



Unemployment Insurance System

Information Technology Performance Audit

May 2024

Financial Audit Division

Office of the Legislative Auditor

State of Minnesota

Financial Audit Division

The division has authority to audit organizations and programs in the state's executive and judicial branches, metropolitan agencies, several "semi-state" organizations, state-funded higher education institutions, and state-funded programs operated by private organizations.

Each year, the division selects several of these organizations and programs to audit. The audits examine the policies and procedures—called internal controls—of the organizations to ensure they are safeguarding public resources and complying with laws that govern their financial and program operations. In addition, the division annually audits the State of Minnesota's financial statements and the financial statements of three state public pension systems. The primary objective of these financial audits is to assess whether the statements fairly present the organization's financial position according to Generally Accepted Accounting Principles.

The Office of the Legislative Auditor (OLA) also has a Program Evaluation Division. The Program Evaluation Division's mission is to determine the degree to which state agencies and programs are accomplishing their goals and objectives and utilizing resources efficiently.

OLA also conducts special reviews in response to allegations and other concerns brought to the attention of the Legislative Auditor. The Legislative Auditor conducts a preliminary assessment in response to each request for a special review and decides what additional action will be taken by OLA.

For more information about OLA and to access its reports, go to: www.auditor.leg.state.mn.us.

May 2, 2024

Members
Legislative Audit Commission

Members
Legislative Commission on Cybersecurity

Matt Varilek, Commissioner
Department of Employment and Economic Development

Tarek Tomes, Commissioner and Chief Information Officer
Minnesota IT Services

This report presents the results of our information technology performance audit of the Unemployment Insurance (UI) system, operated by the Minnesota Department of Employment and Economic Development (DEED) and Minnesota Information Technology Services (MNIT). The objective of this audit was to determine if DEED and MNIT had adequate internal controls to safeguard the confidentiality, integrity, and availability of the information system. We also validated select eligibility controls related to UI benefit eligibility.

In accordance with *Minnesota Statutes* 2023, 13.37, subd. 2, we have removed from the public version of our report language from Finding 3 that we deemed likely to substantially jeopardize the security of information in the UI system. We discussed the specific details with DEED and MNIT.

DEED and MNIT did not agree with all findings, as stated in their response at the end of the report. We have considered all information presented by DEED and MNIT, and believe the evidence we obtained and the testing we performed during the course of the audit supports our conclusions. DEED and MNIT also raised concerns about the expanded scope and objectives of the audit. Generally accepted government auditing standards, which apply to our performance audit work, state, “auditors may need to refine or adjust the audit objectives, scope, and methodology as work is performed.”¹

This audit was conducted by Mark Mathison, CISA, CISSP, CPA Inactive (IT Audit Director); Joe Sass, CISA (IT Audit Coordinator); and IT auditors Dustin Juell, CompTIA Security+; and Peng Xiong.

We received the cooperation of DEED and MNIT staff while performing this audit, and we thank them for their participation.

Sincerely,



Judy Randall
Legislative Auditor



Lori Leysen, CPA
Deputy Legislative Auditor

¹ Comptroller General of the United States, Government Accountability Office, *Government Auditing Standards*, 2018 Revision (Washington, DC, Technical Update April 2021), 155.



OLA

Table of Contents

	<u>Page</u>
Introduction.....	1
Report Summary	3
Conclusions.....	3
Findings and Recommendations	3
Background.....	7
Unemployment Insurance Overview and History.....	7
Audit Scope, Objectives, Methodology, and Criteria	8
Unemployment Insurance System Security Review	11
Information Security Program and Risk Management	11
Data Protection Categorization	14
Identity and Access Management	17
Security Logging and Monitoring.....	22
Threat and Vulnerability Management	24
Disaster Recovery Planning.....	26
Secure System Configuration	28
Unemployment Insurance System Eligibility Control Review.....	31
Unemployment Insurance Modernization Program.....	35
Appendix: MNIT’s Information Security Risk Treatment Procedure	41
Department of Employment and Economic Development and Minnesota IT Services Combined Response	43



OLA

Introduction

The Unemployment Insurance (UI) system is an information technology system managed by the Department of Employment and Economic Development (DEED) and Minnesota Information Technology Services (MNIT). First launched as part of a phased implementation in 2005, the UI system provides a comprehensive web portal that allows individuals to apply for and manage their UI benefits, as well as for employers or their agents to provide earnings data, pay UI taxes, and review UI claims against their accounts. DEED staff, and staff from other state agencies, also utilize the UI system to make eligibility determinations, process appeals, and make benefit payments.

The UI system contains data on more than 470,000 Minnesota employers, as well as data on roughly 2 million individuals and approximately 5 million applications for unemployment insurance benefits. The system also contains nearly 96 million records of benefit payments made to those applicants. DEED and MNIT currently have a \$44 million project underway to modernize the UI system. This project began in 2019 and is expected to finish by November 2024.

We conducted this information technology performance audit to determine whether DEED and MNIT followed applicable policies, standards, and best practices designed to protect the confidentiality, integrity, and availability of the UI system and its data. We audited system controls and agency processes related to access management, data privacy, disaster recovery, security logging and monitoring, and threat and vulnerability management. We also audited key eligibility controls related to UI benefit eligibility.

Internal controls are the policies and procedures management establishes to govern how an organization conducts its work and fulfills its responsibilities. A well-managed organization has strong controls across all of its internal operations. If effectively designed and implemented, controls help ensure, for example, that inventory is secured, computer systems are protected, laws and rules are complied with, and authorized personnel properly document and process financial transactions.

Minnesota Law Mandates Internal Controls in State Agencies

State agencies must have internal controls that:

- Safeguard public funds and assets and minimize incidences of fraud, waste, and abuse.
- Ensure that agencies administer programs in compliance with applicable laws and rules.

The law also requires the commissioner of Management and Budget to review OLA audit reports and help agencies correct internal control problems noted in those reports.

— **Minnesota Statutes 2023, 16A.057**



OLA

Report Summary

Conclusions

The Department of Employment and Economic Development (DEED) and Minnesota Information Technology Services (MNIT) complied with many of MNIT's information security requirements, and had adequate internal controls related to Unemployment Insurance (UI). However, DEED and MNIT did not comply with a variety of MNIT's information security controls related to risk management, identity and access management, security logging and monitoring, vulnerability management, disaster recovery, and secure system configurations. The more significant instances of noncompliance and internal control weakness were in the areas of identity and access management. The list of findings below and the full report provide more information about these and other weaknesses.

Findings and Recommendations

Finding 1. DEED and MNIT inaccurately concluded that the Unemployment Insurance system complied with all information security control requirements and did not report known issues within MNIT's centralized risk and compliance tool. (p. 12)

Recommendations

- DEED and MNIT should document all known risks within their security control compliance self-assessments.
 - DEED and MNIT should track information security risks, findings, weaknesses, and deficiencies—with mitigations and remediations—within MNIT's central risk and compliance tool.
-

Finding 2. DEED and MNIT do not have a process for identifying and securely deleting data records within the Unemployment Insurance system that exceed defined retention periods. (p. 15)

Recommendations

- DEED should follow its records retention schedule or seek to have it changed to suit its business requirements.
 - DEED and MNIT should implement the needed functionality within the Unemployment Insurance system to delete unnecessary records.
-

Finding 3. DEED and MNIT have not fully implemented one-quarter of the identity and access management requirements designed to help protect the Unemployment Insurance system. (p. 18)

Recommendations

For the Unemployment Insurance system, DEED and MNIT should:

- [REDACTED]
 - [REDACTED]
 - Prevent frequent reuse of the same passwords.
 - [REDACTED]
 - Implement required controls for its privileged administrative accounts.
 - [REDACTED]
 - [REDACTED]
[REDACTED]
 - Terminate idle or unattended user sessions.
 - Provide appropriate system-use notifications to all users prior to accessing the system.
-

Finding 4. DEED and MNIT do not comply with all provisions of MNIT's Security Logging and Monitoring Standard for the Unemployment Insurance system. (p. 23)

Recommendation

DEED and MNIT should ensure that the Unemployment Insurance system's logging and monitoring controls are implemented as required by MNIT's Security Logging and Monitoring Standard.

Finding 5. DEED and MNIT do not adequately maintain scanning agents on essential technical devices that support the Unemployment Insurance system. (p. 25)

Recommendations

- DEED and MNIT should ensure that vulnerability and configuration scanning software is properly updated on the Unemployment Insurance system.
 - MNIT should clarify system maintenance responsibilities for its cloud-hosted system to ensure that all supporting software remain up to date.
-

Finding 6. DEED and MNIT did not document their review, updates, or testing of the Unemployment Insurance system's disaster recovery plan. (p. 27)

Recommendation

DEED and MNIT should ensure that disaster recovery plans for the Unemployment Insurance system are reviewed, updated, and tested annually.

Finding 7. DEED and MNIT did not fully document some key processes necessary to ensure full recovery of the Unemployment Insurance system in case of a disaster. (p. 28)

Recommendation

DEED and MNIT should ensure that its disaster recovery plan for the Unemployment Insurance system contains documentation of all key processes and procedures necessary to successfully recover and validate the system.

Finding 8. In some cases, DEED and MNIT did not implement recommended security configurations for the Unemployment Insurance system, nor did they document, within MNIT's centralized risk and compliance tool, the rationale for deviating from the recommended configurations. (p. 29)

Recommendations

- DEED and MNIT should implement recommended security configurations when appropriate.
 - DEED and MNIT should document, within MNIT's centralized risk and compliance tool, system configuration exceptions that do not meet MNIT's security standards.
 - DEED and MNIT should not retain sensitive documents longer than is necessary.
-

Finding 9. DEED uses various external and manual processes to identify suspicious transactions and potentially ineligible individuals, rather than automating these processes within the Unemployment Insurance system. (p. 31)

Recommendations

- DEED and MNIT should evaluate its current manual data-matching processes and look to automate those processes into the Unemployment Insurance system.
 - DEED and MNIT should perform and document their analysis of strengths and weaknesses when deciding whether to implement automated data integrity solutions.
-

Finding 10. DEED and MNIT do not report on all Unemployment Insurance system project-related costs. (p. 38)

Recommendations

- DEED and MNIT should track and report on all project-related costs, including those related to DEED and MNIT staff time.
 - MNIT should develop guidance and recommendations for agencies developing budgets for large or multiyear IT projects.
-

Finding 11. DEED and MNIT continue to custom build identity and access management functionality into the Unemployment Insurance system, rather than modernizing to an off-the-shelf solution. (p. 39)

Recommendation

DEED and MNIT should consult with the Technology Advisory Council, and reaffirm its decision to custom build identity and access management functionality.

Background

Unemployment Insurance Overview and History

The Unemployment Insurance (UI) program provides a temporary, partial wage replacement for workers who become unemployed through no fault of their own.

The UI program is a federal-state partnership; the federal government mandates some provisions, but states individually implement the program through state law.¹ The program—overseen by the U.S. Department of Labor—is administered by the Department of Employment and Economic Development (DEED).

Benefits

State law establishes the amount and duration of UI benefits for Minnesota workers. Generally, eligible individuals who apply for benefits may receive weekly cash payments of up to 50 percent of their prior average weekly wages, up to a dollar cap set in law.

To receive benefits, eligible individuals must submit an initial application and weekly requests for benefits through DEED's Unemployment Insurance system (UI system). DEED uses the information that applicants submit to determine both their initial and ongoing eligibility for benefits, as well as the amount of their cash benefit each week.

Information Technology System

At the center of the UI program is DEED's UI system, which provides Minnesota workers with an online web portal to apply for UI benefits; manage their account; request benefit payments; and provide information, such as hours worked. The UI system also includes an employer portal. The employer portal allows employers (or their agents) to submit wage reports, maintain business information, respond to information requests, pay their unemployment insurance taxes, and view benefits charged to their account. The UI system uses the information entered by applicants and employers to attempt to verify an applicant's identity, determine their eligibility for benefits, and process UI benefit payments.

Minnesota's UI system is a Windows-based Java web application that was first implemented in 2005. The system relies on numerous other components for identity and access management, document storage, workflow processes, correspondence, interactive voice response, batch processing, and data storage. Minnesota Information Technology Services (MNIT) is responsible for the technical implementation, support,

¹ Social Security Act, 42 *U.S. Code*, chapter 7, subchapter III, secs. 501-506 (2022); Federal Unemployment Tax Act, 26 *U.S. Code*, subtitle C, chapter 23, secs. 3301-3311 (2022); and *Minnesota Statutes* 2023, Chapter 268.

and maintenance of the UI system.² MNIT uses Amazon Web Services, Inc. (AWS) for infrastructure hosting of this system.

Annually, the UI system receives approximately 200,000 initial insurance claims.³ In Fiscal Year 2023, DEED collected approximately \$778 million in unemployment insurance premiums from employers and distributed approximately \$953 million in unemployment insurance benefits.⁴ As a result, the UI system contains vast amounts of sensitive data, including Social Security numbers and bank account information.

Unemployment Insurance Modernization Program

DEED began working with MNIT in 2019 on a multiyear endeavor to modernize components of the UI system. Since first implementing the employer portal in 2005 and the applicant portal in 2007, the needs of individual users and the ways in which they want to interact with the UI system have evolved. To address these needs, DEED has obligated more than \$44 million to modernize the UI system, with the goals of improving customer experience, improving flexibility, and strengthening the UI system's infrastructure.⁵ The result is a multiphased program consisting of more than 35 projects that DEED and MNIT hope to finalize by November 2024.

Audit Scope, Objectives, Methodology, and Criteria

We conducted this information technology performance audit to determine whether DEED and MNIT followed applicable policies, standards, and best practices designed to protect the confidentiality, integrity, and availability of the UI system and its data. We also validated key eligibility controls related to UI benefit eligibility. Finally, we gained insights into the UI system modernization efforts to assess impact and potential risks to the control environment. We evaluated policies, procedures, controls, and modernization activities during the period from March 2023 to December 2023.

We designed our work to address the following questions:

- Do the Department of Employment and Economic Development and Minnesota Information Technology Services have adequate internal controls

² Under *Minnesota Statutes* 2023, 16E.01, subd. 1a, MNIT is the state's centralized information technology department tasked with providing oversight, leadership, and direction for information and telecommunications technology policy and the management, delivery, accessibility, and security of executive branch information and telecommunications technology systems and services.

³ This number is based upon a five-year average, excluding COVID-19 unemployment outliers seen during 2020-2021.

⁴ Minnesota Management and Budget, *2023 Annual Comprehensive Financial Report* (St. Paul, 2023), 50.

⁵ Neither DEED nor MNIT received direct appropriations for the UI modernization projects. Originally, DEED and MNIT obligated approximately \$20 million for modernization contracts. Over time, DEED and MNIT have amended the contracts for changes in deliverables and time extensions, which increased the costs of these projects to over \$44 million. Despite the federal government making \$782.9 million of American Rescue Plan Act grants available to states for UI modernization efforts, Minnesota was the only state that did not receive any of these grant funds. DEED has funded the project using other unemployment insurance administrative funds authorized under *Minnesota Statutes* 2023, 298.196.

to safeguard the confidentiality, integrity, and availability of the Unemployment Insurance system?

- Did the Department of Employment and Economic Development and Minnesota Information Technology Services implement reasonable IT edits and system processes to help determine an applicant's eligibility for Unemployment Insurance benefits?
- To what extent will modernization projects address Unemployment Insurance system safeguard controls or eligibility processes?

To answer these questions, OLA auditors:

- Reviewed relevant DEED and MNIT documentation.
- Interviewed relevant DEED and MNIT staff.
- Reviewed relevant UI audit reports and information prepared by other audit firms.
- Examined UI contracts and related project management documents.
- Performed data analysis on UI eligibility and system data.
- Reviewed and validated current UI system configuration documentation, security assessments, and vulnerability scans.
- Examined UI user account access privileges and security policies.
- Reviewed the UI disaster recovery plans for completeness and accuracy.

We conducted this performance audit in accordance with generally accepted government auditing standards.⁶ 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.

Using applicable federal and state laws, and agency policies and standards, we tested whether DEED and MNIT had effective controls in place to protect the confidentiality, integrity, and availability of the UI system.

To assist with our testing and data validation, we obtained access to the UI system's database. When sampling was used, we used a sampling method that complies with generally accepted government auditing standards and that supports our findings and conclusions. That method does not, however, allow us to project the results we obtained to the populations from which the samples were selected.

⁶ Comptroller General of the United States, Government Accountability Office, *Government Auditing Standards, 2018 Revision* (Washington, DC, Technical Update April 2021).



OLA

Unemployment Insurance System Security Review

We gained an understanding of the controls in place and tested significant controls within the Unemployment Insurance (UI) system against key Minnesota Information Technology Services (MNIT) technical security policies and standards based on our assessment of risk.⁷ Our audit looked at the following information security areas:

- Information security program and risk management.
- Data protection categorization.
- Identity and access management.
- Security logging and monitoring.
- Threat and vulnerability management.
- Disaster recovery planning.
- Secure system configuration.

Information Security Program and Risk Management

An information security program helps protect an organization's information technology and data. A security program should include elements such as:

- Information security architecture.
- Policies, standards, procedures, and security guidelines.
- Risk management process.
- The definition and monitoring of metrics.
- The classification of information assets.

MNIT has developed an information security architecture for state systems, putting in place MNIT staff, processes, and technologies. In addition to centralized IT security functions, MNIT security teams are embedded within state agencies, such as the Department of Employment and Economic Development (DEED), to get a deeper understanding of their business needs, compliance requirements, goals, and culture.

During our audit, MNIT had one dedicated security manager embedded at DEED. MNIT has two additional positions allocated to help with DEED's localized security needs; however, those positions remained vacant throughout our audit.

⁷ MNIT publishes its Enterprise Information Security Policies and Standards on their website, <https://mn.gov/mnit/government/policies/security/>, accessed March 15, 2024.

State law stipulates that MNIT must develop information security policies, guidelines, and standards.⁸ The law further stipulates that each department or agency is responsible for the security of its data within the guidelines of established enterprise policy.⁹

To help ensure that the enterprise security policies and standard requirements stay current with changes in agency objectives, legal and regulatory obligations, and information security risks, MNIT information security personnel are mandated to annually review and update these enterprise requirements.¹⁰ As part of our audit, we confirmed that MNIT had reviewed and updated its security program authoritative documents within the prior year. MNIT last updated its policies and standards in October 2023.

Minnesota Management and Budget's (MMB's) risk assessment procedure and MNIT's information security standard require risk assessments.¹¹ MMB's procedure requires that agencies annually conduct a comprehensive review of the organization's most significant business processes and risks. For systems like DEED's UI system, MNIT requires risk and security control assessments be regularly updated. As part of our audit, we validated that DEED and MNIT completed a current risk and security control assessment. Although we confirmed an assessment was completed, our audit found certain inaccuracies with the agencies' self-assessment conclusions.

FINDING 1

DEED and MNIT inaccurately concluded that the Unemployment Insurance system complied with all information security control requirements and did not report known issues within MNIT's centralized risk and compliance tool.

DEED's and MNIT's self-assessment of control compliance concluded that the UI system fully complied with all 248 information security control requirements identified in MNIT's standards.¹² However, as we discuss in the remainder of this report, our audit identified deficiencies related to identity and access management, security logging and monitoring, vulnerability management, disaster recovery, and secure system configurations.

Having an accurate assessment of controls is essential for risk management processes. MNIT's process for managing security risks is outlined in the Appendix. When control gaps are identified—whether found by agency staff, information security professionals, or internal or external auditors—it begins the process for DEED management to either accept risks resulting from the deficiency, or develop remediation plans to mitigate the findings.

⁸ *Minnesota Statutes* 2023, 16E.03, subd. 7.

⁹ *Ibid.*

¹⁰ Minnesota Information Technology Services, *Information Security Program Standard*, version 1.7, Control 5, October 1, 2023.

¹¹ Minnesota Management and Budget, Statewide Operating Procedure 0102-01.2, *Risk Assessment*, April 10, 2023; and Minnesota Information Technology Services, *Information Security Risk Management Standard*, version 1.7, October 1, 2023.

¹² MNIT publishes its Enterprise Information Security Policies and Standards on their website, <https://mn.gov/mnit/government/policies/security/>, accessed March 15, 2024.

MNIT's standards also require that all findings and remediation plans must be documented in its centralized risk and compliance tool to help manage and track progress.

MNIT's centralized risk and compliance tool is also used to request exceptions to information security requirements. When developing security requirements for an organization as large and diverse as state government, MNIT may not be able to anticipate all situations where controls are not required. For example, not all government systems may require multifactor authentication. For this reason, MNIT's information security program allows agencies to request an exception to the mandated controls. MNIT strives to recommend information security best practices and compliance requirements, however, agency leaders are ultimately responsible and need to balance the costs and risks associated with each control. When properly followed, MNIT's centralized risk and compliance tool—through a structured request and approval process—allows for government leaders to track previous decisions and understand reasons a best practice control may not be needed. This can be particularly important within government when previous government officials may have made risk-based decisions that now impact the current administration.

When we inquired as to why some known information security risks and compliance gaps were not being tracked within MNIT's centralized risk and compliance tool, a representative for DEED told us that they chose to track them within an agency-managed tool rather than the centralized tool. Since DEED did not follow the required risk management process, it is difficult to know what information security risks are being mitigated, remediated, or simply accepted by agency leaders.

Having a central repository of information security risks can provide a comprehensive view of the risks across agencies and allow MNIT to better strategize and prioritize remediation efforts. Furthermore, MNIT's centralized risk and compliance tool provides a uniform process for MNIT to communicate risks to executive branch leaders, ensuring that they are aware of the risks, are involved in remediation efforts, and accept the risks.

RECOMMENDATIONS

- **DEED and MNIT should document all known risks within their security control compliance self-assessments.**
 - **DEED and MNIT should track information security risks, findings, weaknesses, and deficiencies—with mitigations and remediations—within MNIT's centralized risk and compliance tool.**
-

To ensure that agency leaders understand their information security risks, MNIT security professionals are required to provide information security program performance metrics to agency leadership.¹³ To help foster this communication, MNIT created risk management scorecards. These scorecards condense a variety of security metrics, including security gaps and remediation efforts, for all agency information systems into five different areas based on the U.S. National Institute of Standards and Technology

¹³ Minnesota Information Technology Services, *Information Security Program Standard*, version 1.7, Control 6, October 1, 2023.

Cybersecurity Framework functional areas.¹⁴ As part of our audit, we validated that MNIT security leaders produced and delivered security metrics to DEED's leadership. However, as noted previously, when risk assessment processes have not been followed, agency leaders may not have an accurate picture of the agency's overall risks.

Data Protection Categorization

MNIT's Data Protection Categorization standard focuses on identifying the data within a system, including whether the data is classified as private or nonpublic and identifying how long the data should be retained.¹⁵ Knowing the classification of the information within a system helps determine the appropriate and minimum level of security controls. By law, unemployment insurance data is classified as private and nonpublic data.¹⁶ State law also requires that government entities keep an inventory of records and a retention schedule approved by both the head of the entity and the records disposition panel.¹⁷ Government entities may only dispose of official records according to the approved records retention schedule.¹⁸ MNIT security standards require agencies to implement data disposal processes for identifying and securely deleting highly sensitive data that exceeds defined retention periods.¹⁹

DEED categorized its information and the UI system with a data protection level as "High," requiring the highest level of controls defined within the MNIT standards.²⁰ Recognizing that the UI system contains sensitive data and processes over \$1 billion of financial resources, we agree that the agency selected the appropriate level of protection. We also found that DEED had an approved records retention schedule in place for unemployment insurance data that complied with MNIT's standard and state law.

DEED's records retention schedule defines the retention periods for 22 different types of unemployment insurance records. The retention periods vary based on the type of record, ranging from 14 quarters to ten years. Our testing did not find any instances where DEED or MNIT had disposed of data that was required to be retained. However, our testing identified that DEED does not dispose of UI records after the specified retention period has passed. With DEED retaining sensitive and not-public data in the UI system beyond the retention period, it subjects the agency to added risk, in that a potential breach could be that much more damaging.

¹⁴ The National Institute of Standards and Technology Cybersecurity Framework is organized by five key functions: Identify, Protect, Detect, Respond, and Recover. U.S. National Institute of Standards and Technology, "Cybersecurity Framework: Quick Start Guide," <https://www.nist.gov/cyberframework/getting-started/quick-start-guide>, accessed February 20, 2024.

¹⁵ Minnesota Information Technology Services, *Data Protection Categorization Standard*, version 1.7, October 1, 2023.

¹⁶ *Minnesota Statutes* 2023, 268.19.

¹⁷ *Ibid.*, 138.17.

¹⁸ *Ibid.*

¹⁹ Minnesota Information Technology Services, *Data Protection Categorization Standard*, version 1.7, Control 3, October 1, 2023.

²⁰ MNIT publishes its Enterprise Information Security Policies and Standards on their website, <https://mn.gov/mnit/government/policies/security/>, accessed March 15, 2024. Each security standard identifies if a control is applicable to data protection categories of "high," "moderate," or "low."

FINDING 2
DEED and MNIT do not have a process for identifying and securely deleting data records within the Unemployment Insurance system that exceed defined retention periods.

Our audit specifically reviewed and tested four types of records to determine whether DEED followed its retention schedule and securely deleted highly sensitive data that exceeded defined retention periods.

- Employer Registration Account Information.** State law requires every business that pays covered wages in Minnesota to register with the UI program.²¹ Registration information includes data such as: the name of the business, address, Federal Employment Identification Number, state taxpayer ID number, business activity, and name(s) and Social Security number(s) for all owners / officers. DEED's retention schedule defined the retention period of employer registration account information as 14 quarters (three years and six months) after no activity. Yet, our testing found more than 223,000 employer account records that have been inactive prior to January 1, 2019, including over 65,000 that have been inactive since DEED brought them into the UI system during the system conversion in 2005. Exhibit 1 shows that DEED, on average, inactivates approximately 11,000 employer account records per year.

Exhibit 1
**Number of Deactivated Employer Account Records in UI System
Summed by Year Deactivated**

Year Deactivated	Number of Employer Account Records
Prior to 2005	65,140
2005	5,852
2006	12,820
2007	11,182
2008	11,695
2009	14,215
2010	12,757
2011	14,013
2012	10,555
2013	10,962
2014	10,591
2015	11,829
2016	10,906
2017	10,310
2018	10,323

Source: Office of the Legislative Auditor, based on data in the UI system.

²¹ *Minnesota Statutes* 2023, 268.035, subd. 29; and 268.042.

- **Wage Detail Records.** Each quarter, employers that have employees in covered employment are required to submit wage detail information.²² On average, DEED receives approximately 3.25 million wage detail records each quarter. According to DEED’s records retention schedule, the retention period for wage detail records is 17 quarters (four years and three months). Our testing identified that the UI system retained more than 144 million wage detail records—approximately 3.25 million wage detail records for each quarter going back to 2005—far beyond the required 17 quarters. These records contain the quarterly earnings for nearly all of Minnesota’s workforce, including each individual’s first name, last name, and Social Security number.²³
- **Benefit Application and Account Information.** To receive benefits, individuals must create an account, submit an initial application, and then submit weekly requests for benefits. On average, DEED receives approximately 200,000 benefit applications per year.²⁴ Some individuals may initially create an account but never apply for or request benefits. DEED’s retention period for benefit application and account information is four years after no activity. Our testing identified that the UI system retained approximately 2.79 million benefit application records submitted between 2005 and 2017.
- **Benefit Payment Information.** DEED’s retention schedule defines the retention period of benefit payment information as three years and three months.²⁵ Our testing identified that DEED retained more than 56 million benefit payment records for UI benefits recipients who were paid between 2005 and 2020.

In our review, we observed that DEED and MNIT had purged approximately 340,000 applicant records in 2013 and 2014. However, according to DEED officials, DEED and MNIT discontinued purging records after identifying potential integrity issues for other data and calculations within the system caused by the data purging.²⁶ Because the UI system architecture relies upon a relational database, the integrity of the system can be jeopardized if records, such as an applicant identification number—which is a key data element for building relationships with other data—is missing, deleted, or no longer available. As such, to avoid “orphaned” records, or other data integrity issues, it is important to have a methodical strategy when purging old data.

²² *Minnesota Statutes* 2023, 268.035, subd. 29; and 268.044.

²³ *Minnesota Statutes* 2023, 268.044, requires that the report must include for each employee in covered employment during the calendar quarter, the employee’s name, Social Security number, the total wages paid to the employee, and total number of paid hours worked.

²⁴ This number is based upon a five-year average, excluding COVID-19 unemployment outliers seen during 2020-2021.

²⁵ Under *Minnesota Statutes* 2023, 268.18, subd. 2(d), the department is authorized to issue a determination of overpayment penalty within 48 months of the establishment of the benefit account upon which the unemployment benefits were obtained through misrepresentation. As such, in some cases, it may be necessary to retain payment details beyond the 39 months outlined within the retention schedules.

²⁶ DEED representatives told us that the purge process deleted some data that was critical to calculating tax rates, determining program eligibility, and completing overpayments.

DEED told us that employer and applicant data is currently retained beyond the retention schedule to maintain data integrity related to critical UI functions for administering the program. In some instances, DEED believed that it needed to retain the data beyond what is currently defined in its retention schedules to support debt collection efforts and federal tax implications. DEED further told us that as part of its modernization efforts (discussed more at the end of this report), it plans to implement new purge functionality that will allow them to purge records that are no longer needed, without impacting data integrity. DEED told us that portions of the purge project will need to be completed as part of the third phase of the modernization program, anticipated to begin in 2024.

While state law states that the agency *may dispose* of the records per the retention schedule, it does not require agencies to dispose of their records.²⁷ However, DEED is not compliant with MNIT's security requirement to develop and implement a disposal process.²⁸ Given the overall sensitivity of the records, DEED is assuming additional risk in retaining this information. This risk is further increased when coupled with the security findings described in this report.

RECOMMENDATIONS

- **DEED should follow its records retention schedule or seek to have it changed to suit its business requirements.**
 - **DEED and MNIT should implement the needed functionality within the Unemployment Insurance system to delete unnecessary records.**
-

Identity and Access Management

Identity and access management defines (1) who individual UI users are, (2) how those users access the UI system, and (3) what functions they can access within the UI system. The UI system has four user types that can log into and access the system:

1. **Applicants** – Individuals applying for and maintaining their benefit accounts.
2. **Employers** – Representatives from businesses employing workers in Minnesota. These users access the system to submit wage detail data, pay their unemployment taxes, view claims against their businesses, and maintain their business profiles as employers.
3. **Agents** – Entities that act on behalf of employers to handle employers' UI obligations. Agents can perform many of the same procedures as employers if employers assign the proper roles to the agents.
4. **Internal Staff** – Government staff working to support county, state, and federal programs related to unemployment insurance.

²⁷ *Minnesota Statutes 2023*, 138.17.

²⁸ Minnesota Information Technology Services, *Data Protection Categorization Standard*, version 1.7, Control 3, October 1, 2023.

As of September 2023, the UI system contained active access accounts for roughly 2 million applicants, 465,000 employers, 28,000 agents, and 500 internal staff. Employers, agents, and internal users also have their own unique user IDs. In some cases, a single individual may have more than one user ID, such as if they work for more than one employer.

Applicants have user accounts to access the UI system through a website portal or an interactive telephone system. Applicants log in using their Social Security number as their user identification (user ID). Although there is a risk of using the Social Security number within the system, we believe that DEED and MNIT have taken reasonable precautions to limit the risk. For example, in addition to encrypting and masking the user ID, applicants are not identified inside the UI system with their Social Security number; rather, they have a unique applicant identifier.

Identity and access management extends beyond the UI system itself. It also includes defining and controlling necessary access to servers, databases, and various other system components and supporting tools that interact with the UI system. MNIT defines expected controls within its identity and access management policy and standard.²⁹ The security standard outlines 40 related controls that we evaluated based on risk to the system.

Our testing focused on key controls related to user accounts and authentication for the UI system, as well as its underlying components. These control requirements help protect DEED and MNIT from inappropriate persons accessing the UI system, and limiting access only to information that is necessary to perform job duties. We found deficiencies related to 10 of MNIT's 40 identity and access management controls.

FINDING 3

DEED and MNIT have not fully implemented one-quarter of the identity and access management requirements designed to help protect the Unemployment Insurance system.³⁰

DEED and MNIT did not ensure that the UI system complied with the following information security requirements:

- [REDACTED]

²⁹ Minnesota Information Technology Services, *Identity and Access Management Policy*, version 1.5, October 1, 2022; and Minnesota Information Technology Services, *Identity and Access Management Standard*, version 1.6, October 1, 2022. In January 2024, MNIT released version 1.7 of its standard, which added three new controls that were not included in the scope of our audit.

³⁰ In accordance with *Minnesota Statutes* 2023, 13.37, subd. 2, we have removed from the public version of our report language from Finding 3 that we deemed likely to substantially jeopardize the security of information in the UI system. We discussed the specific details with DEED and MNIT.

³¹ [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- **UI system password history settings do not comply.** MNIT’s security standards require that passwords must be different from at least the previous 24 passwords used by the respective account.³⁴ However, we found DEED and MNIT have configured the UI system to only restrict individuals from reusing the previous five passwords.
- [REDACTED]
- **Privileged UI administrative accounts are not managed within specialized account management tools.** MNIT’s security standards recognize that some accounts, by function and/or security access, are granted special privileges within an information system and need added levels of control. As such, in addition to tighter password and monitoring requirements, MNIT’s security standards require that, where technically feasible, these privileged accounts must be managed in a

32

33

³⁴ Minnesota Information Technology Services, *Identity and Access Management Standard*, version 1.6, Control 25, October 1, 2022.

35


centralized privileged account management solution—an industry best practice tool specifically designed for tighter control over privileged accounts—and follow special account naming standards.³⁶ However, DEED and MNIT did not use the required tool for the UI system administrative accounts.

- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
 - [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

³⁶ Minnesota Information Technology Services, *Identity and Access Management Standard*, version 1.6, Control 11, October 1, 2022.



37

38

- 
- **Idle users of the UI system are not disconnected timely.** DEED and MNIT configured the UI system to disconnect idle logged-in user sessions after 45 minutes for applicants, and 30 minutes for employers, agents, and internal users. However, MNIT's security standards require that information systems automatically end a user session after 15 minutes of inactivity.³⁹ This control helps to reduce the risk of a user leaving a session unattended and, therefore, inappropriately used by a different person. The risk of this happening is greater if the user logs on from a shared computer that may be available at a public library, workforce center, work location, or home.
 - **No system-use notifications or warning banners are presented to applicants, employers, or agents before allowing access.** MNIT's security standards require that systems contain a warning banner that state entities must display on the webpage before allowing access.⁴⁰ The warning banner must include a notification of any monitoring, recording, or auditing that may occur and a description of the authorized uses of the system. In some cases, the warning banner must reference the civil and criminal penalty for unauthorized use. Although DEED and MNIT provide this notification to internal users, they do not display this notification for applicants, employers, or agents.

DEED and MNIT do provide employers and agents a privacy and security page.⁴¹ However, the information on this page does not fulfill the requirements of the security standard. Further, the content on this page is neither current nor accurate, as it references unsupported internet browsers, outdated encryption protocols, and unused security certificates.

MNIT developed its identity and access management security requirements based on industry best practices and to meet information security compliance requirements. These requirements are designed to protect organizations from inappropriate persons accessing the system and limit access only to information that is necessary to perform job duties. With millions of sensitive data records within the UI system, DEED and MNIT are at greater risks of unscrupulous persons taking advantage of identity and access management control weaknesses.

In some instances, DEED and MNIT were aware of the control weaknesses we identified within the UI system. For example, they have recognized that   would be difficult due to technical and usability

³⁹ Minnesota Information Technology Services, *Identity and Access Management Standard*, version 1.6, Controls 32-33, October 1, 2022.

⁴⁰ *Ibid.*, Control 35, October 1, 2022.

⁴¹ Minnesota Unemployment Insurance, *Privacy and Security*, <https://uimn.org/employers/employer-account/privacy-security/index.jsp>, accessed January 22, 2024.

issues with the UI interactive voice response features. DEED and MNIT have designated a specific project within its modernization program to make improvements to how users of the UI system are authenticated. The goal of this project is to improve password compliance and self-serve user experience. However, as noted in our risk management section of this report, DEED and MNIT have not documented their knowledge of these known control deficiencies, acceptance of the risks, or remediation plans.

RECOMMENDATIONS

For the Unemployment Insurance system, DEED and MNIT should:

- [REDACTED]
 - [REDACTED]
 - **Prevent frequent reuse of the same passwords.**
 - [REDACTED]
 - **Implement required controls for its privileged administrative accounts.**
 - [REDACTED]
 - [REDACTED]
 - **Terminate idle or unattended user sessions.**
 - **Provide appropriate system-use notifications to all users prior to accessing the system.**
-

Security Logging and Monitoring

Logging and monitoring are two essential practices for ensuring the optimal performance, security, and availability of IT systems. Logging is the process of collecting and storing data about the events and activities that occur in an IT system, such as user actions, system changes, errors, and threats. Monitoring is the process of analyzing and evaluating the log data to detect and resolve issues, optimize resources, identify trends, and improve security. MNIT's Security Logging and Monitoring Standard outlines 20 required controls.⁴²

For example, MNIT's standard requires automated logging on all systems to reconstruct the following events:

- All actions taken by accounts with administrative privileges.
- Access to all log data, including initialization, stopping, pausing, or deleting of the logs.

⁴² Minnesota Information Technology Services, *Security Monitoring and Response Policy*, version 1.6, October 1, 2023; and Minnesota Information Technology Services, *Security Logging and Monitoring Standard*, version 1.7, October 1, 2023.

- All login attempts.
- All system log-offs.
- All password changes.
- Changes to database or application records, where the application has been bypassed to produce the change.
- All system and data interactions concerning federal tax information.
- System and application alerts and error messages.
- System and application shutdowns and restarts.
- Security policy modifications.

Because UI system logs are generated in multiple servers, databases, applications, and infrastructure devices, and because these logs can become very large, MNIT's logging and monitoring standard requires a centralized log management service.⁴³

MNIT has developed a centralized security operations center. By design, the security operations center has tools to consolidate various logs from different state systems. These tools help analyze, detect, and report high-risk IT security events. A specialized team of security professionals within MNIT monitor these tools for security alerts, both during standard and nonstandard working hours. These security professionals can also perform deep analysis into detailed security logs to hunt for specific threats. Security activity and alerts can be shared with state agency system owners for additional analysis to help assess the significance of the activity or alerts.

As part of our audit testing, we interviewed administrators working directly with the UI system and staff working within MNIT's central security operations center to gain an understanding of the logging and monitoring processes. We observed certain log files that were available, and validated that required events were captured within those log files.

FINDING 4

DEED and MNIT do not comply with all provisions of MNIT's Security Logging and Monitoring Standard for the Unemployment Insurance system.

The UI system and its subcomponents capture a variety of security events into various log files. However, the following gaps increase the risk that certain security events are not properly detected.

First, DEED and MNIT did not log direct changes to database records that bypassed the UI application.⁴⁴ Some MNIT staff can access the underlying UI system database to add, modify, or delete data. With no log of these edits, DEED and MNIT are not able

⁴³ Minnesota Information Technology Services, *Security Logging and Monitoring Standard*, version 1.7, Control 10, October 1, 2023.

⁴⁴ *Ibid.*, Control 1, October 1, 2023.

to monitor for unauthorized or erroneous changes. When we asked how supervisors and others monitor what changes were being made, a MNIT representative told us that, historically, DEED and MNIT had this logging enabled, and they used the reports to monitor changes to data. However, we were told by MNIT that with recent changes to move the UI system into a cloud-hosting environment, the logging and monitoring were lost.

Second, DEED and MNIT were not using a required centralized log management service to aggregate and analyze UI system events.⁴⁵ As a result, UI administrators had to search multiple systems to find our sample test of successful and unsuccessful logon events, rather than search within one tool. When we asked employees within MNIT's central security operations center about these same tested events, MNIT security staff had no record or visibility of the events, beyond basic network activities. By not utilizing the existing security operations center to help monitor events, there is an increased risk that some high-risk events may not be detected and responded to in a timely manner. For example, by not having tools in place to identify failed attempts to log into the UI system, unscrupulous individuals could try millions of active system user accounts without DEED or MNIT being aware of these actions.

Finally, DEED and MNIT are not retaining security events in accordance with MNIT's security standard.⁴⁶ The standard requires that log data be retained for at least one year, with a minimum of three months immediately available for analysis. Log data for federal tax information must be retained for seven years. However, we found critical events that were being overwritten within days of the actual event. Not only does the deletion of security events not comply with security requirements, with no historical record of actions occurring within the system, DEED and MNIT are not able to effectively monitor for unauthorized or erroneous actions.

RECOMMENDATION

DEED and MNIT should ensure that the Unemployment Insurance system's logging and monitoring controls are implemented as required by MNIT's Security Logging and Monitoring Standard.

Threat and Vulnerability Management

Threat and vulnerability management is a risk-based approach to discovering, prioritizing, and remediating vulnerabilities and misconfigurations in IT environments. MNIT's Threat and Vulnerability Management Standard sets the baseline requirements for executive branch agencies to identify, prioritize, and address information security threats and vulnerabilities.⁴⁷ Based on our review, we found that DEED and MNIT

⁴⁵ Minnesota Information Technology Services, *Security Logging and Monitoring Standard*, version 1.7, Control 10, October 1, 2023.

⁴⁶ *Ibid.*, Control 11, October 1, 2023.

⁴⁷ Minnesota Information Technology Services, *Threat and Vulnerability Management Standard*, version 1.7, October 1, 2023.

generally complied with the Threat and Vulnerability Management Standard and adequately detected and managed technical vulnerabilities based on risk and impact.

MNIT has developed a centralized process to scan all agency computers in MNIT's physical and cloud data centers for both vulnerabilities and compliance with baseline configuration standards. To be effective, MNIT requires state entities to install software—called an “agent”—on each device that needs to be tested.⁴⁸ Once installed, the agent gathers information that shows whether the device may have vulnerability problems and reports the result to a central console, which is reviewed by MNIT. MNIT requires that state entities keep the software current.

FINDING 5

DEED and MNIT do not adequately maintain scanning agents on essential technical devices that support the Unemployment Insurance system.

We sample tested 10 of the 47 primary computer servers that support the UI system to validate that vulnerability scanning occurred and that identified vulnerabilities were part of a remediation plan. During our testing, we found that all sampled servers had outdated versions of the agents installed.

When we reviewed MNIT's process for updating the scanning software, we discovered some confusion on roles and responsibilities for the update and maintenance of the software. MNIT's central support staff told us that servers in MNIT's cloud must be maintained by individual system administrators supporting the agencies. However, we were told by MNIT staff supporting DEED that updates to software, such as the scanning agent, are a central responsibility. Because each group of IT support staff thought the other group was responsible for updating the software, no one had updated it. Without the most current version of the scanning software, scanning results may not be complete, and, in some cases, it may prevent DEED and MNIT from identifying all possible vulnerabilities.

RECOMMENDATIONS

- **DEED and MNIT should ensure that vulnerability and configuration scanning software is properly updated on the Unemployment Insurance system.**
 - **MNIT should clarify system maintenance responsibilities for its cloud-hosted system to ensure that all supporting software remain up to date.**
-

⁴⁸ Minnesota Information Technology Services, *Secure Configuration Standard*, version 1.7, Control 34, October 1, 2023.

Disaster Recovery Planning

Disaster recovery planning for information technology systems helps state agencies be prepared to restore or recover priority systems if service interruptions occur.⁴⁹ Minnesota Executive Order 24-01 requires each state entity to develop a Continuity of Operations Plan and outlines what should be included in the plan. The order requires MNIT to establish information technology disaster recovery plans that align with agencies' priority services.⁵⁰

MNIT has established a policy and a standard outlining disaster recovery planning actions and requirements.⁵¹ Together, these documents outline the requirements for information technology disaster recovery planning activities, including plan development, distribution, review, training, and testing of the plan.

DEED has classified the UI system as a "Priority 2" system due to its economic importance, which means that in the case of a disaster, the UI system must be recovered within the first week of interruption.⁵² However, the UI system disaster recovery plan states that the system should be restored within 48 hours. Although DEED has defined this 48-hour recovery time objective for restoration, DEED has also identified an "immediate" recovery point objective. This means that DEED requires that no data held in the UI system can be lost as the result of a disaster. To comply with the immediate recovery objective, MNIT and DEED have replicated the key database and access systems to prevent data loss.

The disaster recovery strategy for DEED's UI system leverages cloud technologies to ensure that the system can be restored in the event of a disaster within its current hosting zone, but in a data center that is geographically separate from the primary hosting location. We believe that this recovery strategy has the necessary technical components in place to meet DEED's 48-hour recovery time objective. However, we identified certain documentation gaps within the disaster recovery plan itself that could impact MNIT and DEED's ability to meet the 48-hour recovery time objective.

⁴⁹ The Office of the Legislative Auditor released a related audit in September 2022 to determine whether MNIT and selected state agencies had disaster recovery plans to minimize the recovery time of key systems if a major disruptive event or disaster were to occur. The UI system was not one of the four systems included in the scope of that audit. Office of the Legislative Auditor, Financial Audit Division, *Disaster Recovery Strategies for Critical IT Systems* (St. Paul, September 2022).

⁵⁰ State of Minnesota Executive Order 24-01, "Directing the Development and Maintenance of the Minnesota Continuity of Government Plan and Agency Continuity of Operations Plans," January 18, 2024.

⁵¹ Minnesota Information Technology Services, *Information Technology Disaster Recovery Planning Policy*, version 1.6, October 1, 2023; and Minnesota Information Technology Services, *Information Technology Disaster Recovery Planning Standard*, version 1.7, October 1, 2023.

⁵² To assist with prioritization, MNIT and state agencies use four categories that group state services by recovery time objectives. Priority 1 is used for activities that must remain uninterrupted or must be recovered within 24 hours. Priority 2 is assigned to activities that can be interrupted temporarily or might be periodic in nature but must be recovered within the first week of interruption. Priority 3 is assigned for activities that can be interrupted temporarily but must be recovered within the first 30 days of interruption. Priority 4 is reserved for those activities that can be suspended for at least 30 days.

FINDING 6

DEED and MNIT did not document their reviews, updates, or testing of the Unemployment Insurance system's disaster recovery plan.

For the UI system, MNIT's disaster recovery planning standard requires at least an annual review and update of the disaster recovery plan.⁵³ However, the system disaster recovery plan DEED provided to us in March 2023 was last updated on October 21, 2021. Because technology changes rapidly, disaster recovery plans must be kept current. Further, the UI system is currently undergoing many changes as part of its modernization efforts; therefore, updates are that much more important to minimize the risks of outdated documentation.

During a disaster, outdated information within the plan could increase the amount of time that it takes for DEED and MNIT to fully restore the UI system. To help track plan versions, MNIT's disaster recovery plan template includes a section to document annual reviews and updates. Although DEED and MNIT told us that they had reviewed their plan in the last year and no updates were needed, the disaster recovery plan contained no documentation of a review or the required signatures from those accountable for the system.

MNIT's disaster recovery planning standard also requires annual testing of recovery plans.⁵⁴ For testing exercises, the security standards require that DEED and MNIT document test results and any identified deficiencies in an improvement plan.⁵⁵ Training and testing are key activities to ensure that all staff involved in disaster recovery are aware of their responsibilities and that the plan itself contains all necessary information required for restoration. During our audit, neither DEED nor MNIT were able to provide us with any documentation of system recovery exercises. DEED noted that system rebuilds were a normal process prior to 2020, but due to COVID-19 pandemic business disruptions, normal system recovery testing had not been performed.

RECOMMENDATION

DEED and MNIT should ensure that disaster recovery plans for the Unemployment Insurance system are reviewed, updated, and tested annually.

MNIT staff supporting the UI system are very familiar with the system and its technical operation. However, in the event of a disaster, these key staff members may not be available to respond to a call to recover the system. Therefore, current, complete, and clear documentation must be maintained within the disaster recovery plan to ensure that other MNIT staff can be successful in recovering the system.

⁵³ Minnesota Information Technology Services, *Information Technology Disaster Recovery Planning Standard*, version 1.7, Control 3, October 1, 2023.

⁵⁴ *Ibid.*, Control 5, October 1, 2023.

⁵⁵ *Ibid.*

MNIT's disaster recovery planning standard mandates that disaster recovery plans must provide for the recovery and reconstitution of the system "in a trusted, secure, and verifiable manner."⁵⁶ The security standards outline expectations that the disaster recovery plan includes reinstallation of application and system software, reestablishment of configuration settings, and full testing or verification of the system's viability following recovery.

Within the UI system disaster recovery plan, we noted that MNIT had documented many of the restoration processes in detail. However, some key processes, including steps to validate that the system is restored and functioning properly, were not documented in the same level of detail.

FINDING 7

DEED and MNIT did not fully document some key processes necessary to ensure full recovery of the Unemployment Insurance system in case of a disaster.

We found some processes where the plan contained placeholders, incomplete steps, or work-in-progress draft language. For example, details on processes to restore the system's load-balancing technologies, or processes to rebuild data after a ransomware incident, were noted within the plan but were incomplete. Additionally, we found insufficiently documented testing or verification procedures necessary to validate the viability of a recovered system. Without specific verification steps and procedures documented, staff may have varying interpretations of what must be done and overlook necessary system functions.

More detailed steps could include procedures or steps to confirm that an applicant can log into the system or submit an unemployment claim, and/or steps to confirm that payments can be processed. DEED and MNIT may have these procedures documented elsewhere, such as part of a release or deployment checklist, but they should also be contained within the UI system's disaster recovery plan.

RECOMMENDATION

DEED and MNIT should ensure that its disaster recovery plan for the Unemployment Insurance system contains documentation of all key processes and procedures necessary to successfully recover and validate the system.

Secure System Configuration

Secure system configuration management is a process that involves adjusting the default settings of an information system to increase security and reduce risk. Misconfigurations can lead to various problems, including poor system performance, noncompliance with federal or state requirements, inconsistencies between servers, and security vulnerabilities that may be exploited by malicious actors.

⁵⁶ Minnesota Information Technology Services, *Information Technology Disaster Recovery Planning Standard*, version 1.7, Control 13, October 1, 2023.

To help ensure that state systems are securely configured, MNIT has issued its secure configuration standard that highlights 55 configuration-related controls.⁵⁷ MNIT also develops specific technology configuration standards for common operating systems that identify the specific security settings IT staff should apply to each system. In general, these technology standards follow the recommendations documented within the Center for Internet Security benchmarks.⁵⁸

To validate that computer desktops, servers, and other infrastructure technologies have been properly configured, the security industry has developed tools that can scan devices and compare actual configuration settings to the best practice recommendations. MNIT requires that these scans be performed at least monthly on all computer systems that require the highest level of data protection, such as the UI system.⁵⁹ As part of our audit, we validated that MNIT security teams regularly scanned the UI system for compliance with secure configuration requirements. While we confirmed that MNIT performed the scans, we noted that they did not apply all recommended security settings.

FINDING 8

In some cases, DEED and MNIT did not implement recommended security configurations for the Unemployment Insurance system, nor did they document, within MNIT's centralized risk and compliance tool, the rationale for deviating from the recommended configurations.

As part of their efforts to modernize the UI system, DEED and MNIT contracted with an external audit firm to perform an independent validation and verification of the UI system to help identify project risks. As part of this review, the external audit firm performed its own configuration scans in January 2022, on DEED's UI system servers, using Internal Revenue Service security guidelines and standards set by the National Institute of Standards and Technology.⁶⁰ The external audit firm found that the UI system did not meet or only partially met 29 of 266 recommended configurations.

As part of our audit work, we specifically performed a secondary review to determine whether DEED and MNIT had addressed the findings identified by the audit firm. Specifically, we tested the 16 highest-risk recommendations to determine if DEED and MNIT had implemented the recommended security configurations. We found that DEED and MNIT had not implemented 3 of the 16 security configurations we tested.

For the remaining 13 recommendations tested, DEED and MNIT did not fully implement the recommendations because they were either not appropriate for all servers, or could not be implemented due to the current architecture of the UI system. DEED and MNIT

⁵⁷ Minnesota Information Technology Services, *Secure Configuration Standard*, version 1.7, October 1, 2023.

⁵⁸ The Center for Internet Security is a nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practice security solutions. It draws on the expertise of security and IT professionals from government, business, and academia from around the world. Center for Internet Security, "Hardening Images," <https://www.cisecurity.org/cis-hardened-images>, accessed February 20, 2024.

⁵⁹ Minnesota Information Technology Services, *Threat and Vulnerability Management Standard*, version 1.7, Control 9, October 1, 2023.

⁶⁰ The IRS Safeguard Computer Security Evaluation Matrix provides system configuration guidelines for IT environments that receive, process, or store federal tax information.

documented the reason for the exceptions, as required by MNIT's risk management standard, and, in some cases, DEED and MNIT documented controls to mitigate the risk created by the exception.⁶¹ However, DEED and MNIT did not document these exceptions, as required, within MNIT's centralized risk and compliance tool.⁶²

We also noted that one of the configuration weaknesses allowed for the exposure of some potentially sensitive data. Because most files were several years old, the data appeared to be from prior project efforts and were no longer needed. With improper configurations and unneeded sensitive files being retained, the agency is exposed to unnecessary risk of a data breach.

RECOMMENDATIONS

- **DEED and MNIT should implement recommended security configurations when appropriate.**
 - **DEED and MNIT should document, within MNIT's centralized risk and compliance tool, system configuration exceptions that do not meet MNIT's security standards.**
 - **DEED and MNIT should not retain sensitive documents longer than is necessary.**
-

⁶¹ Minnesota Information Technology Services, *Information Security Risk Management Standard*, version 1.7, Controls 5-6, October 1, 2023.

⁶² *Ibid.*, Control 5, October 1, 2023.

Unemployment Insurance System Eligibility Control Review

Our audit also examined whether the Department of Employment and Economic Development (DEED) and Minnesota Information Technology Services (MNIT) had adequate IT processes in place to verify applicants' eligibility for unemployment insurance (UI) benefits. The United States Department of Labor mandates that states implement certain data-matching processes to help verify an applicant's eligibility; they also strongly recommend additional data-matching solutions.⁶³ As part of our review, we examined to what extent the UI system interfaces with the "strongly recommended" data-matching solutions.⁶⁴ Specifically, we looked at the UI system's interfaces with the Interstate Connection Network, Prisoner Update Processing System, and UI Integrity Data Hub.

Unemployment Insurance Interstate Connection Network (ICON)

ICON provides real-time information to assist state staff in identifying if a UI applicant has a UI claim or wages in another state. ICON—using its own interfaces with federal agencies—also allows a state to immediately verify an applicant's Social Security number. Using data analysis, a review of system documentation, and discussions with technology professionals, we confirmed that DEED regularly exchanges data with ICON. We confirmed DEED's various interfaces with ICON occurred both in real-time and on a scheduled basis, depending on the data exchanged.

While the UI system utilizes ICON for data validation, DEED and MNIT have not taken advantage of other available information sources—such as the Prisoner Update Processing System or the UI Integrity Data Hub—to help validate the identity, income status, or employment status of applicants.

FINDING 9

DEED uses various external and manual processes to identify suspicious transactions and potentially ineligible individuals, rather than automating these processes within the Unemployment Insurance system.

Prisoner Update Processing System (PUPS)

To be eligible for UI benefits, an individual must be able to work, available to work, and actively seeking work. Incarcerated individuals do not typically meet the eligibility requirements to receive UI benefit payments as they would not be able or available to work

⁶³ U.S. Department of Labor, Unemployment Insurance Program Letter No. 23-20, *Program Integrity for the Unemployment Insurance (UI) Program and the UI Programs Authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020 - Federal Pandemic Unemployment Compensation (FPUC), Pandemic Unemployment Assistance (PUA), and Pandemic Emergency Unemployment Compensation (PEUC) Programs*, May 11, 2020, 8.

⁶⁴ *Ibid.*

while incarcerated. For this reason, the U.S. Department of Labor strongly encourages state workforce agencies to regularly compare UI claims with prisoner records to help ensure UI benefits are only paid to eligible individuals.

Despite the recommendations by the U.S. Department of Labor, DEED and MNIT are not utilizing PUPS to assist with eligibility determinations for UI applicants or recipients of UI benefits. DEED checks eligibility of applicants using a contracted data source and manual processes external to the UI system. However, DEED indicated to us that it intends to use PUPS data, but the plan has not yet been finalized.⁶⁵ While this project would likely provide strategic value, it is not part of DEED's current modernization plan.

Unemployment Insurance Integrity Data Hub

The U.S. Department of Labor has expanded its service offerings since the COVID-19 pandemic to provide a UI Integrity Data Hub, offering states various tools to prevent and detect fraud. Although the U.S. Department of Labor does not require states to use the UI Integrity Data Hub, they strongly encourage its use and make it available at no cost.⁶⁶ Minnesota, however, is one of the few states that has not yet utilized this service for data matching.⁶⁷ DEED indicated that it believes its staff are already performing some of the same integrity checks and is concerned that the Integrity Data Hub services would result in DEED wrongfully denying an applicant.

While these tools cannot and should not make the ultimate determination that a claim or submission is fraudulent, they can flag potentially suspicious applications and accounts for additional human review.⁶⁸ These tools can also provide automated ongoing monitoring and assurance. Integrating and automating fraud identification and prevention tasks within the UI system can provide DEED with an opportunity to identify ineligible applicants and prevent incorrect payments from being issued.

⁶⁵ DEED submitted an application to access PUPS data in January 2023.

⁶⁶ U.S. Department of Labor, Unemployment Insurance Program Letter No. 24-21, *Encouragement for States to Use the Integrity Data Hub (IDH) available through the Unemployment Insurance (UI) Integrity Center*, May 5, 2022.

⁶⁷ U.S. Department of Labor, *Insights and Successes: American Rescue Plan Act Investments in Unemployment Insurance Modernization* (Washington, DC, November 2023).

⁶⁸ In 2022, OLA released an evaluation report on the UI program's efforts to prevent and detect the use of stolen identities; Office of the Legislative Auditor, Program Evaluation Division, *Unemployment Insurance Program: Efforts to Prevent and Detect the Use of Stolen Identities* (St. Paul, 2022). That report found that the UI system contained a complex set of automated rules that verify applicants' identities and determine their eligibility for benefits. However, the report also noted that DEED staff manually reviewed information that applicants and employers provided to verify applicants' identities and determine their eligibility for benefits. These reviews occur as an additional manual process, outside of the UI system itself.

While these types of enhancements are good candidates for future system modernization projects, we saw no evidence that DEED was including them within its currently scoped strategic modernization portfolio of projects. Although DEED seemed well aware of data-matching services available for use, and identified some valid concerns of using the other system interfaces, we did not see a formal assessment of the options, specifically acknowledging the benefits and risks.

RECOMMENDATIONS

- **DEED and MNIT should evaluate its current manual data-matching processes and look to automate those processes into the Unemployment Insurance system.**
 - **DEED and MNIT should perform and document their analysis of strengths and weaknesses when deciding whether to implement automated data integrity solutions.**
-



OLA

Unemployment Insurance Modernization Program

Modernizing government IT systems is essential for improving efficiency, security, service delivery, and overall government effectiveness. Since first implementing the unemployment insurance (UI) employer portal in 2005 and the applicant portal in 2007, the needs of individual users and the ways in which they want to interact with the UI program have evolved. To address these needs, the Department of Employment and Economic Development (DEED) began working with Minnesota Information Technology Services (MNIT) in 2019 on a multiyear endeavor, obligating to date more than \$44 million to strategically modernize components of the UI system. MNIT's January 2024 IT Project Portfolio Summary report listed a completion date for this project as October 31, 2024, and, despite three end-date extensions, it notes the project status as "Green," indicating the program is controlled, in alignment, and proceeding as planned.⁶⁹

As part of this audit, we gained an understanding of the modernization work being performed on the UI system, interviewed DEED leadership, and reviewed project documents. Because a modernization program provides opportunities for improvement in various business and technical areas, our audit considered strategic changes underway to determine if any newly identified audit findings may have already been scheduled for corrective actions. Finally, we benchmarked DEED and MNIT's modernization efforts to best practices.⁷⁰

In general, we found that DEED and MNIT have appropriately managed its modernization projects. However, we noted two concerns. First, DEED and MNIT were not tracking and reporting on all project-related costs. Second, as part of its modernization efforts, DEED and MNIT may have overlooked some opportunities to interface with existing solutions, which could improve customer experiences, reduce manual tasks, and enhance DEED's ability to prevent and detect unemployment insurance fraud.

Unemployment Insurance Modernization: A Phased Approach

DEED has so far committed more than \$44 million to modernize the UI system, with the goals of improving customer experience, strengthening the UI system infrastructure, and implementing functionality in ways that will more easily support future enhancements.⁷¹ DEED and MNIT's strategic modernization projects for the UI system

⁶⁹ Annual IT project portfolio summary reports are required by *Minnesota Statutes* 2023, 16E.01, subd. 3(f); and Minnesota Information Technology Services, *IT Project Portfolio Summary* (St. Paul, January 15, 2024).

⁷⁰ Our review of the modernization program considered best practices and recommendations from prior OLA reports: Office of the Legislative Auditor, Special Reviews, *Factors That Contributed to MNLARS Problems* (St. Paul, 2019); and Office of the Legislative Auditor, Financial Audit Division, *Minnesota Vehicle Title and Registration System: Final Project Audit* (St. Paul, 2022).

⁷¹ Originally, in 2020, DEED and MNIT obligated approximately \$20 million for modernization contracts. DEED and MNIT have amended the contracts for changes in deliverables and time extensions, raising the cost of these projects to over \$44 million. DEED told us that they anticipate a third phase of the program; however, DEED and MNIT had not identified specific deliverables, anticipated costs, or an end date by the time of this report release.

currently consist of three phases. The completed first phase consisted of projects to modernize the user interface of the UI system, including implementation of a modern web framework and making the system compatible with mobile devices. This phase also included work to provide multilingual capabilities and to improve correspondence functions within the system.

Total contract costs for this first phase included a single contract with Deloitte Consulting, LLP (Deloitte) for \$6.5 million. The contract was finalized in early 2020. Originally, the work was planned to be completed by May 2021. However, due to COVID-19 pandemic delays, an amendment to the contract extended the work through June 2022.

The second phase of DEED and MNIT's UI modernization program—which is still in progress—consists of more than 35 individual projects. Nearly half of these projects address “backend” system issues, including upgrades to address system security and other technical issues, or converting to more modern development frameworks.⁷² Other projects include upgrading document management software, fixing security vulnerabilities, purging data, and improving sign-on functionality. To complete the work, DEED and MNIT contracted with Deloitte to assist with (1) project scope and requirements validation, (2) system coding, (3) system testing, (4) knowledge transfer and training, and (5) system implementation and cutover.⁷³

The second contract with Deloitte was originally executed in March 2020, with a completion date of April 2022, and total cost of \$13,863,532. Over the course of two years and seven amendments for scope changes and time extensions, the contract for this second phase now expires in March 2024 and totals \$36,711,044.⁷⁴ Exhibit 2 shows all amendments to this contract through February 2024.

DEED and MNIT contracted with a second contractor, Berry Dunn, for approximately \$769,000 to perform Independent Verification and Validation audits to help identify project risks.⁷⁵

As of September 2023, DEED, MNIT, and Deloitte had completed approximately 24 of the 35 phase two program projects.

⁷² Backend systems are the tools and components that work behind the scenes to support web applications. They include programming languages, databases, frameworks, and communication mechanisms that handle the server side of web development. They are responsible for managing the servers, databases, and the application logic that enables interaction between the servers and the end users' browsers.

⁷³ DEED and MNIT signed two contracts with Deloitte—one for each phase—totaling approximately \$43.2 million.

⁷⁴ The January 2024 IT Project Portfolio Summary report—mandated by *Minnesota Statutes* 2023, 16E.01, subd. 3(f)—listed a finish date for this project as October 31, 2024. Therefore, we believe that the contract between MNIT and DEED and their vendors may be further amended to reflect this extended timeline.

⁷⁵ *Minnesota Statutes* 2023, 16E.04, subd. 3, requires an outside entity to conduct a risk assessment and prepare a mitigation plan for all IT projects estimated to cost more than \$5 million. Additionally, *Minnesota Statutes* 2023, 16E.01, subd. 3(e), requires an outside entity to conduct an annual independent audit when technology projects are expected to cost over \$10 million. These audits are often referred to as an Independent Verification and Validation assessment.

Exhibit 2**Summary of Unemployment Insurance Modernization Contract Amendments with Deloitte (Second Phase)**

Contract Stages	Date of Amendment	Contract Completion Date	Total Contract Amount
Original Contract	03/27/2020	04/30/2022	\$13,863,532
Amendment #1	09/17/2020	04/30/2022	18,759,823
Amendment #2	11/17/2020	04/30/2022	18,759,823
Amendment #3	03/27/2021	04/30/2022	19,766,707
Amendment #4	09/08/2021	04/30/2022	21,348,509
Amendment #5	04/01/2022	01/31/2023	36,813,509
Amendment #6	06/03/2022	01/31/2023	36,711,044
Amendment #7	12/22/2022	03/26/2024	36,711,044

Source: Office of the Legislative Auditor, based on data in the state's accounting system, as of February 29, 2024.

DEED told us that they anticipate a third phase of the program; however, DEED and MNIT had not identified specific deliverables, anticipated costs, or a completion date by the time of this report release. DEED plans to issue a separate contract for this project phase. DEED has not yet identified funding for this third phase.⁷⁶

As of the end of calendar year 2023, DEED and MNIT have paid Deloitte approximately \$25.8 million for work completed and Berry Dunn \$649,000. Exhibit 3 summarizes total payments by vendor and state fiscal year.

By law, total project costs should include “direct staff costs, all supplemental contract staff and vendor costs, and costs of hardware and software development or purchase.”⁷⁷

Exhibit 3**Unemployment Insurance Modernization Total Payments by Vendor and Fiscal Year, January 1, 2020, through December 31, 2023**

Vendor	2020	2021	2022	2023	2024	Total
Berry Dunn	\$ —	\$ 166,337	\$ 332,679	\$ 150,000	\$ —	\$ 649,016
Deloitte	<u>26,325</u>	<u>4,656,667</u>	<u>9,876,015</u>	<u>6,668,750</u>	<u>4,570,466</u>	<u>25,798,223</u>
Total	\$26,325	\$4,823,004	\$10,208,694	\$6,818,750	\$4,570,466	\$26,447,239

Source: Office of the Legislative Auditor, based on data in the state's accounting system.

⁷⁶ All unemployment insurance jurisdictions, except for Minnesota, have received part of the \$782.9 million American Rescue Plan Act grants that have been designated for UI modernization efforts; U.S. Department of Labor, *Insights and Successes: American Rescue Plan Act Investments in Unemployment Insurance Modernization* (Washington, DC, November 2023).

⁷⁷ *Minnesota Statutes* 2023, 16E.03, subd. 1(f).

FINDING 10**DEED and MNIT do not report on all Unemployment Insurance system project-related costs.**

DEED and MNIT have a responsibility to accurately report on information technology project costs.⁷⁸ Within MNIT's IT Project Portfolio Summary reports, DEED and MNIT have reported an estimated overall project budget of approximately \$43,211,000 for phases one and two of the Unemployment Insurance Strategic Modernization project. These estimates were the contract amounts that MNIT encumbered for Deloitte; \$6.5 million for phase one and \$36,711,044 for phase two. However, these project estimates did not include the estimated audit costs of approximately \$769,000. In addition, the estimated budgets do not factor in the costs related to DEED and MNIT staff time, purchased software licenses, cloud server and workstation costs, or other indirect costs. By not including these costs, DEED and MNIT are underreporting the cost of the modernization project.

MNIT employees generally track their time to projects they have been working on using specific cost codes. One such cost category was labeled as "UI Strategic Projects." Over the past three fiscal years, ten MNIT staff have collectively logged an average of approximately 5,500 hours per year to this program. The total amount charged to this cost category, through the end of December 2023, has exceeded \$1.1 million. However, this cost category has not been included in the budget or expense reports for the UI system modernization program. Additional costs should be expected, as this cost category did not include hours charged by known MNIT project participants, nor did it include any staff time for DEED's program staff working on the projects.

When we asked why all project costs were not included in the budget, a DEED representative noted some conflicting directions from MNIT regarding IT project budgets. Although MNIT's project management procedures provide directions for adding labor and other project costs, those comments were reminiscent of what we heard from the Department of Public Safety during our audit of the new Vehicle Title and Registration System.⁷⁹ For that audit, we recommended that MNIT should develop guidance and recommendations for agencies developing budgets for large or multiyear IT projects.⁸⁰

RECOMMENDATIONS

- **DEED and MNIT should track and report on all project-related costs, including those related to DEED and MNIT staff time.**
 - **MNIT should develop guidance and recommendations for agencies developing budgets for large or multiyear IT projects.**
-

⁷⁸ *Minnesota Statutes* 2023, 16E.01, subd. 3(f) mandates that MNIT report on information technology costs associated with projects. For the state's annual comprehensive financial report, Minnesota Management and Budget's Statewide Operating Policies 0106-01 through 0106-09 require all state agencies to maintain up-to-date and complete records of all existing capital assets, including information system betterments and improvements.

⁷⁹ Minnesota Information Technology Services, *Instructions on how to add budget and project cost in Sciforma*, February 2022.

⁸⁰ Office of the Legislative Auditor, Financial Audit Division, *Minnesota Vehicle Title and Registration System: Final Project Audit* (St. Paul, 2022), 27.

Unemployment Insurance Modernization: Login Project

One of the modernization projects aims to improve how the UI system authenticates users. The goal of this project is to improve password compliance and self-serve user experience. Due to the number of identity and access management issues we have noted in this report, we encourage DEED and MNIT to complete this project. However, we have some concerns regarding the direction of this project.

FINDING 11

DEED and MNIT continue to custom build identity and access management functionality into the Unemployment Insurance system, rather than modernizing to an off-the-shelf solution.

As part of the project, DEED and MNIT have made a deliberate decision not to utilize existing identity and access management solutions. Rather than looking to purchase a vendor-provided identity access management solution, or integrate the UI system with Minnesota's Enterprise Identity and Access Management (MNEIAM) application, DEED plans to continue building this functionality into the UI system.⁸¹ DEED told us that it made this decision based on the licensing and ongoing maintenance and support costs.⁸²

In our opinion, the decision to build custom functionality to validate user identity and authenticate users is contrary to industry best practices and guidance from Minnesota's Technology Advisory Council.⁸³ Additionally, this decision does not align with MNIT's strategic plan. By DEED and MNIT building identity and access management functionality uniquely for the UI system, applicants and businesses will need to have UI-specific accounts and passwords, rather than accessing a streamlined process in which these individuals use credentials they have already established to interact with other state programs.

RECOMMENDATION

DEED and MNIT should consult with the Technology Advisory Council, and reaffirm its decision to custom build identity and access management functionality.

⁸¹ The U.S. Department of Labor encourages use of ID verification systems, such as Login.gov and ID.me. MNEIAM is a vendor-provided identity and access management service managed by MNIT.

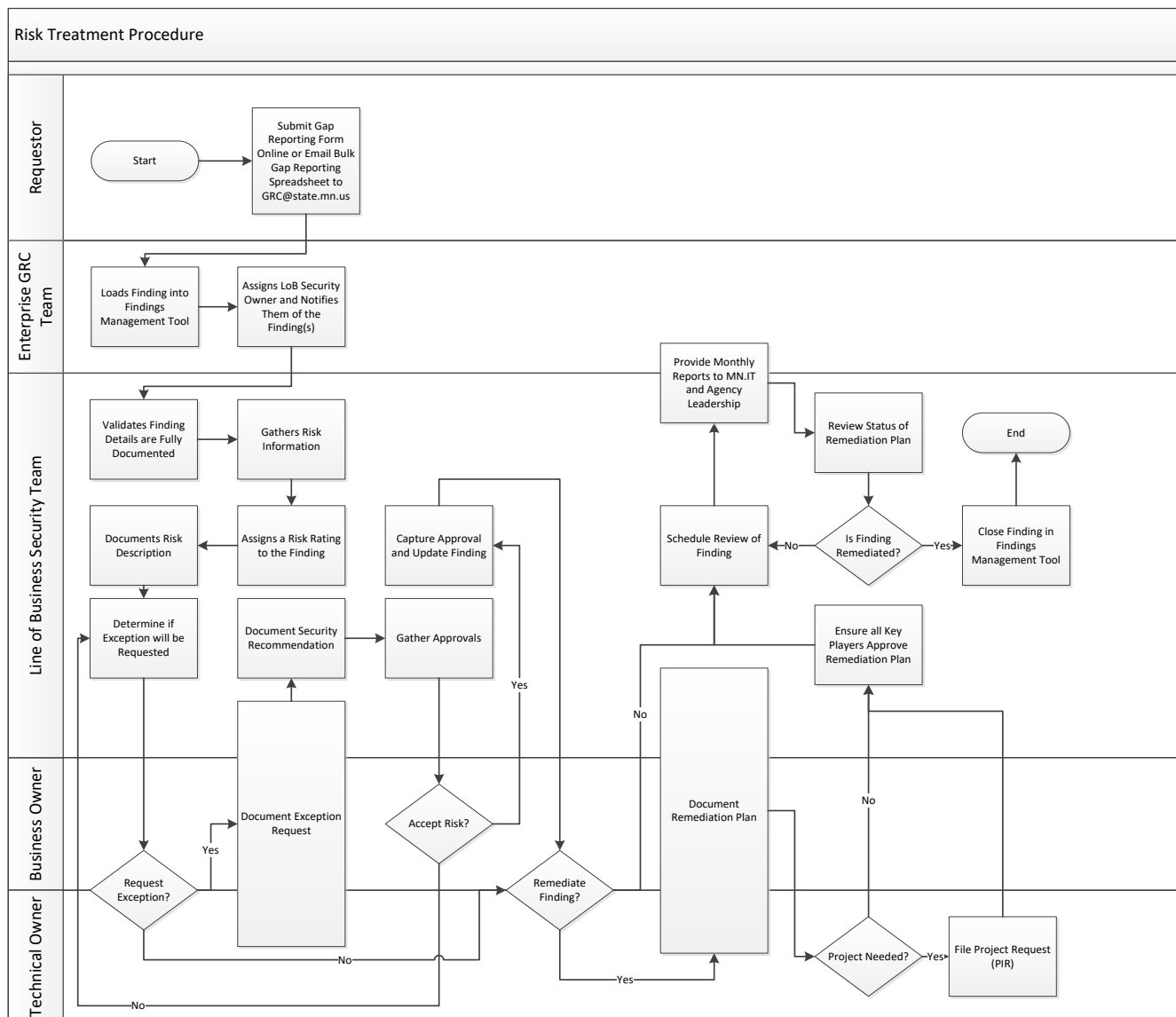
⁸² Identity and access management license, maintenance, and support cost estimates were not included in current budget estimates.

⁸³ *Minnesota Statutes* 2023, 16E.036, created the Technology Advisory Council as a permanent body to advise MNIT and executive branch agencies on strategic information technology initiatives and service delivery. In its June 2020 report on information technology, the council made recommendations for improvements, one of which was to leverage industry solutions. *Report of the State of Minnesota Blue Ribbon Council on Information Technology*, (St. Paul, June 2020), 28.



OLA

Appendix: MNIT's Information Security Risk Treatment Procedure



Source: Minnesota Information Technology Services, *Information Security Risk Treatment Procedure*, version 1.0, January 1, 2017.



OLA

April 26, 2024

Judy Randall
Legislative Auditor
Office of the Legislative Auditor
Room 140 Centennial Building
658 Cedar Street
Saint Paul, MN 55155-1603

Dear Ms. Randall,

On behalf of the Minnesota Department of Employment and Economic Development (DEED) and Minnesota IT Services (MNIT), thank you for the opportunity to respond to this audit report. We first offer general comments on this audit report, and then respond to the specific findings.

General Comments

Minnesota's Unemployment Insurance (UI) program has continuously set a standard of excellence, leading UI programs nationwide in performance, timeliness, and integrity. Through innovative technological solutions and robust infrastructure, DEED and MNIT have worked to deliver seamless and efficient services to Minnesota residents. This has not only ensured timely and accurate processing of unemployment claims in the face of unprecedented pandemic-era demands on its services, but has also enhanced accessibility, responsiveness, and transparency for users. Minnesota's UI program stands as a prime example of effective government collaboration and technological advancement, setting a benchmark for UI programs across the country.

Both DEED and MNIT value audits as an important part of ensuring our programs continue to maintain a high level of performance. IT audits provide independent assurance regarding the security and reliability of digital systems, identifying potential vulnerabilities, and implementing best practices to mitigate risks.

We would like to note, however, that the approach taken with this audit differed significantly from the methodology or the outputs in other professional IT audits. Specifically:

Scope of audit. The UI program has its IT components regularly audited by multiple entities, including the Internal Revenue Service, the Social Security Administration, the independent third-party risk consultant BerryDunn, and others. These IT audits are tightly scoped, rigorous, and follow internationally accepted audit best practices.

DEED and MNIT welcome outside perspectives on the effective operation of key programs, including audits from the aforementioned entities, as well as the Office of the Legislative Auditor. While we understand that audit scope may evolve as audits progress, we would note that many of the goals of this audit have been covered in previous external audits, and that several of this audit's objectives altered throughout the course of the audit. These changes increase the staff time required to respond and differ from our experience in previous audits.

Lack of risk categorization. The inclusion of severity of findings in audit reports would greatly benefit agencies' ability to prioritize risk mitigation activities, and would help ensure program integrity, especially for programs that are often operated with narrow budget margins. The International Organization for Standardization's ISO 19111 proposes major nonconformity, minor nonconformity, observation / opportunity for improvement as categories which help to taxonomize risk. Another commonly used framework is to cite findings as representing a critical, high, medium, or low risk.

Comments on Findings

Finding 1: DEED and MNIT inaccurately concluded that the UI System complied with all information security control requirements and did not report known issues within MNIT's central database of risks.

We would note that the UI program tracks a variety of non-IT risks as well as IT risks. These risks are discussed routinely, including at monthly Governance meetings with both MNIT and DEED agency leadership.

Finding 2: DEED and MNIT do not have a process for identifying and securely deleting data records within the UI System that exceed defined retention periods.

As noted in the report, MNIT and DEED are working to both update retention schedules and implement updated purge processes in 2024. The data involved are complex with many dependencies and users. Development of data deletion criteria in a variegated environment must be done carefully and thoughtfully.

Finding 3. DEED and MNIT have not fully implemented one-quarter of the identity and access management requirements designed to help protect the UI System.

As noted at page 23 of the report, DEED and MNIT have active projects underway to strengthen identity and access management controls both in the short and long term.

Finding 4. DEED and MNIT do not comply with all provisions of MNIT's Security Logging and Monitoring Standard for the UI System.

DEED and MNIT have an active project to remediate this finding and ensure that all relevant environments are enrolled in MNIT's logging and monitoring ecosystem.

Finding 5. DEED and MNIT do not adequately maintain scanning agents on essential technical devices that support the UI System.

DEED and MNIT have remediated this finding and confirmed that all relevant devices are properly enrolled in scanning.

Finding 6. DEED and MNIT did not document their review, updates, or testing of the UI System's disaster recovery plan.

The Federal Disaster related to the pandemic began in 2020 and [ended in May 2023](#). For the entire duration of the Federal and State Disaster, the program continually implemented elements of the existing disaster recovery plan, identified additional elements that the program needed but weren't explicitly in the plan, and documented as appropriate. With conclusion of the disaster, the MNIT and DEED teams have resumed regular testing of the plan.

Finding 7. DEED and MNIT did not fully document some key processes necessary to ensure full recovery of the UI System in case of a disaster.

No comments on this finding.

Finding 8. In some cases, DEED and MNIT did not implement recommended security configurations for the UI System, nor did they document, within MNIT's centralized tracking tool, the rationale for deviating from the recommended configurations.

Baseline recommended security configurations provide general best practices. However, it is not unusual to depart from baseline configurations depending on the specific nature of the application involved, particularly in complex or multicomponent systems such as the UI system. As the report notes, "DEED and MNIT documented the reason for the exceptions, as required by MNIT's risk management standard..."

Finding 9. DEED uses various external and manual processes to identify suspicious transactions and potentially ineligible individuals, rather than automating these processes within the UI System.

We disagree with the way that this finding is presented. It presents a misleading perspective on the program's approach to integrity matching, and it contradicts previous OLA reports on the subject.

As cited in this report, "[OLA's previous UI] report found that the UI System contained a complex set of automated rules that verify applicants' identities and determine their eligibility for benefits." As noted in this report, the UI system already uses ICON, which provides real-time information to immediately verify an applicant's Social Security Number and identify if an applicant has a UI claim or wages in another state. In addition, DEED has already implemented several data matching methods and tools that help validate the identity, income, and employment status of applicants, which have successfully prevented substantial amounts of potentially fraudulent payments. Further, as the OLA noted in a footnote on page 33 of the

report, DEED/UI has an active application to receive PUPS access, which was submitted to the Social Security Administration in January 2023. All these tools are varying forms of process automation.

We believe an “all of the above” approach is the correct approach: thoughtful use of automated third-party data analysis, where appropriate, and where the data tools do not create their own undue risks or problems; automated data analysis and rules based on internal program data; and additional data analysis as emergent threats and trends emerge. All such tools are needed to stay on top of a constantly shifting cybersecurity landscape. All these tools can be a key part of program integrity, but it is not possible to “automate away” risk or outsource it to a third-party vendor, as this report seems to suggest, and a nuanced and careful consideration of any data sharing is needed to avoid creating its own risks.

Finding 10. *DEED and MNIT do not report on all UI System project-related costs.*

We note that DEED and MNIT closely track all program budget items.

Finding 11. *DEED and MNIT continue to custom-build identity and access management functionality into the UI System, rather than modernizing to an off-the-shelf solution.*

We disagree with the way that this finding is presented. The state’s existing enterprise IAM solution is currently being replaced. Configuration details are still being finalized, but MNIT anticipates availability this summer for a new cloud-based statewide solution.

DEED and MNIT have sought to identify interim solutions to provide IAM capabilities that were not previously fiscally feasible before legislative investments MNIT received in 2023.

Understanding that the current solution was reaching end-of-life, it would not have been prudent to implement the current offering.

It is important for agencies to find solutions to implement solutions and controls in current implementations while modernized solutions are implemented. Current and upcoming portfolio work will allow for convergence with this new solution, and interim efforts are required to prepare for this alignment. This is not the creation of a separate IAM solution, but rather preparatory work required to move to any new IAM solution, as well as interim steps which will strengthen various security elements to directly address some of the issues raised in Finding 3.

We would also note that, to date, the Technology Advisory Council (TAC) has not provided tactical affirmation of MNIT and agencies’ discrete technical solutions and decisions; to do so would be a significant departure from their current role as an advisory body providing strategic advice and counsel to state agencies and require a significantly larger commitment of time and resources from the TAC to engage at such a tactical level.

In Summary

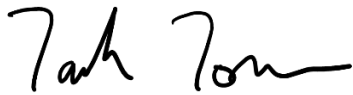
We welcome the input and feedback that external audits provide that help both our agencies administer programs that serve Minnesotans. By highlighting findings and offering

recommendations for improved administration and utilization of state resources, we can collaboratively improve service delivery.

We recognize that we arrive at these evaluations with sometimes greatly differing perspectives, and we appreciate the opportunity to provide feedback. Thank you for the opportunity to include this response letter to provide our perspective, and highlight areas where feedback provided has not been incorporated into the final version of the report.

We hope that the issues raised in this letter can be of use to your office, and to state policymakers more generally, as future IT audits are considered and conducted.

Sincerely,

A handwritten signature in black ink, appearing to read "Tarek Tome". The signature is fluid and cursive, with a long horizontal stroke at the end.

Tarek Tome

Commissioner; Minnesota IT Services

A handwritten signature in black ink, appearing to read "Matt Varilek". The signature is fluid and cursive, with a long horizontal stroke at the end.

Matt Varilek

Commissioner; MN Department of Employment and Economic Development



OLA

Financial Audit Staff

Judy Randall, *Legislative Auditor*
Lori Leysen, *Deputy Legislative Auditor*

Audit Directors

Ryan Baker
Jordan Bjonfald
Kayla Borneman
Mark Mathison
Heather Rodriguez
Valentina Stone
Scott Tjomsland
Zach Yzermans

Audit Coordinators

Joe Sass

Audit Team Leads

Shannon Hatch
Gabrielle Johnson
Holly Runia

Senior Auditors

Tyler Billig
Deb Frost
Lisa Makinen
Alec Mickelson
Duy (Eric) Nguyen
Crystal Nibbe
Erick Olsen
Emily Wiant

Auditors

Joseph Anderson
Ria Bawek
Nicholai Broekemeier
Gabrielle Gruber
Dylan Harris
Nicole Heggem
Andrea Hess
Dustin Juell
Christian Knox
Sheena Kurth
Benjamin Path
Julia Schechter
Zakeeyah Taddese
Peng Xiong

For more information about OLA and to access its reports, go to: www.auditor.leg.state.mn.us.

To offer comments about our work or suggest an audit, evaluation, or special review, call 651-296-4708 or e-mail legislative.auditor@state.mn.us.

To obtain printed copies of our reports or to obtain reports in electronic ASCII text, Braille, large print, or audio, call 651-296-4708. People with hearing or speech disabilities may call through Minnesota Relay by dialing 711 or 1-800-627-3529.



Printed on Recycled Paper

OLA | OFFICE OF THE
LEGISLATIVE AUDITOR



Office of the Legislative Auditor
Suite 140
658 Cedar Street
Saint Paul, MN 55155