# Office of Temporary and Disability Assistance

## National Directory of New Hires Data Security

Report 2023-S-43 | May 2024

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller
Division of State Government Accountability

# Audit Highlights

## Objective

To determine if the Office of Temporary and Disability Assistance has met federal requirements for securing National Directory of New Hires data. Our audit covered the period from March 2020 through January 2024.

## About the Program

The Office of Temporary and Disability Assistance (OTDA) is responsible for supervising State programs that provide assistance and support to eligible families and individuals. Two such programs administered by OTDA are the Temporary Assistance for Needy Families (TANF) and the Supplemental Nutrition Assistance Program (SNAP). As part of managing these programs, OTDA obtains National Directory of New Hires (Directory) data provided by the Office of Child Support Enforcement (OCSE), 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. OTDA uses Directory data to verify TANF and SNAP eligibility information. The identification and verification of this data helps OTDA 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 OCSE. The state agency also must comply with the *Security Requirements for State Agencies Receiving National Directory of New Hires Data* dated August 2021. 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, OTDA must submit a copy of an independent security assessment to OCSE. At the request of OTDA officials, we performed an independent security assessment of the Directory system security controls at OTDA.

## Key Findings

OTDA has taken actions to comply with the federal requirements for securing Directory data. We found that OTDA is fully compliant with 31 of the 32 requirements; the remaining requirement was found to be not applicable due to current practices at OTDA.

## Key Recommendation

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

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

May 8, 2024

Barbara C. Guinn
Acting Commissioner
Office of Temporary and Disability Assistance
40 North Pearl Street
Albany, NY 12243

Dear Acting Commissioner Guinn:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage their resources efficiently and effectively. By so doing, it provides accountability for the 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 Disability Assistance entitled *National Directory of New Hires Data Security*. This audit was performed pursuant to the State Comptroller's authority under 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** ..... 4

**Background** ..... 5

**Audit Findings and Recommendations** ..... 7

Recommendation ..... 7

**Audit Scope, Objective, and Methodology** ..... 8

**Statutory Requirements** ..... 9

Authority ..... 9

Reporting Requirements ..... 9

**Exhibit** ..... 10

**Agency Comments** ..... 19

**Contributors to Report** ..... 20

# Glossary of Terms

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

# Background

The mission of the Office of Temporary and Disability Assistance (OTDA) is to help vulnerable New Yorkers meet their essential needs and advance economically by providing opportunities for stable employment, housing, and nutrition. Two programs administered by OTDA that support this mission are 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. TANF also focuses on 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.

OTDA 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 (OCSE) owns and operates the Directory, which is comprised of information on new hires, quarterly wage, and unemployment insurance.

OCSE is responsible for ensuring the protection of Directory information, even when disclosed to state agencies. Therefore, OCSE has developed the document entitled *Security Requirements for State Agencies Receiving National Directory of New Hires Data*, dated August 2021. 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. OCSE 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, OCSE 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. OTDA has entered into two CMAs with OCSE for the receipt of the 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.

OCSE expects the state agency receiving Directory information to demonstrate its security posture before receiving Directory data and periodically thereafter. Therefore, OCSE 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 OCSE and must include detailed findings (if any) and recommendations to improve the

state agency's plans, procedures, and practices. At the request of OTDA officials, we performed an independent security assessment of the Directory system security controls at the OTDA.

# Audit Findings and Recommendations

We found that OTDA 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 OCSE and OTDA.

We found that OTDA is fully compliant with 31 of the 32 requirements; the remaining requirement was found to be not applicable. For the requirement marked as not applicable, it is not applicable because OTDA does not generate hard-copy reports containing Directory data.

## Recommendation

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

# Audit Scope, Objective, and Methodology

The objective of this audit was to determine whether OTDA has met federal requirements for securing the National Directory of New Hires data. The audit covered the period from March 2020 through January 2024.

To accomplish our objective and assess related internal controls, we audited specific security controls implemented by OTDA to comply with the federal requirements for securing Directory data. As part of our audit, we reviewed relevant OTDA security policies and configurations, records, and reports related to our audit scope. In addition, we held interviews with OTDA and ITS 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 OTDA network.

# Statutory Requirements

## Authority

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.

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. These duties could be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our professional judgment, these duties do not affect our ability to conduct this independent performance audit of OTDA's oversight and administration of security over National Directory of New Hires data.

## Reporting Requirements

We provided a draft copy of this report to OTDA 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. OTDA 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 must 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. | The state agency must 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 must 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 must 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 must 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). | The state agency must 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 | |
| 4 | The state agency must 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 must 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 must receive security and privacy awareness training before accessing NDNH information and at least annually thereafter. The training must 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. | The state agency must 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 must 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 must receive security and privacy awareness training before accessing NDNH information and at least annually thereafter. Training must 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 must 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 must 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. | The state agency personnel with authorized access to NDNH information must 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 must 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 must maintain records of authorized personnel with access to NDNH information. The records must 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 must make such records available to OCSE upon request. | The state agency must maintain records of authorized personnel with access to NDNH information. The records must 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 must make such records available to OCSE upon request. | Compliant | |
| 7 | The state agency must 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 must 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). | The state agency must 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 must 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 | |

| # | TANF Requirement | SNAP Requirement | Compliance Level (TANF and SNAP) | Comments |
|---|---|---|---|---|
| 8 | The state agency must 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 must prohibit the use of non-state agency furnished equipment to access NDNH information without specific written authorization from the appropriate state agency representatives. | Compliant | |
| 9 | The state agency must 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 must 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 must scan the state agency and non-state agency furnished equipment to ensure compliance with the state agency standards. All remote connections must be through a Network Access Control, 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. Personally owned devices must not be authorized (see numbers 8 and 19 of this section for additional information). | The state agency must 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 must 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 must scan the state agency and non-state agency furnished equipment to ensure compliance with the state agency standards. All remote connections must be through a Network Access Control, 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. Personally owned devices must not be authorized. See numbers 8 and 19 of this section for additional information. | Compliant | OTDA has received approval from OCSE that their SSL VPN solution is compliant with NDNH requirements. |
| 10 | The state agency must implement an effective continuous monitoring strategy and program that must 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 must 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 must implement an effective continuous monitoring strategy and program that must 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 must 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 | |

| # | TANF Requirement | SNAP Requirement | Compliance Level (TANF and SNAP) | Comments |
|---|---|---|---|---|
| 11 | The state agency must maintain an asset inventory of all software and hardware components within the boundary of the information system housing NDNH information. The inventory must be detailed enough for the state agency to track and report. | The state agency must maintain an asset inventory of all software and hardware components within the boundary of the information system housing NDNH information. The inventory must be detailed enough for the state agency to track and report. | Compliant | |
| 12 | The state agency must 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 must describe the responsibilities and expected behavior of all individuals who access the system. | The state agency must 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 must describe the responsibilities and expected behavior of all individuals who access the system. | Compliant | |
| 13 | The state agency must 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 must 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 must 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 must 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 must maintain a baseline configuration of the system housing NDNH information. The baseline configuration must 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 must maintain a baseline configuration of the system housing NDNH information. The baseline configuration must 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. | Complaint | |
| 15 | The state agency must 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 must prevent personnel from browsing by using technical controls or other compensating controls. | The state agency must 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 must prevent personnel from browsing by using technical controls or other compensating controls. | Compliant | |

| # | TANF Requirement | SNAP Requirement | Compliance Level (TANF and SNAP) | Comments |
|---|---|---|---|---|
| 16 | The state agency must 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 must be encrypted utilizing a FIPS 140-2 compliant product. | The state agency must 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 must be encrypted utilizing a FIPS 140-2 compliant product. | Complaint | |
| 17 | The state agency must 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 must 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 must 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. | The state agency must 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 | |
| 19 | The state agency must 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 must control remote access through a limited number of managed access control points. | The state agency must 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 must control remote access through a limited number of managed access control points. | Compliant | OTDA has received approval from OCSE that their SSL VPN solution is compliant with NDNH requirements. |
| 20 | The state agency must 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 must 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 must 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 must 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 | |

| # | TANF Requirement | SNAP Requirement | Compliance Level (TANF and SNAP) | Comments |
|---|---|---|---|---|
| 21 | The state agency must 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 60 days after completing authorized use. If the state agency requires the extract for longer than 60 days to accomplish a purpose authorized pursuant to this agreement, the state agency must request permission, in writing, to keep the extract for a defined period of time, subject to OCSE written approval. The state agency must comply with the retention and disposition requirements in the agreement. | The state agency must 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 60 days after completing authorized use. If the state agency requires the extract for longer than 60 days to accomplish a purpose authorized pursuant to this agreement, the state agency must request permission, in writing, to keep the extract for a defined period of time, subject to OCSE written approval. The state agency must comply with the retention and disposition requirements in the agreement. | Complaint | |
| 22 | The state agency must 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 19 of this section for additional information). | The state agency must 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 19 of this section for additional information. | Complaint | |
| 23 | The state agency must erase electronic records after completing authorized use in accordance with the retention and disposition requirements in the 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. | The state agency must erase electronic records after completing authorized use in accordance with the retention and disposition requirements in the 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. | Complaint | |

| # | TANF Requirement | SNAP Requirement | Compliance Level (TANF and SNAP) | Comments |
|---|---|---|---|---|
| 24 | The state agency must 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 must 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 must 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 must disable functionality that allows automatic code execution. The solution must 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). | The state agency must 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 must 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 must 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 must disable functionality that allows automatic code execution. The solution must 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. | Complaint | OTDA has received approval from OCSE that their SSL VPN solution is compliant with NDNH requirements. |
| 25 | The state agency must 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. | The state agency must 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 | |

| # | TANF Requirement | SNAP Requirement | Compliance Level (TANF and SNAP) | Comments |
|---|---|---|---|---|
| 26 | The state agency must 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. | The state agency must 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 must maintain a list of personnel authorized to access facilities and systems processing sensitive data, including NDNH information. The state agency must control access to facilities and systems wherever NDNH information is processed. Designated officials must review and approve the access list and authorization credentials initially and periodically thereafter, but no less often than annually. | The state agency must maintain a list of personnel authorized to access facilities and systems processing sensitive data, including NDNH information. The state agency must control access to facilities and systems wherever NDNH information is processed. Designated officials must review and approve the access list and authorization credentials initially and periodically thereafter, but no less often than annually. | Compliant | |
| 28 | The state agency must label printed reports containing NDNH information to denote the level of sensitivity of the information and limitations on distribution. The state agency must maintain printed reports in a locked container when not in use and must not transport NDNH information off state agency premises. In accordance with the retention and disposition requirements in the agreement, the state agency must destroy these printed reports by burning or shredding. | The state agency must label printed reports containing NDNH information to denote the level of sensitivity of the information and limitations on distribution. The state agency must maintain printed reports in a locked container when not in use and must not transport NDNH information off state agency premises. In accordance with the retention and disposition requirements in the agreement, the state agency must destroy these printed reports by burning or shredding. | Not Applicable | OTDA does not generate any printed reports containing Directory information. |
| 29 | The state agency must 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 must 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 Reporting and 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 must 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. | **Breach Reporting and 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 must 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 | |
| 31 | **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. | **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. | Compliant | OTDA demonstrated their security posture through our independent security assessment as per the *Security Requirements for State Agencies Receiving National Directory of New Hires Data*. |
| 32 | **Security Requirement – Independent Security Assessment:** The state agency must 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 must 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

KATHY HOCHUL
Governor

BARBARA C. GUINN
Commissioner

April 17, 2024

By email to: nmorrell@osc.ny.gov

Nadine Morrell
Audit Director
Office of the State Comptroller
110 State Street 11th Floor
Albany, NY 12236

Re: National Directory of New Hires (NDNH),
2023-S-043; Response to Draft Audit Report

Dear Nadine Morrell:

The following is the response from the Office of Temporary and Disability Assistance (OTDA) to the Office of the State Comptroller (OSC) draft audit report received on March 22, 2024, entitled "National Directory of New Hires Data Security."

OTDA considers the protection of data shared with us by our federal partner agencies a top priority and is pleased that OSC has acknowledged our commitment to providing strong controls over National Directory of New Hires (NDNH) data. We appreciate the determination that OTDA has fully complied with 31 of the 32 federal security requirements, with the remaining requirement deemed not applicable given the current practices in place. As recommended, OTDA will continue to maintain a system of controls that ensures compliance with federal requirements for securing NDNH data.

If you have questions or comments concerning our response to the Preliminary Report, please contact OTDA's Audit Liaison at (518) 473-6035.

Sincerely,

Rajni Chawla
First Deputy Commissioner

cc: Barbara C. Guinn, Acting Commissioner, OTDA

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

# Contributors to Report

## Executive Team

**Andrea C. Miller** - *Executive Deputy Comptroller*
**Tina Kim** - *Deputy Comptroller*
**Stephen C. Lynch** - *Assistant Comptroller*

## Audit Team

**Nadine Morrell**, CIA, CISM - *Audit Director*
**Amanda Eveleth** - *Audit Manager*
**Daniel Raczynski** - *Audit Supervisor*
**Justin Dasenbrock**, CISA, ITIL - *IT Audit Manager*
**Christopher Bott** - *IT Audit Supervisor*
**Jonathan Julca** - *Information Systems Auditor*
**Amos Odju** - *Information Systems Auditor*

**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

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