Thomas P. DiNapoli
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

May 30, 2012

Ms. Elizabeth R. Berlin
Executive Deputy Commissioner
New York State Office of Temporary and Disability Assistance
40 North Pearl Street
Albany, New York 12243

Re: Security Controls over National Directory of New Hires Data
Report 2012-S-9

Dear Commissioner Berlin:

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 audited aspects of the security controls in place over National Directory of New Hires data at the New York State Office of Temporary and Disability Assistance. Our audit covered the period February 27, 2012 through March 30, 2012.

Background

The Office of Temporary and Disability Assistance (Office) is responsible for supervising State programs that provide assistance and support to eligible families and individuals. One of these programs is the Temporary Assistance for Needy Families Program (Needy Families Program). This program provides assistance to needy families with (or expecting) children, and promotes individual responsibility and family independence. As part of managing this program, 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 national wage and employment information. The Office uses Directory data, to verify Needy Families Program eligibility information. The identification and verification of this data helps the Office close cases where assistance is not warranted; reduces the caseload and amount paid in benefits by the State through the Needy Families Program; and helps to identify and resolve any fraudulent activity by program recipients.

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 2010. These requirements define the administrative, technical, and physical security controls required to be implemented by the State agency prior to receiving Directory data.

Per the Federal requirements, the State agency receiving Directory data must submit a Security and Privacy Self Assessment that details what the agency is doing to comply with all security requirements. Also, every four years the State agency must submit to Child Support Enforcement a copy of a security assessment conducted by a group independent from the State agency.

At the request of Office officials, we performed an independent security assessment of the administrative, technical, and physical security controls over Directory data at the Office.

Results of Audit

The Office has taken sufficient actions to comply with all applicable Federal requirements for securing Directory data. This includes meeting the administrative, technical, and physical security requirements set forth by the Security Requirements for State Agencies Receiving National Directory of New Hires Data. One requirement was not applicable based on the current practices at the Office. Appendix A details Office compliance with these requirements.

Audit Scope, Objectives and Methodology

We audited specific security controls implemented by the Office to comply with the Federal requirements for securing Directory data. This audit took place from February 27, 2012 through March 30, 2012. The overall objective of our audit was to determine if the Office met all Federal security requirements for securing Directory data.

We conducted our 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

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 reviewed security over the matched Directory text files received from Child Support Enforcement, as well as the Office database to which these files are uploaded. 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.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include

operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds and other payments. In addition, the Comptroller appoints members to certain boards, commissions and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Authority

The audit was performed according to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

Major contributors to this report include Brian Reilly, Nadine Morrell, Claudia Christodoulou, Jennifer Van Tassel, and Jared Hoffman.

We wish to thank the management and staff of the Office of Temporary and Disability Assistance for the courtesy and cooperation extended to our auditors during this audit.

Very truly yours,

John Buyce, CPA, CIA, CGFM
Audit Director

cc: Tom Lukacs, Division of the Budget

Requirement Category – Administrative

Security Requirement	Compliant	Partially Compliant	Non-Compliant	Comments
The State Agency must ensure that access to and disclosure of the NDNH information will be restricted to only authorized personnel who need the NDNH information to perform their official duties as authorized by this agreement.	X			
The State Agency must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized personnel have access to NDNH information.	X			
The State Agency must ensure that all personnel who will access NDNH information are advised of the confidentiality of the results, the safeguards required to protect the results, and the civil and criminal sanctions for noncompliance contained in the applicable federal and state laws, including section 453(1) (2) of the Social Security Act. 42 U.S.C. § 653(l) (2).	X			
The State Agency must establish security awareness training for personnel that includes information about their responsibility for proper use and protection of NDNH information, and the possible sanctions for misuse. Security awareness training must occur when new personnel are hired and at least annually thereafter. All training must address the Privacy Act and other federal and state laws governing use and misuse of NDNH information.	X			
The State Agency must ensure that nondisclosure oaths, rules of behavior, or equivalent documents are signed by all personnel with authorized access to the NDNH information in accordance with the terms of this agreement. The nondisclosure oaths, rules of behavior, or equivalent documents will outline the authorized purposes for which the NDNH information may be used and the civil and criminal penalties for unauthorized use.	X			
The State Agency must maintain records of authorized personnel with access to the NDNH information. The records must contain a copy of each individual's signed nondisclosure oath, rules of behavior, or equivalent document and proof of the individual's participation in security awareness training. The State Agency must make such records available to OCSE within two working days of a request for such records.	X			
The State Agency must have appropriate procedures in place to report security or privacy incidents (unauthorized disclosure involving personal information), or suspected incidents involving NDNH information. Confirmed and suspected incidents in either electronic or physical form must be reported to the FPLS Information Systems Security Officer (ISSO) designated on this Security Addendum immediately upon discovery but in no case later than one hour after discovery. The requirement for the State Agency to report suspected incidents of NDNH information to OCSE exists in addition to, not in lieu of, any State Agency requirements to report to any other reporting agencies.	X			
The State Agency must ensure that personnel accessing NDNH information remotely (e.g., telecommuting) are still subject to the safeguarding requirements provided in this Security Addendum.	X			

Requirement Category – Technical

Security Requirement	Compliant	Partially Compliant	Non-Compliant	Comments
The State Agency must utilize and maintain technological (logical) access controls that limit access to NDNH information to only those personnel identified in the records maintained by the State Agency, pursuant to section A of this addendum, who are authorized for such access based on their official duties.	X			
The State Agency must ensure that the NDNH information will not be subject to browsing.	X			
The State Agency must ensure the transmission and storage of all NDNH data provided pursuant to this agreement in a manner that safeguards the data and prohibits unauthorized access. All data transmitted between the State Agency and OCSE must be via a mutually approved and secured data transfer method. All electronic data transmissions must be encrypted utilizing a FIPS 140-2 compliant, NIST certified product.	X			
The State Agency must prohibit NDNH information from being copied to and stored on State Agency mobile media (e.g., laptops, CD-ROMs, USB drives) unless encrypted at the disk level.	X			
The State Agency must prohibit the use of personally owned computing devices (e.g., laptops, desktops, computers, PDAs, Blackberries, IPODs, MP3 players, flash drives) and privately owned computing and communications devices resident in commercial or public facilities (e,g., hotels, convention centers, or airports) from transmitting and/or storing NDNH data.	X			The Office has received approval from the Office of Child Support Enforcement for the limited use of personally-owned computing devices with access via their SSL/VPN solution.
The State Agency must prohibit any remote access to the NDNH information unless such access occurs via a secure and encrypted (FIPS 140-2 compliant) transmission link and using two-factor authentication as required by OMB M-06-16. Remote access should be controlled through a limited number of managed access control points. If two-factor authentication cannot be provided, the state agency may submit a description, in writing, of compensating controls. OCSE must approve the use of the compensating controls in writing before remote access is allowed.	X			Although two-factor authentication is not used, the Office has received approval from the Office of Child Support Enforcement for the limited use of their SSL/VPN solution.

Requirement Category – Technical (Continued)

The State Agency must implement and maintain a fully automated audit trail system. At a minimum, data collected through the audit trail system must associate each query transaction to its initiator, capture date and time of system event, and type of event. Audit logs must capture the addition, modification, and/or deletion of data and should be regularly reviewed/analyzed for indications of inappropriate or unusual activity.	X			
The State Agency must log all computer-readable data extracts (secondary store or file with duplicate NDNH data) from any database holding NDNH data and verify each extract has been erased within two years of receipt. If the extract is still required 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, and OCSE may grant such permission in writing.	X			
The State Agency must implement a time-out function for remote access and mobile devices that require a user re-authenticate after no more than 30 minutes of inactivity.	X			

Requirement Category – Physical

Security Requirement	**Compliant**	**Partially Compliant**	**Non-Compliant**	**Comments**
The State Agency must ensure that all NDNH information provided pursuant to this agreement will be stored in an area that is physically safe from access by unauthorized personnel during duty hours as well as nonduty hours or when not in use.	X			
The State Agency must maintain a list of personnel authorized to access facilities and systems processing sensitive data, including NDNH data. Access to facilities and systems must be controlled wherever sensitive data is processed. Designated officials shall review and approve the access list and authorization credentials initially and periodically but no less often than annually.	X			
The State Agency must ensure that printed reports containing NDNH information will include a label that denotes the sensitivity of the information, and that the information will be used for official government use only. These printed reports are to be kept in a locked container when not in use and never transported off the State Agency premises. When no longer needed, these printed reports are to be destroyed by shredding or burning.	N/A			The Office prohibits printing any reports containing NDNH data.
The State Agency must ensure that locks and other protective measures are used at all physical access points (including designated entry/exit points) to prevent unauthorized access to computer and support areas containing NDNH information.	X			