



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

Division of State Government Accountability

Security and Effectiveness of the Department of Labor's Unemployment Insurance System

Office of Information Technology Services



Report 2014-S-9

February 2015

Executive Summary

Purpose

To determine whether the Department of Labor's (Department) Unemployment Insurance System is secure, operating effectively, and available to continue critical processing in the event of a disaster or mishap that disables normal processing. This audit covers the period February 12, 2014 through September 23, 2014.

Background

The New York State Office of Information Technology Services (ITS) was established in November 2012 as part of a New York State IT transformation to consolidate and merge State agencies and streamline services. ITS is responsible for providing centralized information technology (IT) services to the State and its governmental agencies. ITS' Enterprise Operations group oversees systems operations and service management, and the Enterprise Information Security Office (EISO) is responsible for oversight and coordination of security services. ITS organized 42 of the State agencies into nine clusters based on type of service provided. The Department is one of five agencies that comprise the Human Services Cluster. During the transition to ITS Enterprise-developed policies and processes, ITS is charged with ensuring proper controls are in place to protect the vast amount of personal data stored in the Department's systems, maintaining compliance with applicable security standards, and ensuring continuity of effective and efficient operations.

Key Findings

- The Unemployment Insurance System data has not yet been classified as required by current Security Policy, even though 80 of the 83 unemployment insurance applications in use by the Department have been deemed mission critical. The Security Policy indicates that all agency information should be classified on an ongoing basis based on its confidentiality, integrity, and availability.
- Almost two years after the transition of services, ITS still does not have a Service Level Agreement in place governing responsibilities and services provided to the agencies that comprise the Human Services Cluster, including the Department. Specifically, the Service Level Agreement defines mutual expectations, roles and responsibilities, service level outcomes, and financial commitments.
- Although system changes are logged, there is no indication of when these changes have been implemented, thereby reducing accountability.

Key Recommendations

- Complete the process of classifying the unemployment insurance data.
- Complete and sign the new Service Level Agreement as soon as possible.
- Maintain a completion date of all patches/changes applied to Department software to ensure the integrity of the unemployment insurance data.

Other Related Audits/Reports of Interests

[Office for Technology: Procurement and Contracting Practices \(2010-S-71\)](#)

[Office of Information Technology Services: Procurement and Contracting Practices \(2013-F-24\)](#)

**State of New York
Office of the State Comptroller**

Division of State Government Accountability

February 24, 2015

Ms. Margaret Miller
NYS Chief Information Officer
Office of Information Technology Services
Empire State Plaza
P.O. Box 2062
Albany, NY 12220

Dear Ms. Miller:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage government resources efficiently and effectively and, by so doing, providing accountability for tax dollars spent to support government-funded services and 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 entitled *Security and Effectiveness of the Department of Labor's Unemployment Insurance System*. 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 draft report, please feel free to contact us.

Respectfully submitted,

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

Table of Contents

Background	5
Audit Findings and Recommendations	7
Data Classification	7
Service Level Agreement	8
Ease and Efficiency	8
User Access Management	9
Software Patching and Change Management	10
Disaster Recovery and Business Continuity	10
Recommendations	10
Audit Scope and Methodology	11
Authority	11
Reporting Requirements	12
Contributors to This Report	13
Agency Comments	14

State Government Accountability Contact Information:

Audit Director: John Buyce

Phone: (518) 474-3271

Email: StateGovernmentAccountability@osc.state.ny.us

Address:

Office of the State Comptroller
 Division of State Government Accountability
 110 State Street, 11th Floor
 Albany, NY 12236

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

Background

The Office of Information Technology Services (ITS) was established in November 2012 as part of a New York State IT transformation to consolidate and merge State agencies and streamline services. ITS is responsible for providing centralized information technology (IT) services to the State and its governmental agencies, combining talent and assets from various agencies to foster innovation, build skills, and promote development in order to meet customer needs. To achieve this, ITS organized the IT employees from 42 State agencies, accounting for more than 4,000 employees, into nine clusters based on type of services provided: Environment and Energy, Financial, Administrative and General Services, General Government, Health, Human Services, Behavioral Health, Public Safety, and Transportation and Economic Development. ITS' objectives include consolidating cluster infrastructure operations for each agency cluster and improving cluster effectiveness and integration.

ITS is headed by a Chief Information Officer, who governs statewide IT strategic direction, policy, and provision of services. ITS' Enterprise Operations group oversees systems operations and service management for each cluster, and the Enterprise Information Security Office (EISO) is responsible for oversight and coordination of security services. EISO has assumed the functions, powers, and duties of the former Office of Cyber Security and Critical Infrastructure Coordination (CSCIC), including governance, compliance and risk management, incident response and digital forensics, security monitoring and intelligence, vulnerability and threat management, secure systems engineering and architecture, security training and awareness, and cluster security services. In addition, the EISO is responsible for setting statewide security policies and developing standards for use by all State agencies. The EISO is revising the Cyber Security Policies (Security Policy) currently in effect, issued by the former CSCIC, in order to establish baseline standards and policies with which all clusters' policies must align. ITS standards and policies will follow the framework of the National Institute of Standards and Technology.

The Department of Labor (Department) is one of five agencies that comprise the Human Services Cluster (Cluster). The Department's mission is to protect workers, assist the unemployed, and connect job seekers to jobs. The Department also protects the safety and health of workers and the public, and helps the unemployed via temporary payments called unemployment insurance. The Department relies heavily on IT to accomplish its mission, including such core systems as the Unemployment Insurance System. The Unemployment Insurance System allows for temporary income for eligible workers who lose their jobs through no fault of their own. To accomplish its mission, the Department uses 182 computer applications, of which about 83 are used for the Unemployment Insurance System.

During the transition to ITS Enterprise-developed policies and processes, ITS is charged with ensuring proper controls are in place to protect the vast amount of personal data stored in Department systems, maintain compliance with applicable security standards, and ensure continuity of effective and efficient operations.

Cluster management issued a strategic plan outlining and prioritizing Cluster-wide initiatives. This plan also outlines the Cluster's planning and governance processes, summarizes the long-term vision and resource constraints, and describes the various investments planned. Department officials remain responsible for the administration of the Department's Business Continuity planning.

Audit Findings and Recommendations

To determine whether the Department's Unemployment Insurance System is secure, operating effectively, and available to continue critical processing in the event of a disaster or mishap, we evaluated a range of system controls, including compliance with security standards, access management, change management, and system uptime. We identified areas – specifically data classification and user access management – in need of improvement. We also found that ITS and the Human Services Cluster do not have a Service Level Agreement (SLA) outlining responsibilities since the transformation began. Further, ITS officials need to continue to move forward with their short- and long-term succession planning to address impending constraints ITS faces with the older programming languages used. We also examined system uptime to determine the stability of the systems used to process Department transactions and found that ITS systems satisfactorily address this issue. We also evaluated disaster recovery and business continuity processes and found these areas to be working as expected.

In our previous audit of ITS – *Security and Effectiveness of Department of Motor Vehicles' Licensing and Registration Systems* (2013-S-58, issued in September 2014) – we noted that, before the transformation began, ITS did not conduct an underlying risk assessment to identify potential policy conflicts or other procedural issues among agencies, which could thereby assist with a smooth transition. Further, throughout the previous audit, we found that Cluster officials were not always able to answer our questions or direct us to knowledgeable individuals familiar with our audit areas in a timely manner. During this current audit related to the Department, we found similar conditions.

Data Classification

We found the Unemployment Insurance System data has not yet been classified as required by the Security Policy, even though 80 of the 83 unemployment insurance applications in use by the Department have been deemed mission critical.

The Security Policy indicates that all agency information should be classified on an ongoing basis based on its confidentiality, integrity, and availability. Further, Standard PS08-001, Information Classification and Control notes that:

- All information assets must have an information owner established;
- Each classification will have an approved set or range of controls;
- An information asset must be classified based on its highest level necessitated by its individual data elements;
- All personal, private, or sensitive information will be classified with a confidentiality level of high; and
- A written or electronic inventory of all State entities' information assets must be maintained.

According to ITS officials, the determination of which applications were mission critical was based on ITS' experience working with the business to support their applications. However, without classifying all the data residing on its network, management has no assurance that they are adequately protecting all of the Department's unemployment insurance data.

In response to our preliminary findings, ITS officials noted that ITS and Department business officials are working on a glossary of business terms for the unemployment insurance data and the ISO will classify the data after this process is complete. Officials expected the data to be classified by the end of 2014.

Service Level Agreement

The Cluster and ITS do not have a current SLA in place, almost two years after the start of the transition. According to the ITS website, "The Service Level Agreement (SLA) between CIO/OFT (ITS) and the Cluster defines our mutual expectations, roles and responsibilities, service level outcomes, and financial commitments."

The last SLA is between the Department and the former Office for Technology (OFT) in the form of a memorandum signed November 9, 2010. This documents the Department's agreement with the core SLA document describing all the services the former CIO/OFT would provide, including pricing and performance measures for all services. In addition, according to the Cluster Strategic Plan draft for 2014-15, Cluster teams will continue to support and maintain agency applications as agreed to in the draft SLAs with each individual agency within the Cluster. Internal processes and practices will be refined throughout the year to ensure that Cluster staff continue to provide effective and efficient service to their varied customers.

However, as the IT transition has evolved, numerous changes have occurred within ITS, and without an updated SLA that reflects these changes and describes them in detail, there is no assurance that the Cluster agencies, including the Department, are receiving the services they need or want.

In response to our preliminary findings, ITS officials indicated they are working with the Cluster agencies toward a complete and detailed SLA, and noted this will require assent from both parties.

Ease and Efficiency

The Department stores all unemployment insurance data on its mainframe, which was programmed primarily using the older programming languages Assembler, PL/1, and COBOL. According to ITS officials, these languages are currently still supported. The pool of individuals who are proficient in Assembler and PL/1 is small. To ensure the Department's mainframe operates without interruption due to this diminishing resource, it is essential that ITS have a succession plan in place to address impending constraints.

The unit leader informed us that, of the 53 staff who work on the Unemployment Insurance

System, very few know Assembler or PL/1, and the unit leader requests help from different IT areas if the need arises. This deficiency was identified in the Department's December 2013 Disaster Recovery Testing of the Unemployment Insurance System, which stated: "Due to staff unavailability, it became evident during the testing process that some technical aspects are known to only one person. The knowledge base needs to be expanded via: a) employee cross training, b) better documentation, and c) defined succession plan for responsibilities."

In response to our preliminary findings, ITS officials noted there are about 85 programs written in Assembler and PL/1, and they believe they have an adequate number of staff that can be leveraged should the programs need to be changed. In addition, ITS cited both a short-term (less than 5 years) and a long-term (more than 5 years) succession plan for the Department, as follows:

- The short-term plan is to partner with the Office of Temporary and Disability Assistance and issue a Request for Proposal to procure skilled COBOL resources should ITS be unable to support the Department's legacy COBOL applications with State staff. This RFP is currently in draft form.
- The long-term plan is to modernize the Department's unemployment insurance systems and eliminate the Department's dependency on its legacy mainframe applications.

We encourage ITS officials to routinely review their ability to support these older languages and continue to move forward to ensure they have sufficient and timely resources available for their processes.

User Access Management

The Department uses a mainframe and a database for its Unemployment Insurance System. All user access rights must be approved by ITS' Information Resource Representative (IRR). Managers request user rights on behalf of their staff and each year must submit a provisioning/deprovisioning form to notify the IRR of any changes in user access. We tested employees' access to determine whether user access is accurate and appropriate.

Appropriate Access

We judgmentally selected 10 users who have access to the mainframe to see if they have the appropriate access. Three of the 10 users had access to applications that were no longer needed. Officials removed the unneeded access immediately.

We also selected 10 users who had open accounts with approved access to the Unemployment Insurance database, which contains some sensitive information. Only 2 of the 10 had a justification as to why they needed access. We were unable to determine whether access was appropriate for the remaining eight.

In response to our preliminary findings, officials noted that they are in the process of creating a new database report of active accounts, which will enable them to review the accounts more frequently and determine appropriateness.

Unemployment Insurance Database

There are a total of 19 accounts created for the Unemployment Insurance Benefit Production database. Eight (42.11%) of the 19 accounts were never logged into, never locked, and never expired. Of these eight, seven (87.5%) had an “open” account status. In response to our preliminary findings, officials noted that they do not believe there is a security concern with this because the “password” is expired upon creation. The expiration date column can’t be populated with a date until a successful log-in occurs. ITS states that the database unit will generate a new report of new accounts with no log-in for itself to address these accounts. We contend that these individuals may not need these accounts and should be removed.

Software Patching and Change Management

According to ITS policy, the maintenance of State entity-developed software must be logged to ensure changes are authorized, tested, and accepted by management.

We found ITS does have a log of changes to the Unemployment Insurance System. However, the log contains no indication of when changes are completed. ITS officials noted they believe the date in the “deadline date” field is the same as the completion/implementation date; however, there is no supporting documentation to show that the changes/patches to the Unemployment Insurance System software/applications were completed or implemented. In response to our inquiries, ITS officials stated that, going forward, they will start entering a completion date.

Disaster Recovery and Business Continuity

Our tests showed the Department’s Business Continuity planning processes are comprehensive and complete. We also found ITS’ Disaster Recovery process properly includes testing of the mainframe and supporting servers that process unemployment insurance data. The audit team found these tests are being conducted. We noted that the location and condition of the current data center which houses the Department’s mainframe and supporting servers have some minor physical control weaknesses. However, the Department plans to relocate to a new data center, and this move should address these physical weaknesses. The planned move is scheduled for completion before the end of 2014.

Recommendations

1. Complete the process of classifying the unemployment insurance data.
2. Complete and sign the new Service Level Agreement as soon as possible.

3. Develop and implement a succession plan, including Assembler and COBOL program languages training, to ensure continuity of Department operations and service.
4. Ensure user accounts and access are reviewed for appropriateness on a regular basis.
5. Going forward, maintain a completion date of all patches/changes applied to Department software to ensure the integrity of the unemployment insurance data.

Audit Scope and Methodology

We audited the security, effectiveness, and long-term sustainability of core Department IT systems at ITS for the period February 12, 2014 through September 23, 2014. The objective of our audit was to determine whether the Department's Unemployment Insurance System is secure, operating effectively, and available to continue processing in the event of a disaster or mishap that disables normal processing.

To accomplish our objective and determine whether associated internal controls are adequate, we interviewed selected ITS and Department officials and staff to obtain an understanding of ITS Enterprise, Cluster, and Department policies and procedures. To complete our audit work, we reviewed supporting documentation for data classification, user access, change management, business continuity, disaster recovery, and uptime in order to determine compliance with established policies. We also made visits to data center locations.

We conducted our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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

Authority

The audit was performed 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.

Reporting Requirements

We provided a draft copy of this report to ITS officials for their review and comment. We considered their comments in preparing this report and have included them in their entirety at the end of it. ITS officials generally concurred with our report's recommendations and indicated that certain actions have been and will be taken to address them.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Chief Information Officer 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 recommendations contained herein, and if the recommendations were not implemented, the reasons why.

Contributors to This Report

John Buyce, CPA, CIA, CFE, CGFM, Audit Director
Brian Reilly, CFE, CGFM, Audit Manager
Nadine Morrell, CISM, CIA, CGAP, Audit Supervisor
Michel Turmel, Examiner-in-Charge
Kelly Evers Engel, Staff Examiner
Patrick Lance, Staff Examiner
Dylan Spring, Staff Examiner
Marzie McCoy, Senior Editor

Division of State Government Accountability

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

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

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

Vision

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

Mission

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

Agency Comments



ANDREW M. CUOMO
Governor

Empire State Plaza
P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

MARGARET MILLER
NYS Chief Information Officer
Director, Office of IT Services

December 9, 2014

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

Re: Audit Report 2014-S-9

Dear Mr. Buyce:

In regards to your Draft Audit Report 2014-S-9 issued by the Office of the State Comptroller (OSC), which covers the results of your audit on the Security and Effectiveness of the Department of Labor's Unemployment Insurance System, please find our written response from ITS's viewpoint for your consideration. Please feel free to contact me for any questions or clarifications.

Sincerely,

A handwritten signature in blue ink that reads 'Theresa Papa'.

Theresa Papa
Director of Administration

Office of Information Technology (ITS) Response to:

Office of Information Technology Services/Department of Labor
Security and Effectiveness of DOL's Unemployment Insurance System
Audit Report 2014-S-9
Draft Report

Recommendation:

1. Complete the process of classifying the Unemployment Insurance data.

ITS Response:

The Office of Information Technology Services (ITS) is in agreement with the Office of the State Comptroller's findings.

New York State information security policy, as noted by OSC, requires each State entity to classify all information according to its confidentiality, integrity and availability. Classification of information helps protect the information that the Department of Labor (DOL) uses and maintains to serve its customers.

The Department of Labor has made progress in classifying its information. In recent years, data classification (DC) projects were funded by grants from the United States Department of Labor (USDOL). The federal grants allowed for a consultant to be dedicated to DC activities. Because the grants were of a limited duration, DOL was unable to fully classify all data. Although data classification is not currently funded by a federal grant, USDOL continues to monitor the Department's progress for compliance with federal security standards.

DOL is proceeding with data classification, using DOL program unit staff, with consultation provided by ITS's Information Security Office. As an on-going project, information assets are being classified at the database field level. DOL plans to create a Data Dictionary for DOL staff to reference a business glossary with data classification for information assets. During 2014, the Unemployment Insurance Division initiated a project to classify data for the Employer Rating applications. Accordingly, project staff discussed the sensitivity of data that comprise the applications, and reviewed security methods that protect personal, private and sensitive information (PPSI).

DOL's information owners are aware of their responsibilities for making classification and control decisions regarding use of their information. Data is protected through adherence to

DOL policy and procedure, which is available for reference by all staff on the Agency's Intranet. Questions about access, use, release, storage, and retention of data classified at the high confidential level are addressed by DOL managers. Proper use of such information is also supported by DOL's information security awareness and training program, and through consultation with the ITS Human Services Cluster (Cluster) Information Security Office. Should PPSI be misused, lost, or breached, DOL staff will report the security incident according to established procedure in order to assist in the containment, investigation, notification and mitigation concerning the incident.

The Office of Information Technology Services, as custodian for DOL information that is maintained in ITS computer systems, follows state security policy. This also helps protect data which is classified as personal, private, and sensitive.

Recommendation:

2. Complete and sign the Service Level Agreement as soon as possible.

ITS Response:

ITS is in agreement with the Office of the State Comptroller's findings.

ITS continues to work with the Human Services Cluster agencies towards a complete and detailed SLA. This will require assent from both parties which ITS is working towards.

Recommendation:

3. Develop and implement a succession plan, including Assembler and COBOL program languages training, to ensure continuity of DOL operations and service.

ITS Response:

ITS is actively working on succession planning for the Legacy area that maintains the Unemployment Insurance system:

- For the past several years the IT division at the Department of Labor had been operating in a period of attrition and was unable to hire new staff to backfill items. The ITS/DOL Legacy team is now actively recruiting staff to backfill some of the positions lost.

- ITS/DOL makes every attempt to cross train staff in the Legacy area so they are best able to support DOL users. ITS/DOL will continue to re-allocate developer resources when necessary so that knowledge transfer can take place when staff are planning to retire or leave.
- ITS/DOL has both a short term (less than 5 years) and a long term (more than 5 years) succession plan:
 - The short term plan is to continue to hire staff to backfill staff lost through attrition, and train staff to become proficient in the older technologies. In addition, ITS/DOL will partner with other agencies in the Cluster to leverage staff augmentation contract/procurement vehicles to acquire skilled COBOL resources should ITS state staff become unable to support DOL's legacy systems.
 - The long term plan is to modernize DOL's UI systems and eliminate DOL's dependency on its legacy mainframe applications.

Recommendation:

4. Ensure user accounts and access are reviewed for appropriateness on a regular basis.

ITS Response:

ITS currently has a sound process in place for user access control by way of the Information Resource Representative (IRR) system. With the IRR process:

- ITS Service Desk staff receives User Access Management change requests from all Division Information Resource Representatives (IRRs), not just the ITS IRR. To that end, it is the responsibility of the user's supervisor to alert their Division IRRs of any needed User Access Management changes. This is clearly defined in DOL's General Administration Manual, which is shared with all DOL. Once the IRR notifies the ITS Service Desk of the requested change via a Service Request, the Service Desk will complete the change and close the Request.
- ITS Service Desk Staff also perform a check of the Department's employee separations on a bi-weekly basis.
 - The DOL Personnel office generates a list of employee separations and provides it to ITS Service Desk staff. This is a list of HR transactions including: employee transfers to other State agencies; employee deaths; employee retirements; employee separations from State service.
 - ITS Service Desk staff cross reference employees designated on this list with active user accounts and open Service Requests to ensure access is either disabled or in the process of being disabled.
 - If there is an active user account, and there is no open Service Request to remove the account, Service Desk staff immediately creates a Service Request to

remove the access. The process to remove the access is not done unilaterally, and the user's Division IRR is contacted to verify that the account is properly modified and grant the Service Desk approval to terminate the user access. Once IRR approval is received, the account is terminated.

Going forward, the ITS Service Desk will periodically provide IRRs a report to review user account access.

Recommendation:

5. Going forward, maintain a completion date of all patches/changes applied to Department software to ensure the integrity of the Unemployment Insurance data.

ITS Response:

ITS currently has a complete and viable change management process in place that provides adequate controls of changes made to UI information systems and software. The processes for mainframe and open systems changes are:

- All requests for changes to a UI application are initiated with a programming request submitted in FootPrints. These requests for changes include both mainframe and open-system applications. ITS staff hold bi-weekly meetings with DOL management representatives from both the Employer and Benefits domains where the requests are discussed, prioritized, scheduled to be worked, and closed when complete. Each time a comment is added to a request, or the status is changed (submitted, postponed, in-progress etc.) an email is generated by FootPrints to the submitter of the request and everyone that is copied on the request.
- All changes to UI open system applications are scheduled for release with an A-Info ticket opened in FootPrints after approval from UI management during the change control process. Regular releases are scheduled at least a week in advance and are discussed at the weekly release management meeting. Code releases occur during regular maintenance windows, Wednesday and Friday mornings. Emergency releases can be scheduled outside of the regular maintenance cycle with senior management approval.

Going forward, ITS staff will include a completion date on all change requests before closing them.