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
auditors.nebraska.gov

July 30, 2021

John R. Selmer, Director
Nebraska Department of Transportation
1500 Nebraska Hwy 2
Lincoln, Nebraska 68502

Dear Mr. Selmer:

This letter is provided pursuant to AICPA Auditing Standards AU-C Section 265B.A17, which permits the early communication of audit findings due to their significance and the urgent need for corrective action. The audit work addressed herein was performed as part of the fiscal year ended June 30, 2021, Annual Comprehensive Financial Report (ACFR) audit. This communication is based on our audit procedures through June 30, 2021. Because we have not completed our audit of the fiscal year 2021 ACFR, additional matters may be identified and communicated in our final report.

In planning and performing our audit of the State's financial statements as of and for the year ended June 30, 2021, in accordance with auditing standards generally accepted in the United States of America, we considered the State's internal control over financial reporting (internal control) as a basis for designing the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, 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.

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 was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified.

We noted certain internal control or compliance matters related to the activities of the Department, or other operational matters, which are presented below for your consideration. The following comment and recommendation, which has been discussed with the appropriate members of the agencies and their management, are intended to improve internal control or result in other operating efficiencies.

Draft copies of this letter were furnished to the Department to provide management with an opportunity to review and to respond to the comment and recommendation contained herein. Any formal response received has been incorporated into this letter. Such response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, the auditor does not express an opinion on it. Such response has been objectively evaluated and recognized, as appropriate, in the letter. A response that indicates corrective action has been taken was not verified at this time, but it will be verified in the next audit.

The following is our comment and recommendation for the year ended June 30, 2021.

NITC Information Security Policy

The Nebraska Information Technology Commission's (NITC) nine members are appointed by the Governor with the approval of the Legislature. Neb. Rev. Stat. § 86-516(6) (Reissue 2014) directs the NITC to "[a]dopt minimum technical standards, guidelines, and architectures upon recommendation by the technical panel."

NITC Technical Standards and Guidelines, Information Security Policy 8-209 (July 2017), "State and agency security planning and reporting," requires State agencies to have an Information Security Plan, a System Security Plan, and a Plan of Action and Milestones Report on file. The NITC has established specific elements to be included in its Information Security Strategic Plan (8-210), System Security Plan (8-211), and Plan of Action and Milestones Report (8-212).

As a result, the Auditor of Public Accounts (APA) tested some of the key elements of those NITC Technical Standards and Guidelines to verify compliance by the Department. Though having various documents that contained some of the necessary elements, the Department lacked documentation to support that it met all required elements, as described below.

The APA noted that the Department did not have a summary of the overall information risk assessments and current risk levels, detailed descriptions of significant security risks, and plans to mitigate or remediate those risks, as required in 8-210.

The APA noted also that none of the significant requirements set out in 8-211 were met.

For risks and findings identified by the APA in a prior-year audit and for any risks identified by the Department through its own internal and external assessments, if any, the Department lacked a Plan of Action & Milestones Report (8-212).

During the fiscal year ended June 30, 2021, the Department lacked formal plans that describe fully the current controls in place for protecting information at a level commensurate with the sensitivity level of the Department's systems. A similar finding was noted during the previous audit.

On July 8, 2021, the NITC significantly changed the aforementioned policies. NITC Information Security Policy 8-209 now reads as follows:

> *Pursuant to the terms of certain federal data exchange agreements, state agencies may be required to maintain the following documentation:*
>
> *(1) Information security strategic plan (section 8-210);*
> *(2) System security plan (section 8-211); and*
> *(3) Other information security*
>
> *For agencies not subject to federal data exchange agreements, these planning documents are considered guidelines and recommended as best practice.*

The revised policy 8-209 eliminates the prior requirement for maintenance of a Plan of Action & Milestones Report (8-212). During the fiscal year ended June 30, 2021, the Department did not have any Federal data exchange agreements requiring the documentation identified in 8-209.

> While there have been significant changes to the NITC Technical Standards and Guidelines with regard to security planning and reporting, we continue to recommend that the Department review the revisions and formally document compliance with these updated requirements, specifically formally documenting a risk assessment and tracking how the Department is addressing those risks, even if not required by Federal data exchange agreements, as the NITC still recommends this as best practice.

Department Response: As a result of last year's recommendation, "We recommend the Department work with the Office of the Chief Information Officer to satisfy the requirements of the NITC Information Security Policy.", NDOT engaged and worked with the OCIO, NITC, and its advisory groups to have the referenced NITC policies revised to reflect current responsibilities, as modified by the State's IT consolidation processes.

These policies were officially adopted by the NITC on July 8th, 2021. These updates no longer require NDOT to develop an agency specific Information Security Strategic Plan (8-210), System Security Plan (8-211), and Plan of Action and Milestones Report (8-212).

NDOT appreciates the recommendation to formally document a risk assessment and track how we're addressing those risks. NDOT will work with the OCIO to identify if it is appropriate for NDOT to monitor and address risks in addition to what is being done to secure State systems by the OCIO.

* * * * * *

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 suitable for any other purpose. However, this communication is a matter of public record, and its distribution is not limited.

Zachary Wells, CPA, CISA
Audit Manager