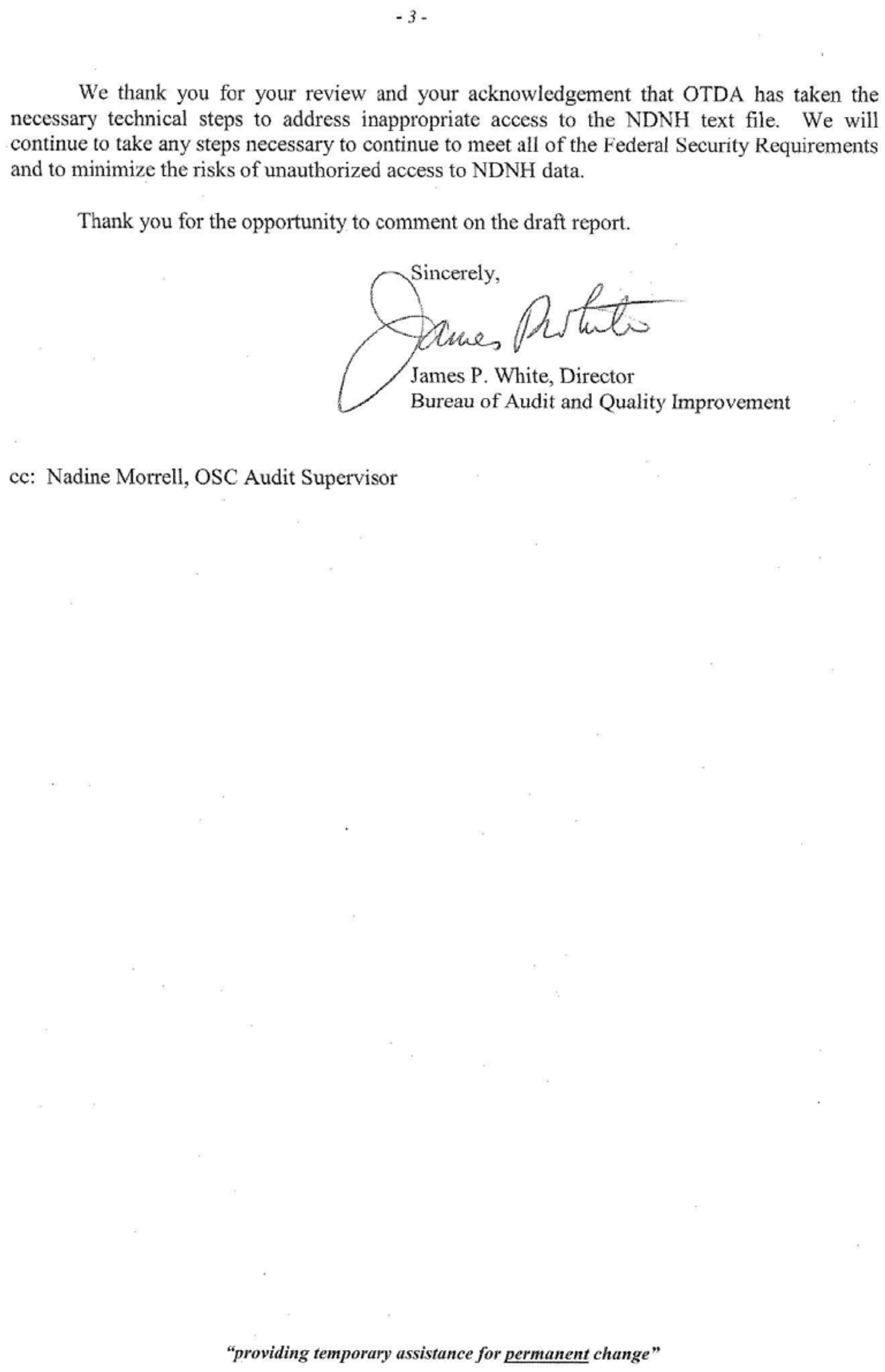
OTDA disagrees with the finding that "at least 138 individuals (119 Office for Technology network administrators, 11 Office network staff, and 8 Office Finance employees) had access to Directory data when only 5 people needed to access this data)".

***
Comment
1**

As stated above, while certain OFT and OTDA employees have administrative rights to the server, they do not have direct access to the NDNH data. As stated previously, OTDA cannot supersede the administrative credentials that are assigned to network administrators.

Now that OTDA has implemented the OSC recommendation regarding encryption of the file on the server, we believe this further mitigates the possibility of unauthorized access of the data.

* See State Comptroller's Comment, page 10



We thank you for your review and your acknowledgement that OTDA has taken the necessary technical steps to address inappropriate access to the NDNH text file. We will continue to take any steps necessary to continue to meet all of the Federal Security Requirements and to minimize the risks of unauthorized access to NDNH data.

Thank you for the opportunity to comment on the draft report.

Sincerely,

James P White

James P. White, Director
Bureau of Audit and Quality Improvement

cc: Nadine Morrell, OSC Audit Supervisor

APPENDIX B - STATE COMPTROLLER COMMENT ON AUDITEE RESPONSE

1. Although the 138 OFT and OTDA employees we identified in the report do not have direct access to the NDNH data, these employees, by virtue of their administrative rights, could still take ownership of the NDNH directories and files. However, as noted in the Office's response, officials have implemented our recommendation regarding file encryption to further secure the data. We believe this step limits the risk associated with the numerous employees with administrative rights.