Office of Temporary and Disability Assistance

National Directory of New Hires Data Security

Report 2019-S-67 | May 2020

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

Division of State Government Accountability

Audit Highlights

Objective

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 June 2, 2016 to March 3, 2020.

About the Program

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 the *Security Requirements for State Agencies Receiving National Directory of New Hires Data* dated August 2018. These 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 30 of the 32 requirements; the remaining two requirements were found to be not applicable due to current practices at the Office and modifications of federal reporting requirements.

Key Recommendation

- Continue to maintain a system of controls that ensure compliance with federal requirements for securing Directory data.

Office of the New York State Comptroller
Division of State Government Accountability

May 20, 2020

Michael P. Hein
Commissioner
Office of Temporary and Disability Assistance
40 North Pearl Street
Albany, NY 12243

Dear Mr. Hein:

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 so doing, 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,

Division of State Government Accountability

Contents

Glossary of Terms

Term	Description	Identifier
Child Support Enforcement	Office of Child Support Enforcement	*Federal Agency*
CMA	Computer Matching Agreement	*Key Term*
Directory	National Directory of New Hires	*Key Term*
ITS	Office of Information Technology Services	*State Agency*
Office	Office of Temporary and Disability Assistance	*State Agency*
SNAP	Supplemental Nutrition Assistance Program	*Key Term*
TANF	Temporary Assistance for Needy Families	*Key Term*

Background

The Office of Temporary and Disability Assistance (Office) is responsible for supervising programs that provide temporary assistance to help needy men, women, and children. 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 the document entitled *Security Requirements for State Agencies Receiving National Directory of New Hires Data*, dated August 2018. 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 Directory information is protected and 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 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 Recommendation

We found that Office officials have taken actions to comply with the federal requirements for securing Directory data set forth in the *Security Requirements for State Agencies Receiving National Directory of New Hires Data*, and defined in the TANF and SNAP CMAs between Child Support Enforcement and the Office.

We found that the Office is fully compliant with 30 of the 32 requirements; the remaining two requirements were found to be not applicable.

For the two requirements marked as not applicable, one requirement is not applicable 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 where state agencies receiving Directory data are no longer required to submit the Security and Privacy Self-Assessment.

Recommendation

1. Continue to maintain a system of controls that ensure compliance with federal requirements for securing Directory data.

Audit Scope, Objective, 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 June 2, 2016 through March 3, 2020.

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.

Statutory Requirements

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.

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.

Reporting Requirements

We provided a draft copy of this report to Office officials for their review and comment. Their comments were considered in preparing this final report and are included in their entirety at the end of it. Office officials agreed with our recommendation and noted that they will continue their security monitoring and maintain their system controls as recommended.

Within 180 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.

Exhibit

Office of Temporary and Disability Assistance
National Directory of New Hires (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, NDNH information to authorized personnel who need 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 maintain an ongoing management oversight and quality assurance program 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 non-compliance contained in the applicable federal and state laws, including section 453(l)(2) of the Social Security Act. 42 U.S.C. § 653(l)(2).	The state agency shall advise all authorized personnel who will access NDNH information of the confidentiality of NDNH information, the safeguards required to protect NDNH information, and the civil and criminal sanctions for non-compliance contained in the applicable state and federal laws, including section 453(l)(2) of the Social Security Act. 42 U.S.C. §653(l)(2).	Compliant	

#	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, the Computer Matching and Privacy Protection Act, and other federal and state laws governing use and misuse of NDNH information.	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, the Computer Matching and Privacy Protection Act, and other state and federal laws governing use and misuse of NDNH information.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
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 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 NDNH information, the privacy and security safeguards contained in this agreement and security addendum, 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.	Compliant	
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 OCSE 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 OCSE upon request.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
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 in section VII.A of this security addendum. The requirement for the state agency to report confirmed or suspected incidents involving NDNH information to OCSE exists in addition to, not in lieu of, any state agency requirements to report to the United States Computer Emergency Readiness Team (US-CERT).	The state agency shall have appropriate procedures in place to report confirmed and suspected security or privacy incidents (unauthorized use or disclosure involving personally identifiable information), 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 OCSE, as designated in this security addendum. The requirement for the state agency to report confirmed or suspected incidents involving NDNH information to OCSE exists in addition to, not in lieu of, any state agency requirements to report to the United States Computer Emergency Readiness Team (US-CERT).	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 from the appropriate state agency representatives.	Compliant	The Office has received approval from Child Support Enforcement that their 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. See numbers 8 and 18 of this section for additional information.	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 (NAC) solution, 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 devices shall not be authorized. See numbers 8 and 19 of this section for additional information.	Compliant	The Office has received approval from Child Support Enforcement that their SSL VPN remote access solution is compliant with NDNH requirements.

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
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 that shall 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.	Compliant	
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 detailed enough for the state agency to track and report.	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 detailed enough for the state agency to track and report.	Compliant	
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.	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.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
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.	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.	Compliant	
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.	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.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
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.	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 by using technical controls or other compensating controls.	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. All electronic state agency transmissions of information shall be encrypted utilizing a FIPS 140-2 compliant product.	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. All electronic state agency transmissions of information shall be encrypted using a FIPS 140-2 compliant product.	Compliant	
17.	The state agency shall transfer and store NDNH information only on state agency-owned portable digital media and mobile computing and communications devices that are encrypted at the disk or device level, using a FIPS 140-2 compliant product. See numbers 8 and 18 of this section for additional information.	The state agency shall transfer and store NDNH information only on state agency owned portable digital media and mobile computing and communications devices that are encrypted at the disk or device level, using a FIPS 140-2 compliant product. See numbers 8 and 18 of this section for additional information.	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 computing resources resident in commercial or public facilities (for example, hotels, convention centers, airports) from accessing, transmitting, or storing NDNH information.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
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. The state agency shall control remote access through a limited number of managed access control points.	The state agency shall prohibit remote access to NDNH information, except via a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication. The state agency shall control remote access through a limited number of managed access control points.	Compliant	The Office has received approval from Child Support Enforcement that their SSL VPN remote access solution is compliant with NDNH requirements.
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 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.	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 OCSE'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 files 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 OCSE written approval. The state agency shall comply with the retention and disposition requirements in the agreement.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
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. See numbers 8, 9, and 18 of this section for additional information.	The state agency shall use 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. See numbers 8, 9, and 19 of this section for additional information.	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 from its storage media after completing authorized use in accordance with the retention and disposition requirements in the computer matching agreement (See Disposition of Matched Items in section VI of the computer matching agreement). When storage media are disposed of, the media will be destroyed or sanitized so that the erased records are not recoverable.	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 Virtual Private Network (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. See numbers 8 and 18 of this section for additional information.	The state agency shall implement a NAC solution in conjunction with a Virtual Private Network (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 agency 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. See numbers 8 and 19 of this section for additional information.	Compliant	The Office has received approval from Child Support Enforcement that their 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 this 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.	The state agency shall ensure that the organization responsible for the data processing facility storing, transmitting, or processing NDNH information complies with the security requirements established in this 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.	Compliant	
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 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.	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. 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 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. In accordance with the retention and disposition requirements in the agreement (See Disposition of Matched Items in section VI of computer matching agreement), the state agency shall destroy these printed reports by burning or by shredding with a cross-cut shredder.	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 and 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 OCSE 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 OCSE, as designated in this security addendum. The state agency is responsible for all reporting and notification activities, and associated costs of breach remediation, including but not limited to investigating the incident; communicating with required state government breach response officials; notifying individuals whose information is breached; notifying any third parties, including the media; 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; correcting the vulnerability that allowed the breach; and any other activities, as required by OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and other federal law and guidance.	**Breach and Reporting Notification Responsibility:** Upon disclosure of NDNH information from OCSE to the state agency, the state agency is the responsible party in the event of a confirmed or suspected breach of the information, including responsibility for any costs associated with breach mitigation and remediation. 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 OCSE, as designated in 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; notifying any third parties, including the media; notifying any other public and private sector agencies involved; responding to inquiries about the breach; resolving all issues surrounding the information breach; performing any follow-up activities; correcting the vulnerability that allowed the breach; and any other activity, as required by OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and other federal law and guidance.	Compliant	

#	TANF Requirement	SNAP Requirement	Compliance Level (TANF and SNAP)	Comments
31.	**Security Certification - Security Posture:** The state agency has submitted to OCSE the required documentation and OCSE has reviewed and approved the state agency's security posture.	**Security Requirement - Security Posture:** The state agency has submitted to OCSE the required documentation and OCSE 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.
32.	**Security Requirement - Independent Security Assessment:** The state agency shall submit to OCSE 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.	**Security Requirement - Independent Security Assessment:** The state agency shall submit to OCSE 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.	Compliant	

Agency Comments

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

ANDREW M. CUOMO
Governor

MICHAEL P. HEIN
Commissioner

BARBARA C. GUINN
Executive Deputy Commissioner

May 6, 2020

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

Dear Mr. Reilly:

The following is the response of the Office of Temporary and Disability Assistance (OTDA) to the Office of State Comptroller (OSC) draft report **2019-S-67** dated April 13, 2020 entitled "National Directory of New Hires Data Security."

Recommendation: Continue to maintain a system of controls that ensure compliance with federal requirements for securing directory data.

Response: OTDA agrees with this recommendation and acknowledges OSC's findings that the Office is fully compliant with 30 of the 32 federal requirements and that the remaining two requirements were not applicable. OSC also acknowledged the emphasis OTDA has placed on providing strong controls over National Directory of New Hires data. In the future, OTDA will continue our security monitoring and maintain our system controls as recommended in the report.

If you have any questions, please feel free to contact me directly.

Sincerely,

Rajni Chawla, Director
Bureau of Audit and Quality Control

cc: Michael Hein
Barbara Guinn
Krista Rock
Stephen Bach
Thomas Gosh
Lisa Schweigert
Annah Geiger

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

Contributors to Report

Executive Team

Tina Kim - *Deputy Comptroller*

Ken Shulman - *Assistant Comptroller*

Audit Team

Brian Reilly, CFE, CGFM - *Audit Director*

Nadine Morrell, CIA, CISM - *Audit Manager*

Brian Krawiecki, CIA - *Audit Supervisor*

Don Cosgrove - *Examiner-in-Charge*

Christopher Bott - *Senior Examiner*

Nicole Cappiello - *Senior Examiner*

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