New York State Office of the State Comptroller
Thomas P. DiNapoli

Division of State Government Accountability

National Directory of New Hires Data Security

Office of Temporary and Disability Assistance

Report 2016-S-27 July 2016

Executive Summary

Purpose

To determine whether the Office of Temporary and Disability Assistance has met Federal requirements for securing National Directory of New Hires data. The audit covers the period April 11, 2016 to June 2, 2016.

Background

The Office of Temporary and Disability Assistance (Office) is responsible for supervising State programs that provide assistance and support to eligible families and individuals. Two such programs administered by the Office are the Temporary Assistance for Needy Families (TANF) and the Supplemental Nutrition Assistance Program (SNAP). As part of managing these programs, the Office obtains National Directory of New Hires (Directory) data provided by the Office of Child Support Enforcement (Child Support Enforcement), a subdivision of the U.S. Department of Health and Human Services (Health and Human Services).

The Directory data is comprised of information on new hires, quarterly wage, and unemployment insurance. The Office uses Directory data to verify TANF and SNAP eligibility information. The identification and verification of this data helps the Office identify and resolve any fraudulent activity by program recipients, as well as maintain program integrity.

All State agencies that receive and process Directory data must demonstrate a strong security posture and comply with the security requirements established by Health and Human Services and Child Support Enforcement. The State agency also must comply with Child Support Enforcement's Security Requirements for State Agencies Receiving National Directory of New Hires Data (Requirements), dated March 2015. The Requirements define the administrative, technical, and physical security controls required to be implemented by the State agency prior to receiving Directory data.

Every four years, the Office must submit a copy of an independent security assessment to Child Support Enforcement. At the request of Office officials, we performed an independent security assessment of the Directory system security controls at the Office.

Key Findings

- The Office has taken actions to comply with the Federal requirements for securing Directory data. We found that the Office is fully compliant with 23 of the 32 requirements and partially compliant (in-progress) with seven requirements, and two requirements were not applicable due to current practices at the Office and modifications of Federal reporting requirements.

Key Recommendation

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

Other Related Audits/Reports of Interest

Office of Temporary and Disability Assistance: Security Controls over National Directory of New Hires Data (2012-S-9)

Office of Temporary and Disability Assistance: National Directory of New Hires Data Security (Follow-Up Report) (2009-F-29)

Office of Temporary and Disability Assistance: National Directory of New Hires Data Security (2008-S-49)

State of New York
Office of the State Comptroller

Division of State Government Accountability

July 18, 2016

Mr. Samuel D. Roberts
Commissioner
Office of Temporary and Disability Assistance
40 North Pearl Street
Albany, NY 12243

Dear Mr. Roberts:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage government resources efficiently and effectively. By doing so, it provides 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 of the Office of Temporary and Disability Assistance entitled *National Directory of New Hires Data Security*. 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,

Office of the State Comptroller
Division of State Government Accountability

Table of Contents

State Government Accountability Contact Information:
Audit Director: John Buyce
Phone: (518) 474-3271
Email: StateGovernmentAccountability@osc.state.ny.us
Address:
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

This report is also available on our website at: www.osc.state.ny.us

Background

The Office of Temporary and Disability Assistance (Office) is responsible for supervising programs that provide assistance and support to eligible families and individuals. These programs: assist welfare recipients and potential welfare recipients in entering employment, promote access to economic supports for low-income working State citizens, connect individuals with special needs to appropriate services, and help reduce child poverty.

Two of these programs administered by the Office are the Temporary Assistance for Needy Families (TANF) and the Supplemental Nutrition Assistance Program (SNAP). The TANF program assists needy families who either have, or are expecting, children. The program also focuses on promoting individual responsibility for the recipient, as well as family independence. The SNAP program provides monthly electronic benefits, which can be used like cash, to purchase food at authorized retail food stores. Eligibility and benefit levels are based on household size, income, and other factors.

The Office verifies recipient eligibility for both the TANF and SNAP programs by matching recipient data against Federal data from the National Directory of New Hires (Directory). The Federal Office of Child Support Enforcement (Child Support Enforcement) owns and operates the Directory, which is comprised of information on new hires, quarterly wage, and unemployment insurance.

Child Support Enforcement is responsible for ensuring the protection of Directory information, even when disclosed to State agencies. Therefore, Child Support Enforcement has developed its Security Requirements for State Agencies Receiving National Directory of New Hires Data (Requirements), dated March 2015. This document deals with the security requirements and privacy safeguards that a State agency must have in place before receiving, storing, distributing, or otherwise using Directory information. Child Support Enforcement requires strong security controls to ensure that Directory information is protected and that there is individual accountability in protecting and maintaining the privacy of this information.

Furthermore, Child Support Enforcement enters into a Computer Matching Agreement (CMA) with agencies that receive Directory information. The CMA describes the purpose, legal authority, justification, and expected results of the match, description of the records, retention and disposition of the information, and reimbursement and performance reporting requirements. The Office has entered into two CMAs with Child Support Enforcement for the receipt of Directory data for both the TANF and SNAP programs.

The New York State Office of Information Technology Services (ITS) is responsible for the administration and management of the information system housing Directory data. This management responsibility includes, but is not limited to, applying updates, patch management controls, and providing physical security over the information system itself, which is housed at the ITS State Data Center.

Child Support Enforcement expects the State agency receiving Directory information to demonstrate its security posture before receiving Directory data and periodically thereafter. Therefore, Child Support Enforcement requires the State agency to have an independent security assessment conducted within the last four years by an unbiased, outside entity. This security assessment must include information on the security controls defined within the CMA. The independent security assessment must then be submitted to Child Support Enforcement, and must include detailed findings (if any) and recommendations to improve the State agency's plans, procedures, and practices. At the request of Office officials, we performed an independent security assessment of the Directory system security controls at the Office.

Audit Findings and Recommendations

We found that Office 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 TANF and SNAP CMAs between Child Support Enforcement and the Office.

We found that the Office is 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 (in-progress), the Office has developed policies and procedures to address the requirements. However, these documents, and the controls discussed therein, are still being revised and implemented by the Office, and, where applicable, developed with the assistance and support of ITS.
- For the two requirements marked as not applicable, one requirement does not apply because the Office does not generate hard-copy reports containing Directory data. The second requirement is no longer applicable due to changes in the Federal reporting requirements by which State agencies receiving Directory data are no longer required to submit the Security and Privacy Self-Assessment.

We reported additional sensitive technical information concerning these findings to Office officials during meetings and on-site visits over the course of the audit, and consequently, do not address them in detail in this report due to their confidential nature.

Recommendation

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

Audit Scope and Methodology

Our audit determined whether the Office of Temporary and Disability Assistance has met Federal requirements for securing National Directory of New Hires data. The audit covers the period April 11, 2016 through June 2, 2016.

To accomplish our objective and assess related internal controls, we audited specific security controls implemented by the Office to comply with the Federal requirements for securing Directory data. As part of our audit, we reviewed relevant Office security policies and configurations, records, and reports related to our audit scope. In addition, we held interviews with Office staff responsible for securing Directory data. We also verified certain technical and physical controls where necessary per our audit scope. As such, we did not review security over the entire Office network.

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.

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

We provided a draft copy of this report to Office officials for their review and formal comment. Their comments were considered in preparing this final report and are attached in their entirety at the end of it. Officials agreed with our observations and pledged to continue their security monitoring and enhancement efforts in the future.

Within 90 days after 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 recommendation contained herein, and if the recommendation was not implemented, the reasons why.

Contributors to This Report

John F. Buyce, CPA, CIA, CFE, CGFM, Audit Director
Nadine Morrell, CIA, CISM, CGAP, Audit Manager
Bob Mainello, CPA, Audit Supervisor
Jared Hoffman, OSCP, GPEN, GWAPT, Examiner-in-Charge
Rachael Hurd, Senior Examiner
Nicole Tommasone, Senior Examiner

Division of State Government Accountability

Andrew A. SanFilippo, Executive Deputy Comptroller
518-474-4593, asanfilippo@osc.state.ny.us

Tina Kim, Deputy Comptroller
518-473-3596, tkim@osc.state.ny.us

Brian Mason, Assistant Comptroller
518-473-0334, bmason@osc.state.ny.us

Vision

A team of accountability experts respected for providing information that decision makers value.

Mission

To improve government operations by conducting independent audits, reviews and evaluations of New York State and New York City taxpayer financed programs.

Exhibit

Office of Temporary and Disability Assistance
NDNH Data Security Requirements TANF and SNAP Programs

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
1.	The state agency shall restrict access to, and disclosure of, the NDNH information to authorized personnel who need the NDNH information to perform their official duties in connection with the authorized purposes specified in the agreement.	The state agency shall restrict access to, and disclosure of, the NDNH information to authorized personnel who need the NDNH information to perform their official duties in connection with the authorized purposes specified in the agreement.	Compliant	
2.	The state agency shall establish and maintain an ongoing management oversight and quality assurance program to ensure that only authorized personnel have access to NDNH information.	The state agency shall establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized personnel have access to NDNH information.	Compliant	
3.	The state agency shall advise all authorized personnel who will access NDNH information of the confidentiality of the NDNH information, the safeguards required to protect the NDNH information, and the civil and criminal sanctions for noncompliance contained in the applicable federal and state laws, including Section 453 of the Social Security Act. 42 U.S.C. § 653(1)(2).	The state agency shall advise all authorized personnel who access NDNH information of the confidentiality of NDNH information, the safeguards required to protect the NDNH information, and the civil and criminal sanctions for non-compliance contained in the applicable federal and state laws, including subsection 453 of the Social Security Act. 42 U.S.C. § 653(1)(2).	Compliant	

Note. NDNH = National Directory of New Hires; TANF = Temporary Assistance for Needy Families; SNAP = Supplemental Nutrition Assistance Program.

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
4.	The state agency shall deliver security and privacy awareness training to personnel with authorized access to NDNH information and the system that houses, processes, or transmits NDNH information. The training shall describe each user's responsibility for proper use and protection of NDNH information, how to recognize and report potential indicators of insider threat, and the possible sanctions for misuse. All personnel shall receive security and privacy awareness training before accessing NDNH information and at least annually thereafter. The training shall cover the matching provisions of the federal Privacy Act and other federal and state laws governing use and misuse of NDNH information.	The state agency shall deliver security and privacy awareness training for authorized personnel. The training shall include information about the responsibility of such personnel for proper use and protection of NDNH information, recognizing and reporting potential indicators of insider threat, and the possible sanctions for misuse. All personnel shall receive security and privacy awareness training prior to accessing NDNH information and at least annually thereafter. Such training shall address the matching program provisions of the federal Privacy Act and other federal and state laws governing the use and misuse of NDNH information.	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.
5.	The state agency personnel with authorized access to NDNH information shall sign non-disclosure agreements, rules of behavior, or equivalent documents before system access annually and if changes in assignment occur. The non-disclosure agreement, rules of behavior, or equivalent documents shall outline the authorized purposes for which the state agency may use the NDNH information and the civil and criminal penalties for unauthorized use. The state agency may use "wet" and/or electronic signatures to acknowledge non-disclosure agreements, rules of behavior, or equivalent documents.	The state agency personnel with authorized access to NDNH information shall sign nondisclosure agreements, rules of behavior or equivalent documents prior to system access annually and if changes occur. The non-disclosure agreement, rules of behavior, or equivalent documents shall outline the authorized purposes for which the NDNH information may be used by the state agency and the civil and criminal penalties for unauthorized use. The state agency can use "wet" and/or electronic signatures to acknowledge non-disclosure agreements, rules of behavior, or equivalent documents.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
6.	The state agency shall maintain records of authorized personnel with access to the NDNH information. The records shall contain a copy of each individual's signed non-disclosure agreement, rules of behavior or equivalent document and proof of the individual's participation in security and privacy awareness training. The state agency shall make such records available to Child Support Enforcement upon request.	The state agency shall maintain records of authorized personnel with access to the NDNH information. The records shall contain a copy of each individual's signed non-disclosure agreement, rules of behavior or equivalent document and proof of the individual's participation in security and privacy awareness training. The state agency shall make such records available to Child Support Enforcement within two working days of a request for such records.	Compliant	
7.	The state agency shall have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure involving personal information), or suspected incidents involving NDNH information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state agency shall report confirmed and suspected incidents, in either electronic or physical form, to the Federal Parent Locator Service (FPLS) Information Systems Security Officer (ISSO) designated on section VI.A of this security addendum. The requirement for the state agency to report confirmed or suspected incidents involving NDNH information to Child Support Enforcement exists in addition to, not in lieu of, any state agency requirements to report to any other reporting agencies.	The state agency shall have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure or use involving personal information), or suspected incidents involving NDNH information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state agency shall report confirmed and suspected incidents, in either electronic or physical form, to the Federal Parent Locator Service (FPLS) Information Systems Security Officer (ISSO) designated in Section VI.A of this security addendum. The requirement for the state agency to report confirmed or suspected incidents involving NDNH information to Child Support Enforcement exists in addition to, not in lieu of, any state agency requirements to report to any other reporting agencies.	Compliant	
8.	The state agency shall prohibit the use of non-state agency furnished equipment to access NDNH information without specific written authorization from the appropriate state agency representatives.	The state agency shall prohibit the use of non-state agency furnished equipment to access NDNH information without specific written authorization for use of the equipment from the appropriate state agency representatives.	Compliant	The Office has received approval from Child Support Enforcement that its SSL VPN remote access solution is compliant with NDNH requirements.

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
9.	The state agency shall require that personnel accessing NDNH information remotely (for example, telecommuting) adhere to all the security and privacy safeguarding requirements provided in this security addendum. State agency and non-state agency furnished equipment shall have appropriate software with the latest updates to protect against attacks, including, at a minimum, current antivirus software and up-to-date system patches and other software patches. Before electronic connection to state agency resources, the state agency shall scan the state agency and non-state agency furnished equipment to ensure compliance with the state agency standards. All remote connections shall be through a Network Access Control, and all data in transit between the remote location and the agency shall be encrypted using Federal Information Processing Standards (FIPS) 140-2 encryption standards. Personally owned mobile devices shall not be authorized.	The state agency shall require that personnel accessing NDNH information remotely (for example, telecommuting) adhere to all the security and privacy safeguarding requirements provided in this security addendum. State agency and non-state agency furnished equipment shall have appropriate software with the latest updates to protect against attacks, including, at a minimum, current antivirus software and up-to-date system patches and other software patches. Prior to electronic connection to state agency resources and at least twice yearly thereafter, the state agency shall scan the state agency and non-state agency furnished equipment to ensure compliance with a set of standards developed by the state agency. All connections must be through a Network Access Control solution, and all data in transit between the remote location and the agency must be encrypted using Federal Information Processing Standards (FIPS) 140-2 encryption standards. Equipment that may be authorized does not include mobile devices such as Personal Digital Assistants (PDA), smartphones, tablets, iPods, MP3 players, or flash drives.	Compliant	The Office has received approval from Child Support Enforcement that its SSL VPN remote access solution is compliant with NDNH requirements.
10.	The state agency shall implement an effective continuous monitoring strategy and program to ensure the continued effectiveness of security controls by maintaining ongoing awareness of information security, vulnerabilities, and threats to the information system housing NDNH information. The continuous monitoring program shall include configuration management, patch management, vulnerability management, risk assessments before making changes to the system and environment, ongoing security control assessments, and reports to state agency officials as required.	The state agency shall implement an effective continuous monitoring strategy and program to ensure the continued effectiveness of security controls by maintaining ongoing awareness of information security, vulnerabilities, and threats to the information system housing NDNH information.	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.

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
11.	The state agency shall maintain an asset inventory of all software and hardware components within the boundary of the information system housing NDNH information. The inventory shall be at a level of granularity deemed necessary by the state agency for internal tracking and reporting. Child Support Enforcement maintains an inventory of all software and hardware components within the boundary of the information system housing the agency input file.	Not Applicable - TANF only requirement	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.
12.	The state agency shall maintain a system security plan describing the security requirements for the system housing NDNH information and the security controls in place or planned for meeting those requirements. The system security plan shall describe the responsibilities and expected behavior of all individuals who access the system.	Not Applicable - TANF only requirement	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.
13.	The state agency shall maintain a plan of action and milestones (corrective action plan) for the information system housing NDNH information to document plans to correct weaknesses identified during security control assessments and to reduce or eliminate known vulnerabilities in the system. The state agency shall update the corrective action plan as necessary based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.	Not Applicable - TANF only requirement	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.

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
14.	The state agency shall maintain a baseline configuration of the system housing NDNH information. The baseline configuration shall include information on system components (for example, standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture.	Not Applicable - TANF only requirement	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.
15.	The state agency shall limit and control logical and physical access to NDNH information to only those personnel authorized for such access based on their official duties, and identified in the records maintained by the state agency pursuant to numbers 6 and 27 of this section. The state agency shall prevent personnel from browsing case files not assigned to them by using technical controls or other compensating controls.	SNAP TECH 1: The state agency shall utilize and maintain technological (logical) access controls that limit access to NDNH information to only those personnel who are authorized for such access based on their official duties and identified in the records maintained by the state agency. SNAP TECH 2: The state agency shall prevent browsing with technical controls that limit access to NDNH information to assigned cases and areas of responsibility.	Compliant	
16.	The state agency shall transmit and store all NDNH information provided pursuant to this agreement in a manner that safeguards the information and prohibits unauthorized access.	The state agency shall transmit and store all NDNH information provided pursuant to this agreement in a manner that safeguards the information and prohibits unauthorized access. The state agency and Child Support Enforcement exchange NDNH information via a mutually approved and secure data transfer method which utilizes FIPS 140-2 encryption standards.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
17.	The state agency shall prohibit NDNH information from being transferred to and stored on portable digital media and mobile computing and communications devices unless encrypted at the disk or device level, using a FIPS 140-2 compliant product.	The state agency shall prohibit NDNH information from being copied to, and stored on, digital media (for example, diskettes, magnetic tapes, external/removable hard drives, flash drives, compact disks, and digital video disks) and mobile computing and communications devices (for example, laptops, smartphones, tablets, notebook computers, PDAs, cellular telephones, digital cameras, and audio devices) unless encrypted at the disk or device level, using a FIPS 140-2 compliant product.	Compliant	
18.	The state agency shall prohibit the use of computing resources resident in commercial or public facilities (for example, hotels, convention centers, and airports) from accessing, transmitting, or storing NDNH information.	The state agency shall prohibit the use of digital media and computing and communications devices resident in commercial or public facilities (for example, hotels, convention centers, airports) from transmitting and/or storing NDNH information.	Compliant	
19.	The state agency shall prohibit remote access to the NDNH information, except via a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication, as required by OMB M-06-16. The state agency shall control remote access through a limited number of managed access control points. If the state agency cannot provide two-factor authentication, the state agency shall submit to Child Support Enforcement a written description of compensating controls, subject to written approval by Child Support Enforcement before allowing remote access.	The state agency shall prohibit remote access to the NDNH information, except through the use of a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication, as required by OMB M-06-16. The state agency shall control remote access through a limited number of managed access control points. If the state agency cannot provide two-factor authentication, the state agency shall submit to Child Support Enforcement a written description of compensating controls, subject to written approval by Child Support Enforcement prior to allowing remote access.	Compliant	The Office has received approval from Child Support Enforcement that its SSL VPN remote access solution is compliant with NDNH requirements.

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
20.	The state agency shall maintain a fully automated audit trail system with audit records that, at a minimum, collect data associated with each query transaction to its initiator, capture date and time of system events and types of events. The audit trail system shall protect data and the audit tool from addition, modification or deletion and should be regularly reviewed and analyzed for indications of inappropriate or unusual activity.	The state agency shall maintain a fully automated audit trail system with audit records that, at a minimum, collect data associated with each query transaction to its initiator, capture date and time of system events and type of events. The audit trail system shall protect data and the audit tool from addition, modification, and/or deletion and should be regularly reviewed/analyzed for indications of inappropriate or unusual activity.	Compliant	
21.	The state agency shall log each computer-readable data extract (secondary store or file with duplicate NDNH information) from any database holding NDNH information and verify that each extract has been erased within 90 days after completing required use. If the state agency requires the extract for longer than 90 days to accomplish a purpose authorized pursuant to this agreement, the state agency shall request permission, in writing, to keep the extract for a defined period of time, subject to Child Support Enforcement's written approval. The state agency shall comply with the retention and disposition requirements in the agreement.	The state agency shall log each computer-readable data extract (secondary store or file with duplicate NDNH information) from any database holding NDNH information and verify that each extract has been erased within 90 days after completing required use. If use of the extract is still required to accomplish a purpose authorized pursuant to this agreement and complies with the retention and disposition requirements in the agreement, the state agency shall request permission, in writing, to keep the extract for a defined period of time, subject to Child Support Enforcement's written approval.	Compliant	
22.	The state agency shall utilize a time-out function for remote access and mobile devices that require a user to re-authenticate after no more than 30 minutes of inactivity.	The state agency shall utilize a time-out function for remote access and mobile devices that require a user to re-authenticate after no more than 30 minutes of inactivity.	Compliant	
23.	The state agency shall erase electronic records after completing authorized use in accordance with the retention and disposition requirements in the agreement.	The state agency shall erase electronic records after completing the authorized use in accordance with the retention and disposition requirements in the agreement.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
24.	The state agency shall implement a Network Access Control (also known as Network Admission Control [NAC]) solution in conjunction with a VPN option to enforce security policy compliance on all state agency and non-state agency remote devices that attempt to gain access to, or use, NDNH information. The state agency shall use a NAC solution to authenticate, authorize, evaluate, and remediate remote wired and wireless users before they can access the network. The implemented NAC solution shall evaluate whether remote machines are compliant with security policies through host(s) integrity tests against predefined templates, such as patch level, service packs, antivirus, and personal firewall status, as well as custom created checks tailored for the state enterprise environment. The state agency shall disable functionality that allows automatic code execution. The solution shall enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing the state network and resources while maintaining an audit record on users' access and presence on the state network.	The state agency shall implement a Network Access Control (also known as Network Admission Control [NAC]) solution in conjunction with a VPN option to enforce security policy compliance on all state agency and non-state agency devices that attempt to gain access to, or use, NDNH information. The state agency shall use a NAC solution to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users before they can access the network. The NAC solution chosen or employed is capable of evaluating whether remote machines are compliant with security policies through host(s) integrity tests against predefined templates, such as patch level, service packs, antivirus, and personal firewall status, as well as custom created checks tailored for the state enterprise environment. In addition, functionality that allows automatic execution of code shall be disabled. The solution shall enforce security policies by blocking, isolating, or quarantining non-compliant devices from accessing the state network and resources while maintaining an audit record/report on users' access and presence on the state network.	Compliant	The Office has received approval from Child Support Enforcement that its SSL VPN remote access solution is compliant with NDNH requirements.

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
25.	The state agency shall ensure that the organization responsible for the data processing facility storing, transmitting, or processing the NDNH information complies with the security requirements established in the security addendum. The "data processing facility" includes the personnel, facilities, documentation, data, electronic and physical records and other machine-readable information, and the information systems of the state agency including, but not limited to, employees and contractors working with the data processing facility, statewide centralized data centers, contractor data centers, and any other individual or entity collecting, storing, transmitting, or processing NDNH information.	Not Applicable - TANF only requirement	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.
26.	The state agency shall store all NDNH information provided pursuant to the agreement in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.	The state agency shall store all NDNH information provided pursuant to this agreement in an area that is physically safe from access by unauthorized persons during duty hours as well as non-duty hours or when not in use.	Compliant	
27.	The state agency shall maintain a list of personnel authorized to access facilities and systems processing sensitive data, including NDNH information. The state agency shall control access to facilities and systems wherever NDNH information is processed. Designated officials shall review and approve the access list and authorization credentials initially and periodically thereafter, but no less often than annually.	The state agency shall maintain a list of personnel authorized to access facilities and systems processing sensitive data, including NDNH information. The state agency shall control access to facilities and systems wherever sensitive information is processed. Designated officials shall review and approve the access list and authorization credentials initially and periodically thereafter, but no less often than annually.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
28.	The state agency shall label printed reports containing NDNH information to denote the level of sensitivity of the information and limitations on distribution. The state agency shall maintain printed reports in a locked container when not in use and shall not transport NDNH information off state agency premises. When no longer needed, in accordance with the retention and disposition requirements in the agreement, the state agency shall destroy printed reports by shredding or burning.	The state agency shall label printed reports containing NDNH information to denote the level of sensitivity of the information and the limitation on distribution. The state agency shall maintain the printed reports in a locked container when not in use and never transport NDNH information off state agency premises. When no longer needed, in accordance with the retention and disposition requirements in the agreement, the state agency shall destroy printed reports by shredding or burning.	Not Applicable	The Office does not generate any printed reports containing Directory information.
29.	The state agency shall use locks and other protective measures at all physical access points (including designated entry and exit points) to prevent unauthorized access to computer and support areas containing NDNH information.	The state agency shall use locks and other protective measures at all physical access points (including designated entry/exit points) to prevent unauthorized access to computer and support areas containing NDNH information.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
30.	**Breach and Reporting Notification Responsibility:** Upon disclosure of NDNH information from Child Support Enforcement to the state agency, the state agency is the responsible party in the event of a breach or suspected breach of the information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state agency shall report confirmed and suspected incidents, in either electronic or physical form, to the FPLS ISSO designated in section VII.A of this security addendum. The state agency is responsible for all reporting and notification activities, including but not limited to: investigating the incident; communicating with required state government breach response officials; notifying individuals whose information is breached; communicating with any third parties, including the media, as necessary; notifying any other public and private sector agencies involved; responding to inquiries about the breach; resolving all issues surrounding the breach of NDNH information; performing any necessary follow-up activities to correct the vulnerability that allowed the breach; and any other activities, as required by Child Support Enforcement.	**Breach and Reporting Notification Responsibility:** Upon disclosure of NDNH information from Child Support Enforcement to the state agency, the state agency is the responsible party in the event of a breach or suspected breach of the information. Immediately upon discovery, but in no case later than one hour after discovery of the incident, the state agency shall report confirmed and suspected incidents, in either electronic or physical form, to the FPLS ISSO designated in section VI.A of this security addendum. The state agency is responsible for all reporting and notification activities, including but not limited to: investigating the incident; communicating with required state government breach response officials; notifying individuals whose information is breached; communicating with any third parties including the media, as necessary; notifying any other public and private sector agencies involved; responding to inquiries about the breach; resolving all issues surrounding the breach of NDNH information; performing any necessary follow-up activities to correct the vulnerability that allowed the breach; and any other activities as required by Child Support Enforcement.	Compliant	
31.	**Security Certification – Security Posture:** The state agency has submitted to Child Support Enforcement the required documentation and Child Support Enforcement has reviewed and approved the state agency's security posture.	**Security Certification – Security Posture:** The state agency has submitted to Child Support Enforcement the required security documentation and Child Support Enforcement has reviewed and approved the state agency's security posture.	Not Applicable	The Office is no longer required to submit the Security and Privacy Self-Assessment over NDNH security controls to Child Support Enforcement.

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
32.	**Independent Security Assessment:** The state agency shall submit to Child Support Enforcement a copy of a recent independent security assessment every four years. Refer to the Office of Child Support Enforcement Division of Federal Systems Security Requirements for State Agencies Receiving National Directory of New Hires Data, Section VI, for additional guidance. If major organizational and/or system framework changes have taken place since the previous independent security assessment, the state agency shall have an independent security assessment conducted within six (6) months of the change. The state agency shall submit the results of the independent assessment to Child Support Enforcement.	**Independent Security Assessment:** The state agency shall submit to Child Support Enforcement a copy of a recent independent security assessment every four years. Refer to the Office of Child Support Enforcement Division of Federal Systems Security Requirements for State Agencies Receiving National Directory of New Hires Data, Section VI, for additional guidance. If major organizational and/or system framework changes have taken place since the previous independent security assessment, a new independent security assessment shall be conducted and submitted to Child Support Enforcement within six (6) months of the changes. The state agency must provide Child Support Enforcement with the results of the independent assessment.	Compliant	

Agency Comments

Office of Temporary and Disability Assistance

ANDREW M. CUOMO
Governor

SAMUEL D. ROBERTS
Commissioner

MICHAEL PERRIN
Executive Deputy Commissioner

July 13, 2016

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

Dear Mr. Buyce:

The following is the response of the Office of Temporary and Disability Assistance (OTDA) to the Office of State Comptroller (OSC) draft report 2016-S-27 dated July 6, 2016 entitled "National Directory of New Hires Data Security."

We appreciate your auditors' work on this project and OSC's acknowledgement of the emphasis OTDA has placed on providing strong controls over National Directory of New Hires data. In particular, we note your conclusion that OTDA has taken "extensive actions to comply with the Federal requirements." In the future, OTDA will continue our security monitoring and enhancement efforts.

We appreciate the professionalism displayed by your auditors during the course of this audit. If you have any questions, please feel free to contact me directly.

Respectfully,

Kevin Kehmna

Kevin Kehmna, Director
Bureau of Audit and Quality Improvement

cc: Samuel Roberts
Michael Perrin
Krista Rock
Stephen Bach
Thomas Gosh
Valerie Boyd
Kathleen Murphy

Riverview Center, Suite 410, 40 North Pearl Street, Albany, NY 12243-0001 | www.otda.ny.gov