NEW YORK STATE OF OPPORTUNITY | Office of Temporary and Disability Assistance

ANDREW M. CUOMO
Governor

SAMUEL D. ROBERTS
Commissioner

MICHAEL PERRIN
Executive Deputy Commissioner

September 27, 2016

Mr. John Buyce
Audit Director
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236-0001

Re: Office of the State Comptroller's Final Audit Report (2016-S-27) regarding the National Directory of New Hires (NDNH) Data Security

Dear Mr Buyce:

As required by Section 170 of the Executive Law, this is the New York State Office of Temporary and Disability Assistance's (OTDA) response to the above-mentioned final report. This response will also be sent under separate cover to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees as required.

The audit found that OTDA "officials have taken extensive actions to comply with the Federal requirements for securing Directory data as set forth in the Requirements, and defined in the Temporary Assistance for Needy Families (TANF) and Supplemental Nutrition Assistance Program (SNAP) Computer Matching Agreement (CMA) between Child Support Enforcement and OTDA." The audit also determined that OTDA was fully compliant with 23 of the 32 requirements and partially compliant (in-progress) with seven requirements, and two requirements were not applicable. For the seven requirements identified as partially compliant, the audit found that OTDA had developed policies and procedures to address the requirements; however, the documents and controls reviewed were still being revised and implemented by OTDA and were being developed with the assistance and support of the Office of Information Technology Services (ITS).

The following details the actions OTDA has taken in response to the one recommendation offered in the report.

Recommendation: **To OTDA and ITS**

"Continue to develop and implement controls for those requirements identified as in-progress."

OTDA Response to the Recommendation

The seven requirements cited by OSC as partial compliance primarily involve areas where OTDA has a monitoring responsibility over ITS activities as they pertain to the NDNH data on servers maintained in the ITS data center. These activities include server administration, maintenance and support of the operating system (O/S), patch management of critical security updates, vulnerability scans to identify potential security risks, development of a baseline configuration and software inventory, and completion of required training by ITS staff who have physical and/or logical access to the server housing NDNH data.

OTDA and ITS have developed a comprehensive monitoring strategy to ensure the continued effectiveness of the security controls implemented to meet the requirements of the CMA. The attached document outlines the reporting processes developed by OTDA and ITS to further enhance the security protocols for those areas cited as partial compliance.

Sincerely,

Sam Roberts

Samuel D. Roberts
Commissioner

Attachment

OTDA 90 Day Response – 2016-S-27

Compliance Level Per OSC Audit (TANF and SNAP)	OSC Comments	OTDA Response
In-Progress	The Office is in the process of developing procedures to ensure all administrative staff with access to the information system housing Directory data have taken the necessary annual training. Per the Office's NDNH Security Policy, this includes implementing an oversight control where ITS will provide the Office a listing of staff who have administrative access to the information system housing Directory data, and confirmation that they have completed the required training.	All OTDA staff with access to NDNH data must complete the required training on an annual basis. To ensure ITS staff with physical and logical access to the server housing NDNH data in the ITS data center have likewise completed the training, ITS will provide an annual list of staff with such access, along with confirmation that the required training has been completed (OTDA has received the list from ITS for 2016).
In-Progress	The Office is in the process of developing policies and procedures outlining the necessary controls to fully address this requirement. The Office is currently working with ITS to ensure an effective, continuous monitoring strategy is in place over the information system housing Directory data.	OTDA has received a commitment from ITS for periodic reports to enable OTDA to monitor server security activities administered by ITS. The reports will provide information regarding the following: 1) Server Operating System updates 2) Server patch updates 3) User Access – list of ITS staff with both logical and physical access to the server housing the NDNH data 4) Server vulnerability scanning of the server 5) Data backup – confirmation that the backup files are retained for 30 days 6) ITS staff training compliance – confirmation that ITS staff with user access have completed the mandatory training
In-Progress (TANF only)	The Office has identified the software and hardware components to be included in its asset inventory. The Office anticipates the completion of the inventory by mid-June 2016.	OTDA has prepared an inventory of software and hardware components installed on the server housing the NDNH data. This inventory is included in the "NDNH Security Policies and Procedures" manual and will be updated on an annual basis.

In-Progress (TANF only)	The Office has developed a policy that documents system security requirements for the information system housing Directory data, and is in the process of finalizing and implementing those controls in conjunction with ITS.	OTDA continues to enhance its "NDNH Security Policies and Procedures" manual to include additional information in the areas cited by OSC as "partial compliance". The document has been updated to reflect the receipt of periodic reports from ITS that will enable OTDA to monitor server security activities administered by ITS. The document will continue to be reviewed and updated to reflect ongoing monitoring strategies implemented to ensure the security protocols developed to meet the CMA requirements are current and applicable.
In-Progress (TANF only)	The Office has developed a policy defining high-level procedures to follow in the event weaknesses on the information system housing Directory data are identified. The Office also plans to develop a separate "Corrective Action Policy Plan and Procedures" document that will further detail specific actions to be taken in the event established controls identify a security threat.	OTDA has developed a "Corrective Action Policy Plan and Procedures" outlining the potential risks and specific actions to be taken to mitigate those risks. The Plan also incorporates OTDA's monitoring responsibilities of ITS server security responsibilities and associated risks. The plan will be reviewed and updated periodically to ensure any weakness or risks in the security posture implemented for NDHN data is identified in a timely manner and an action plan is implemented.
In-Progress (TANF only)	The Office has developed a policy listing configuration items to be included as a baseline for the information system housing Directory data. The Office is still in the process of collecting and finalizing this information for completeness.	OTDA has developed a baseline configuration inventory of the system housing NDNH data. This configuration inventory will be included in the "NDNH Security Policies and Procedures" manual and reviewed annually to ensure accuracy and completeness.

OTDA 90 Day Response – 2016-S-27

In-Progress (TANF only)	The Office has developed a policy detailing plans for oversight monitoring of ITS responsibilities. This includes working with ITS to develop a process by which the Office can monitor the activities of ITS as they relate to management and administration of the information system housing Directory data. According to the Office's policy, ITS is aware of the Office's monitoring responsibilities, and ITS is investigating how to appropriately meet all reporting requirements.	We have received a commitment from ITS for reports to enable OTDA to monitor server security activities. The reports will provide information regarding the following: 1) Server Operating System updates 2) Server patch updates 3) User Access – list of ITS staff with both logical and physical access to the server housing the NDNH data 4) Server vulnerability scanning of the server 5) Data backup – confirmation that the backup files are retained for 30 days 6) ITS staff training compliance – confirmation that ITS staff with user access have completed the mandatory training ITS has already provided reports and documentation to allow OTDA to monitor and confirm compliance with the server security requirements outlined in the Computer Matching Agreement, and will continue to provide these reports on a periodic basis.