NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Charlie Janssen
State Auditor

Charlie.Janssen@nebraska.gov
PO Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
www.auditors.nebraska.gov

January 23, 2018

John Albin, Commissioner
Nebraska Department of Labor
550 South 16th Street
Lincoln, Nebraska 68509

Dear Commissioner Albin:

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the State of Nebraska (State) as of and for the year ended June 30, 2017, in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, we have issued our report thereon dated December 14, 2017. In planning and performing our audit, we considered the State's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements of the State, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

In connection with our audit described above, we noted certain internal control or compliance matters related to the activities of the Nebraska Department of Labor (Department) or other operational matters that are presented below for your consideration. These comments and recommendations, which have been discussed with the appropriate members of the Department's management, are intended to improve internal control or result in other operating efficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

Our consideration of internal control included a review of prior-year comments and recommendations. To the extent the situations that prompted the recommendations in the prior year still exist, they have been incorporated in the comments presented for the current year. All other prior-year comments and recommendations (if applicable) have been satisfactorily resolved.

Our consideration of internal control was for the limited purpose described in the first paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies. Given these limitations during our audit, we did not identify any deficiencies in internal control that we consider to be material weaknesses or significant deficiencies. However, material weaknesses or significant deficiencies may exist that were not identified.

Draft copies of this letter were furnished to the Department to provide management with an opportunity to review and to respond to the comments and recommendations contained herein. All formal responses received have been incorporated into this letter. Responses have been objectively evaluated and recognized, as appropriate, in the letter. Responses that indicate corrective action has been taken were not verified at this time, but they will be verified in the next audit.

The following are our comments and recommendations for the year ended June 30, 2017.

1. Allowance for Doubtful Accounts Contribution Receivable

The Department reported a balance of $481,490 in receivables due from employers for unemployment insurance taxes based upon wages for March 2017 and prior. The Department did not perform a calculation to estimate an uncollectible amount. Additionally, the Department reported that $12,699,992 was due from employers for unemployment taxes based upon wages for April through June 2017. Likewise, the Department did not calculate an estimate to determine how much of this amount was uncollectible.

A good internal control plan and sound business practices require procedures to ensure information used to compile financial statements is complete and accurate.

When adequate procedures are not in place to ensure the completeness and accuracy of financial information used to compile the financial statements, there is a greater risk that material misstatements may occur and remain undetected.

A similar finding was noted during the previous audit.

> We recommend the Department implement procedures to estimate how much of the receivables are uncollectible in order to ensure receivables are not overstated in the State's financial statements.

Department Response: Members of Finance and Tax will meet to devise a way to estimate this amount since the current system cannot provide all the data necessary. The new combined Tax/Benefit system should help to remedy this in the future.

2. Annual Review of Users/Terminated Users

During a review of users with access to the Department's Tax Management System (TMS) and Benefit Payment System (BPS), it was noted that the Department did not perform a periodic review of users with access to either application. During a review of user listings, we noted two terminated employees still had user access to BPS, and one terminated employee still had user access to NEworks. During a separate test of terminated application users, we also noted another former employee's access to NEworks was not removed timely. At the time of testing, terminated users had retained access from 9 to 365 business days after their termination dates.

Nebraska Information Technology Commission (NITC) Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.7.2, User Account Management, states the following:

> *A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (read, write, delete, etc.). The "Principle of Least Privilege" should be used to ensure that only authorized individuals have access to applications and information and that these users only have access to the resources required for the normal performance of their job responsibilities . . . . Agencies or data owner(s) should perform annual user reviews of access and appropriate privileges.*

Failure to review periodically user access to applications and to remove terminated users timely creates the opportunity for inappropriate access to State resources.

> We recommend the Department implement procedures to periodically review, at a minimum annually, user access to its applications. We also recommend the Department implement procedures to ensure user access is disabled or deleted within three business days of a user's termination.

Department Response: We recently undertook a significant review of our procedures in this area and implemented several changes regarding access to data in our information systems.

The "UI Security Procedure-Access Rights Termination at Separation" procedure became effective 1/1/2018 and the "UI Security Procedure-BPS Usage Review Procedures" became effective on 12/8/2017. These procedures are available for your inspection.

We are in the process of drafting a new procedure to address the ongoing review of individuals who access the Mainframe System and it should be available by the end of January.

In terms of NEworks, removal requests are processed the same day they are received. In addition to manual deactivation of NEworks accounts, staff users with a temporary assignment are set up with a future deactivation date/time defined in their NEworks account and their access is automatically terminated if they log-in beyond that date and time.

3. Business Continuity Plan

During a review of the Agency's Business Continuity Plan, we noted the plan had not been updated since 2012.

A good business continuity plan, which may encompasses disaster recovery planning, includes making available reliable and useful information for decision making when faced with a disaster or other event causing or creating the potential for a loss of business continuity. A good business continuity plan also includes regular testing and updating of the plan.

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.3.2, Agency Accountability, states, in relevant part, the following:

> *To ensure interruptions to normal agency business operations are minimized and critical agency business applications and processes are protected from the effects of major failures, each agency, in cooperation with the Chief Information Officer, must develop disaster recovery and business continuity plans that meet the recovery requirements defined by the agency.*

NITC Standards and Guidelines, Information Technology Disaster Recovery Plan Standard 8-201 (August 2006), states in relevant part:

> *Each agency must have an Information Technology Disaster Recovery Plan that supports the resumption and continuity of computer systems and services in the event of a disaster. The plan will cover processes, procedures, and provide contingencies to restore operations of critical systems and services as prioritized by each agency. The Disaster Recovery Plan for Information Technology may be a subset of a comprehensive Agency Business Resumption Plan which should include catastrophic situations and long-term disruptions to agency operations.*
>
> *The Information Technology Disaster Recovery Plan should be effective, yet commensurate with the risks involved for each agency. The following elements, at a minimum, must be included:*
>
> - *Identification of critical computer systems and services to the agency's mission and business functions.*
> - *Critical systems and services preservation processes and offsite storage strategy and methods to protect storage media.*
> - *Documented dependencies upon other State agency's or entities that support critical systems and services.*
> - *Contingency plans for different types of disruptions to critical systems and services, i.e. hardware failure, etc.*
> - *Information technology responsibilities for implementation and disaster management.*
> - *Procedures for reporting events, as well as escalating an event within an agency.*
> - *Identification of copy distribution and multiple site storage of plan documents.*
> - *Multi-year training, exercising, and improvement plans.*
> - *Annual plan review, revision, and approval process.*

When the Business Continuity Plan is not reviewed and updated periodically, reliable and useful information may not be available when a disaster or other business interruption occurs, increasing the risk of extended downtime.

> We recommend the Department implement procedures to review annually and to update the information contained in its Business Continuity Plan.

Department Response: NDOL has worked with DAS to develop a comprehensive and State integrated Continuity of Operations Plan (COOP) to be finalized in 2018, which includes an Information Technology Disaster Recovery Plan. Section V-2 of the proposed plan addresses an annual review by the NDOL Continuity Program Manager as well as a complete review of functions and continuity of operations to be conducted by the NDOL-COOP Work Group every four years. The NDOL Continuity Program Manager will provide the Continuity Administrator with a summary of the yearly review process and a copy of the revised plan once approved. NDOL staff shall be informed of changes made to continuity of operations procedures after plan revisions and during annual refresher training.

4. Review of Users with Access to TMS and BPS Database Tables

During a review of Tax Management System (TMS) and Benefit Payment System (BPS) database tables containing significant financial information, we noted the Department did not conduct a periodic review of users with access to those database tables. We noted users from the

Department of Health and Human Services (DHHS), the Supreme Court, and the Office of the Chief Information Officer (OCIO) were members of groups with access to these database tables. A documented review would allow the Department to be aware of all users with access to these database tables, to restrict access to only Department employees who require access to fulfill their job duties, and to verify that users employed by other agencies still require access. We noted 30 OCIO, 1 Supreme Court, and 4 DHHS users had access to one or more significant database tables.

NITC Standards and Guidelines, Information Security Policy 8-101 (December 2013), Section 4.7.2, User Account Management, states, in relevant part, the following:

> *A user account management process will be established and documented to identify all functions of user account management, to include the creation, distribution, modification and deletion of user accounts. Data owner(s) are responsible for determining who should have access to information and the appropriate access privileges (read, write, delete, etc.). The "Principle of Least Privilege" should be used to ensure that only authorized individuals have access to applications and information and that these users only have access to the resources required for the normal performance of their job responsibilities . . . . Agencies or data owner (s) should perform annual user reviews of access and appropriate privileges.*

When user database access is not periodically reviewed and terminated users are not removed timely, it creates the opportunity for inappropriate access to State resources.

> We recommend the Department implement procedures to review periodically user access to the database tables with sensitive TMS and BPS information. We also recommend the Department periodically review user access with other agencies to ensure only users requiring access to Department resources have such access.

Department Response: Please see response to item 2 regarding changes to procedures for removing terminated users. In regards to database access by other agencies, OCIO has access for system support purposes, and we have contracts in place with HHS and the Supreme Court allowing access.

* * * * *

Our audit procedures are designed primarily on a test basis and, therefore, may not bring to light all weaknesses in policies or procedures that may exist. Our objective is, however, to use our knowledge of the Department and its interaction with other State agencies and administrative departments gained during our work to make comments and suggestions that we hope will be useful to the Department.

This communication is intended solely for the information and use of the Department, the Governor and State Legislature, others within the Department, Federal awarding agencies, pass-through entities, and management of the State of Nebraska and is not intended to be, and should not be, used by anyone other than the specified parties. However, this communication is a matter of public record, and its distribution is not limited.

Philip J. Olsen, CPA, CISA
Audit Manager