



Office of the State Auditor

Performance Audit

January 2025

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.

January 29, 2025

Members
Legislative Audit Commission

The Honorable Julie Blaha, State Auditor
Office of the State Auditor

This report presents the results of our performance audit of the Office of the State Auditor (OSA) for the period July 1, 2021, through December 31, 2023. The objectives of this audit were to determine if the office had adequate internal controls over selected financial activities and its information technology assets, and complied with significant finance-related legal requirements.

In accordance with *Minnesota Statutes 2024, 13.37*, subd. 2, we have removed from the public version of our report language from Finding 7 that we deemed likely to substantially jeopardize the security of OSA systems. We discussed the specific details with OSA.

This audit was conducted by Zach Yzermans, CPA (Audit Director); Mark Mathison, CISA, CISSP, CPA Inactive (IT Audit Director); and auditors Ria Bawek; Nicholai Broekemeier; Deb Frost, CISA; Nicole Heggem; Ben Path; and Peng Xiong.

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

Sincerely,



Judy Randall
Legislative Auditor



Lori Leysen, CPA
Deputy Legislative Auditor



OLA

Table of Contents

	<u>Page</u>
Introduction.....	1
Report Summary	3
Conclusions.....	3
Findings and Recommendations	3
Background.....	7
Audit Scope, Objectives, Methodology, and Criteria	8
Payroll Expenditures	13
Employee Pay Rates	13
Pay Rate Increases	14
Payroll Processing.....	15
Holiday Pay.....	15
Overtime Pay	15
Leave Balance Adjustments.....	16
Other Paid Leave.....	17
Separation Pay	17
Nonpayroll Expenditures	19
Equipment and Other Goods and Services	19
Space Rentals	19
Asset Management.....	20
Professional/Technical Services Contracts	23
Employee Expense Reimbursements.....	23
Receipts.....	25
Audit Fees	25
Deposits.....	25
Seminar Workshop Fees	26
Information Technology Security Controls	27
Information Security Program and Risk Management	28
Inventory and Control of IT Hardware and Software Assets.....	30
Security Awareness Training.....	32
Identity and Access Management	33
Physical Security	35
Security Logging and Monitoring.....	35
Network, Data, and Communication Protections.....	37
Office of the State Auditor Response	39



OLA

Introduction

The Office of the State Auditor (OSA) oversees local government finances by auditing local government financial statements and reviewing documents, data, reports, and reported complaints regarding local government activities. The office also collects and analyzes financial information from local governments that serves as the basis of the statutorily required reports it issues.

In this audit, we focused on whether OSA had internal controls to ensure that it safeguarded state resources, appropriately spent state funds, and accurately paid its vendors and employees in compliance with state laws and policies. Auditors focus on internal controls as a key indicator of whether an organization is well managed.

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 2024, 16A.057



OLA

Report Summary

Conclusions

The Office of the State Auditor generally complied with the significant finance-related legal requirements we tested and generally had adequate internal controls. However, we identified instances of noncompliance and an internal control weakness related to asset management.

The Office of the State Auditor implemented some best practices for information technology security controls. However, we identified several areas in which the office should implement additional controls or strengthen existing controls to better protect its information technology resources.

Findings and Recommendations

Finding 1. The Office of the State Auditor did not assign asset numbers to all of its capital asset acquisitions, nor did it record those assets in its capital asset system, as required by its policy. (p. 21)

Recommendations

- The Office of the State Auditor should assign asset numbers to all capital asset acquisitions and record those assets in its capital asset system.
- The Office of the State Auditor should strengthen internal controls over assets to ensure it assigns asset numbers to all of its capital asset acquisitions and records all capital assets in its capital asset system.

Finding 2. The Office of the State Auditor did not manage its asset inventory in compliance with state or office policies. (p. 21)

Recommendations

- The Office of the State Auditor should conduct and document a full physical inventory of assets annually, to comply with both state and office policies.
- The Office of the State Auditor should update its capital asset system to reflect the results of its annual inventories and investigate discrepancies between its physical inventory and capital asset system.

Finding 3. The Office of the State Auditor has not implemented an information security program that aligns with best practices. (p. 28)

Recommendation

The Office of the State Auditor should implement an information security program that aligns with best practices. As part of its implementation, the office should:

- Establish expectations and requirements for its information technology operations and security within office policies, standards, and procedures.
- Conduct security control assessments of its information assets.
- Develop and implement a plan to regularly track information technology vulnerabilities.

Finding 4. The Office of the State Auditor's inventory of information technology hardware and software did not contain important maintenance and security-related information. (p. 31)

Recommendation

The Office of the State Auditor should maintain an inventory of information technology assets that includes information prescribed by best practices.

Finding 5. The Office of the State Auditor has hardware and software that is outdated and no longer supported by its vendors or manufacturers. (p. 32)

Recommendation

The Office of the State Auditor should establish and implement a plan to replace its outdated hardware and software.

Finding 6. The Office of the State Auditor did not conduct annual security awareness training for its employees. (p. 32)

Recommendations

- The Office of the State Auditor should establish requirements for its information security awareness program.
- The Office of the State Auditor should provide security awareness training to its employees on an annual basis.

Finding 7. The Office of the State Auditor did not always follow best practices when authenticating users that access its information technology assets and software. (p. 33)

Recommendations

- The Office of the State Auditor should require more complex passwords for accounts with broad access.
- The Office of the State Auditor should [REDACTED]
[REDACTED].

Finding 8. The Office of the State Auditor does not have a comprehensive security logging and monitoring program in place to detect and respond to security threats. (p. 36)

Recommendation

The Office of the State Auditor should implement a comprehensive security logging and monitoring program.

Finding 9. The Office of the State Auditor does not follow best practices to detect, respond to, and prevent potential threats to its network. (p. 37)

Recommendations

- The Office of the State Auditor should maintain and update network documentation annually, or when significant changes occur.
- The Office of the State Auditor should ensure its network infrastructure is kept up-to-date.
- The Office of the State Auditor should implement necessary network intrusion detection and prevention capabilities.



OLA

Background

Minnesota Constitution, Article V, establishes the Office of the State Auditor (OSA) as part of the executive branch of state government; the office operates primarily under the authority provided in the Minnesota Constitution and *Minnesota Statutes*, Chapter 6. The State Auditor is elected to a four-year term that begins the first Monday in January following the general election.

Julie Blaha was first elected as State Auditor in November 2018 and was re-elected in November 2022.

The mission of OSA is to oversee local government finances for Minnesota taxpayers by helping to ensure financial integrity and accountability in local government activities.

The office is divided into seven divisions:

1. Audit Practice – Conducts financial and compliance audits of local governments, including cities, counties, and other political subdivisions.
2. Constitution – Performs outreach and provides educational resources to state and local officials, local finance professionals, and the public.
3. Government Information – Collects, reviews, compiles, and analyzes financial information from the state’s local governments.
4. Legal and Special Investigations – Provides legal support to all divisions in the office, responds to local government legal inquiries, and investigates allegations of unlawful use of public resources.
5. Operations – Supports all activities within the office by providing the accounting, facilities management, technology support, and human resources services for all divisions.
6. Pension – Oversees local public pension plans and provides support on compliance with various state laws that govern plan administration and investment activity.
7. Tax Increment Financing – Provides oversight for the compliance and controls around proper treatment, use, and reporting of tax increment funds.

The office conducts its audit work from six different locations throughout the state: Duluth, Mankato, Marshall, Moorhead, Rochester, and St. Paul; the accounting and human resources functions are performed only in St. Paul.

Funding for the office comes primarily from the General Fund, with the Tax Increment Financing Division funded by a special revenue account. For auditing services, the Audit Practice Division collects audit fees and deposits them into the General Fund as nondedicated receipts.

Audit Scope, Objectives, Methodology, and Criteria

We conducted this audit to determine whether the Office of the State Auditor had adequate internal controls and complied with significant finance-related legal requirements. The audit scope included payroll expenditures, nonpayroll expenditures, receipts, and general information technology security controls. The period under examination was from July 1, 2021, through December 31, 2023. Exhibit 1 shows the office's appropriations, receipts, and expenditures during the scope of the audit.

Exhibit 1
Appropriations, Receipts, and Expenditures, July 1, 2021, through December 31, 2023

Appropriations	Amount
General Fund ^a	\$39,069,000
Miscellaneous Special Revenue ^b	342,709
Cancelled ^c	(6,226,570)
Total	\$33,185,139

Receipts	Amount
Audit Fees	\$12,992,941
Other Receipts ^d	124,246
Total	\$13,117,187

Expenditures	Amount
Payroll	\$21,081,264
Nonpayroll	3,331,266
Total	\$24,412,530

^a *Laws of Minnesota* 2021, First Special Session, chapter 12, art. 1, sec. 4; *Laws of Minnesota* 2023, chapter 62, art. 1, sec. 4; and *Minnesota Statutes* 2024, 6.91.

^b *Minnesota Statutes* 2024, 469.177, subd. 11.

^c OSA did not spend \$395 from the Fiscal Year 2022 appropriation or \$6,226,174 from the Fiscal Year 2023 appropriation. The Fiscal Year 2023 cancellation includes \$1.5 million of unused funding for the office's School Finance Accountability Team. Each year's amount cancelled back to the General Fund.

^d "Other Receipts" consists primarily of accounting software and seminar fees. See Exhibit 4 for more details.

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

Payroll Expenditures

This part of the audit focused on the accuracy of compensation paid to OSA employees. We designed our work to address the following questions:

- Were the Office of the State Auditor's internal controls adequate to ensure it accurately compensated employees in compliance with applicable legal provisions?
- Did the Office of the State Auditor accurately compensate employees in compliance with applicable legal provisions?
- Did the Office of the State Auditor resolve a prior audit finding?¹

To gain an understanding of OSA's internal controls and compliance, we interviewed its employees. We also analyzed holiday pay, leave balance adjustments, and paid leave to determine compliance with state policy and employment agreements.

Additionally, we tested:

- The starting salaries for a sample of employees hired during the scope of the audit; all pay rate changes for employees in all relevant state bargaining agreements; a sample of pay rate changes for employees covered by the Office of the State Auditor Plan; a sample of retroactive pay rate adjustments; and the salary of the State Auditor.
- A sample of employee timesheets.
- A sample of payroll report reviews.
- A sample of overtime payments.
- A sample of separation payments.
- All compensatory time payoffs.

Nonpayroll Expenditures

This part of the audit focused on expenditures associated with rent, equipment, employee expense reimbursements, professional/technical services contracts, parking fees, and all remaining expenditures for goods and services. We designed our work to address the following questions:

- Were the Office of the State Auditor's internal controls adequate to ensure it safeguarded its financial resources, accurately paid vendors in accordance with management's authorizations, and complied with finance-related legal provisions?

¹ Office of the Legislative Auditor, Financial Audit Division, *Office of the State Auditor: Internal Controls and Compliance Audit* (St. Paul, 2021). In the prior audit, we found that OSA did not classify and approve overtime earned for certain employees, as required by state employment plans.

- Did the Office of the State Auditor comply with applicable state and internal policies?
- Did the Office of the State Auditor resolve a prior audit finding?²

To gain an understanding of OSA's internal controls and how it satisfies requirements, we interviewed its employees. We analyzed certain expenditures to determine compliance with state policy. We also tested all rent expenditures and analyzed office space utilization. Additionally, we tested samples of:

- Capital assets.
- Assets the office disposed of during the audit period.
- Equipment acquisitions.
- Professional/technical services contracts.
- Goods and services payments.
- Employee expense reimbursements.

Receipts

This part of the audit reviewed the fees the office collected for audit services, other receipts collected from various sources, and daily check deposits. We designed our work to address the following questions:

- Did the Office of the State Auditor have controls in place to ensure revenue activities complied with significant legal requirements?
- Did the Office of the State Auditor comply with significant legal requirements and internal policies related to revenue?

To gain an understanding of OSA's internal controls and how it satisfies compliance requirements related to receipts, we interviewed its employees. We tested fees and deposits to determine accuracy and compliance with state policy. We also reviewed the fees collected by the office to determine if it charged sufficient hourly rates to cover the costs of the audit services performed. Specifically, we tested:

- A sample of audit fee receipts.
- A sample of daily check deposits.
- All seminar fee receipts.

² Office of the Legislative Auditor, Financial Audit Division, *Office of the State Auditor: Internal Controls and Compliance Audit* (St. Paul, 2021). In the prior audit, we found that OSA did not adequately separate duties for an employee who had a majority of the assets assigned to them and also had administrative access to the capital asset system.

Information Technology Security Controls

This part of the audit reviewed whether OSA had implemented general information technology (IT) security controls to protect data used, retained, and stored by the office. We focused our control review on hardware and software related to the office's networks, remote access, directory services, and workstations (work computers, laptops, and desktops). We looked at controls within the following information security areas:

- Information security program and risk assessment
- Inventory and control of IT hardware and software assets
- Security awareness training
- Identity and access management
- Physical security
- Security logging and monitoring
- Network, data, and communication protections

We designed our work to address the following questions:

Did the Office of the State Auditor:

- Develop an information security program that aligns with industry best practices?
- Develop IT policies and standards that define security and development expectations?
- Complete any assessments to evaluate its security risks?
- Have processes to scan its IT hardware and software for vulnerabilities?
- Maintain an accurate and current inventory of its IT hardware and software?
- Perform security awareness training?
- Timely remove system access when employees left the office?
- Implement strong password requirements?
- Use multifactor authentication for network access, web-facing applications, and privileged accounts?

- Regularly review system permissions to validate that employee access remains appropriate?
- Implement adequate physical and environmental controls to protect its IT assets?
- Maintain an audit log of IT security events and monitor for incidents?
- Implement and manage network security devices (such as firewall, intrusion detection systems, etc.)?
- Encrypt sensitive data in transit and at rest?

To answer these questions, we reviewed OSA's security policies, interviewed its employees, observed system configurations, validated that the office implemented key technical controls, and tested the effectiveness of certain technical controls.

We conducted this performance audit in accordance with generally accepted government auditing standards.³ 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. 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.

We assessed internal controls against the most recent edition of the internal control standards, published by the U.S. Government Accountability Office.⁴ To identify compliance criteria for our audit, we examined state and federal laws, state administrative rules, state contracts, and policies and procedures established by Minnesota Management and Budget and the Department of Administration, as well as internal policies and procedures established by the Office of the State Auditor. For assessing information technology security controls, we also utilized industry best practices prescribed by the National Institute of Standards and Technology, and the Center for Internet Security.⁵

³ Comptroller General of the United States, Government Accountability Office, *Government Auditing Standards, 2018 Revision* (Washington, DC, Technical Update April 2021).

⁴ Comptroller General of the United States, Government Accountability Office, *Standards for Internal Control in the Federal Government* (Washington, DC, September 2014). In September 2014, the State of Minnesota adopted these standards as its internal control framework for the executive branch.

⁵ U.S. National Institute of Standards and Technology (NIST), Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020; and Center for Internet Security (CIS), *CIS Critical Security Controls*, Version 8.1 (August 2024).

Payroll Expenditures

As of December 2023, the Office of the State Auditor (OSA) employed 80 staff. During the scope of the audit, the office had \$21,081,264 in payroll expenditures. Exhibit 2 shows the payroll expenditures by type.

Exhibit 2

Payroll Expenditures, July 1, 2021, through December 31, 2023

Payroll Expenditures	Gross Pay	Employer Expenses ^a	Total
Hours Worked and Leave Taken	\$14,690,222	\$5,071,159	\$19,761,381
Overtime Pay	474,169	65,175	539,344
Separation Pay	293,358	103	293,461
Retroactive Pay Rate Adjustments	183,716	52,576	236,292
Leave Conversions to Deferred Compensation	31,978	8,703	40,681
Compensatory Time Payoffs	23,169	3,579	26,748
Other ^b	2,000	181,357	183,357
Total	\$15,698,612	\$5,382,652	\$21,081,264

^a “Employer Expenses” includes OSA’s shares of FICA, insurance, and retirement contributions.

^b “Other” includes payments for unemployment insurance, workers’ compensation, and miscellaneous payroll costs. We did not audit these other payroll expenditures.

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

Employee Pay Rates

OSA employees fall under one of five different employment agreements: the Office of the State Auditor Plan; the American Federation of State, County, and Municipal Employees (AFSCME) Agreement; the Commissioner’s Plan; the Minnesota Association of Professional Employees (MAPE) Agreement; and the Middle Management Association (MMA) Agreement.

OSA’s plan and the state employment agreements establish the salary ranges for OSA employees. Under Minnesota rules, state agencies—including OSA—have the authority to set the starting salaries for new employees within a position’s salary range, up to certain limits.⁶ To exceed those limits, agencies must obtain approval from Minnesota Management and Budget (MMB). During the scope of the audit, OSA hired or rehired 29 employees, including 28 with starting salaries that required MMB’s approval. We reviewed the approval for the starting salaries for eight of these employees and found no significant issues.

The Minnesota Constitution states that the salaries of executive officers, including the Governor, Lieutenant Governor, Attorney General, Secretary of State, and State Auditor

⁶ Minnesota Rules, 3900.2100, <https://www.revisor.mn.gov/rules/3900.2100/>, accessed January 2024.

“shall be prescribed by law.”⁷ The last salary increase authorized by the Compensation Council for these officers occurred on July 1, 2023.⁸ We confirmed that OSA paid the correct salary to the State Auditor.

Pay Rate Increases

Employees receive periodic pay rate increases based on provisions in the applicable employment agreements. Under the OSA plan, employees may receive a performance-based salary increase each year if they are not at the top of the salary range assigned to their position.⁹ Under the Commissioner’s plan, employees may receive both a general salary increase and a performance-based salary increase each year.¹⁰ To receive either type of increase, the appointing authority must certify that the employee’s job performance was satisfactory.

Under the employment agreements with AFSCME, MAPE, and MMA, eligible employees receive annual general salary increases, and semiannual or annual step progression salary increases.¹¹ In odd years, employees are eligible for the general salary increases if they are not at the top of the salary range assigned to their position; in even years, all employees are eligible. Employees are eligible for the step progression increases if they are not at the top of the salary range assigned to their position; the appointing authority can withhold increases because of unsatisfactory job performance.

During the scope of the audit, 15 employees covered by the OSA plan received a total of 29 pay rate increases. We reviewed the certifications of satisfactory job performance and compared the pay rate increases to the maximum increases allowed in the plan for all pay rate increases. We found no issues.

Similarly, during the scope of the audit, 67 employees covered by the AFSCME, MAPE, or MMA employment agreements received a total of 220 pay rate increases; 67 received a total of 168 general salary increases, and 33 of the 67 received a total of 52 step progression salary increases. We confirmed that each employee received no

⁷ *Minnesota Constitution*, art. V, sec. 4.

⁸ *Minnesota Statutes* 2024, 15A.082. During the scope of the audit, the State Auditor’s salary was \$108,485 (fiscal years 2022 and 2023) and \$118,249 (Fiscal Year 2024).

⁹ Office of the State Auditor (OSA), *Office of the State Auditor Plan, July 1, 2019 – June 30, 2021*; and *Office of the State Auditor Plan, July 1, 2021 – June 30, 2023*. The plans allowed for one performance-based salary increase each year, up to 6 percent.

¹⁰ Minnesota Management and Budget, *Commissioner’s Plan, July 1, 2021 through June 30, 2023*, and *July 1, 2023 through June 30, 2025*, Chapter 14.

¹¹ American Federation of State, County, and Municipal Employees (AFSCME), *Agreement between Minnesota State Employees Union AFSCME, Council No. 5, AFL-CIO and the State of Minnesota, July 1, 2021, through June 30, 2023*, and *July 1, 2023, through June 30, 2025*, art. 18, secs. 3-5; Minnesota Association of Professional Employees (MAPE), *Unit 14: General Professional Labor Agreement Between the State of Minnesota and the Minnesota Association of Professional Employees, July 1, 2021 – June 30, 2023*, and *July 1, 2023 – June 30, 2025*, art. 24, secs. 3-5; and Middle Management Association (MMA), *Agreement between the State of Minnesota and the Middle Management Association, July 1, 2021, through June 30, 2023*, and *July 1, 2023, through June 30, 2025*, art. 16, secs. 3-5. The agreements provided general salary increases of 2.5 percent effective July 1, 2021, and July 1, 2022, and 5.5 percent effective July 1, 2023.

more than three general salary increases during the scope of the audit, and we tested the accuracy of all step progression salary increases. We found no issues.

OSA records pay rate increases in the state's payroll system with an effective date. If that effective date is within the current or a future pay period, the payroll system will calculate pay at the new rate starting on the effective date. If that effective date is in a prior pay period, the state pays the employee a retroactive pay rate adjustment. During the scope of the audit, the office paid 145 retroactive pay rate adjustments totaling \$183,716 to 79 employees. We tested the accuracy of a random sample of 24 retroactive pay rate adjustments and found no issues.

Payroll Processing

State employees are paid biweekly. OSA follows state policy, which requires both employees and their supervisors to approve timesheets.¹² Employees enter their hours worked in the office's billing system. Once approved, payroll staff manually enter these employees' time in the state's payroll system. During the scope of the audit, office employees completed 4,809 biweekly timesheets. We tested a random sample of 40 timesheets and found no issues.

Holiday Pay

Employee agreements provided employees with 11 annual paid holidays in fiscal years 2022 and 2023, 5 paid holidays in the partial Fiscal Year 2024 of our audit period, and 1 floating holiday each fiscal year.¹³ During the scope of the audit, the office paid employees \$612,870 for 15,454 holiday hours, and \$58,441 for 1,506 floating holiday hours. We tested all holiday and floating holiday pay and found no significant issues.

Overtime Pay

The employment agreements for most OSA employees include provisions that allow them to earn overtime. Overtime can be compensated in the form of cash added to employee paychecks or compensatory time that the employee can use as paid time off in future pay periods. Under the OSA plan, and the MAPE and MMA agreements, exempt employees earn overtime at straight-time and nonexempt employees earn overtime at time and one-half.¹⁴

¹² Minnesota Management and Budget, Statewide Operating Policy and Procedure PAY0017, *Self Service Time Entry*, issued February 2011.

¹³ OSA plans, 2019-2021 and 2021-2023; AFSCME agreements, 2021-2023 and 2023-2025, art. 7, sec. 2; MAPE agreements, 2021-2023 and 2023-2025, art. 11, sec. 2; MMA agreements, 2021-2023 and 2023-2025, art. 9, sec. 2; and Minnesota Management and Budget, *Commissioner's Plan*, 2021-2023 and 2023-2025, Chapter 3, and *Managerial Plan*, July 1, 2021 through June 30, 2023, and July 1, 2023 through June 30, 2025, Chapter 3.

¹⁴ Straight-time means an employee's regular hourly pay rate. Time and one-half means an employee's regular hourly pay rate times 1.5.

Exempt employees are generally not entitled to overtime pay under the Fair Labor Standards Act. However, the OSA plan, and the MAPE and MMA agreements provide for overtime to exempt employees when assigned to a special project or a special work assignment, in addition to their normal job duties, with advance supervisor approval.¹⁵ Under the AFSCME agreement, employees earn overtime at time and one-half.¹⁶ The office follows state policy, which requires approval in advance for all overtime compensation.¹⁷

During the scope of the audit, the office paid \$474,169 of overtime in cash and \$46,761 of overtime as compensatory time to 51 employees in 1,094 timesheets. We tested a random sample of 60 timesheets and 4 additional timesheets selected based on our analysis for approval, eligibility, and accuracy of the pay rate. We found no significant issues. In addition, we determined that the office resolved the prior audit finding related to overtime.¹⁸

Leave Balance Adjustments

Employees' leave balance calculations are mostly automated in the state's payroll system, but some users have the ability to manually adjust those balances.¹⁹ During the scope of the audit, OSA processed nine leave balance adjustments for six employees.

Employees earn between four and nine hours of vacation leave each biweekly pay period, based on length of service.²⁰ Employees may accumulate a vacation leave balance to any amount, provided it is reduced to a cap of 260 or 275 hours at least once each fiscal year.²¹ If the vacation leave balance is not reduced to the cap at some point

¹⁵ OSA plans, 2019-2021 and 2021-2023, Chapter 3; MAPE agreements, 2021-2023 and 2023-2025, art. 27, sec. 3(C); and MMA agreements, 2021-2023 and 2023-2025, art. 11, sec. 2(B).

¹⁶ AFSCME agreements, 2021-2023 and 2023-2025, art. 18, sec. 2.

¹⁷ Minnesota Management and Budget, Statewide Operating Policy and Procedure PAY0012, *Requesting and Reporting Overtime*, issued September 2009.

¹⁸ Office of the Legislative Auditor, Financial Audit Division, *Office of the State Auditor: Internal Controls and Compliance Audit* (St. Paul, 2021). In the prior audit, we found that OSA did not classify and approve overtime earned for MMA employees as a special project. The MMA agreement for 2023-2025 updated its language for exempt employees, allowing employees to receive overtime "when specifically assigned or directed to work additional hours within the pay period."

¹⁹ Minnesota Management and Budget, Statewide Operating Policy and Procedure PAY0026, *Leave Balance Adjustments*, issued December 2007. In certain situations, an agency may need to manually adjust or establish an employee's paid leave balance. This function is typically performed by payroll or human resource employees.

²⁰ OSA plans, 2019-2021 and 2021-2023, Chapter 5; AFSCME agreements, 2021-2023 and 2023-2025, art. 8, sec. 2(A); MAPE agreements, 2021-2023 and 2023-2025, art. 10, sec. 2; MMA agreements, 2021-2023 and 2023-2025, art. 8, sec. 1(C); and Minnesota Management and Budget, *Commissioner's Plan*, 2021-2023 and 2023-2025, Chapter 4, and *Managerial Plan*, 2021-2023 and 2023-2025, Chapter 4.

²¹ OSA plans, 2019-2021 and 2021-2023, Chapters 4 and 5; AFSCME agreements, 2021-2023 and 2023-2025, art. 8, sec. 2(F); MAPE agreements, 2021-2023 and 2023-2025, art. 10, sec. 2; MMA agreements, 2021-2023 and 2023-2025, art. 8, sec. 1(E); and Minnesota Management and Budget, *Commissioner's Plan*, 2021-2023 and 2023-2025, Chapter 4, and *Managerial Plan*, 2021-2023 and 2023-2025, Chapter 4. The OSA plans allow for an accrual cap of 260 hours for nonmanagerial employees and 275 hours for managers. AFSCME, MAPE, and MMA agreements allow an accrual cap of 275 hours.

during the fiscal year, the balance is automatically reduced to the cap by the state's payroll system at the end of the fiscal year. Minnesota Management and Budget may temporarily suspend the automatic reduction to the cap in emergency situations.²²

We tested all nine leave balance adjustments during our audit scope and found no issues.

Other Paid Leave

State Policy, as well as OSA's plan, the Commissioner's Plan, and the AFSCME, MAPE, and MMA agreements provide for up to 480 hours for family medical leave and up to 240 hours of paid parental leave.²³

During the scope of the audit, the office paid 15 employees \$231,156 for family medical leave and paid parental leave.²⁴ We reviewed all of these payments to determine if any employees exceeded the limits for family medical leave and paid parental leave. We found no issues.

Separation Pay

Upon separation from state service, employees may be eligible to receive various types of separation payments. All employees receive payments for unused vacation leave and compensatory time, up to limits established in the applicable employment agreements. Employees that meet certain eligibility requirements related to age and years of service also receive severance payments for a percentage of unused sick leave.

During the scope of the audit, OSA made \$293,357 in separation payments to 17 former employees. We tested the accuracy of and eligibility for a random sample of seven employees and one judgmentally selected employee with separation payments and found no issues.

²² Minnesota Management and Budget, *Commissioner's Plan*, 2021-2023 and 2023-2025, Chapter 4, and *Managerial Plan*, 2021-2023 and 2023-2025, Chapter 4. Temporary suspension does not apply to other employment agreements.

²³ Minnesota Management and Budget, Human Resources/Labor Relations Policy 1409, *Family and Medical Leave Act (FMLA)*, issued December 1, 2014, revised December 16, 2015, and Human Resources/Labor Relations Policy 1435, *Paid Parental Leave*, issued November 16, 2016, revised January 28, 2020; OSA plans, 2019-2021 and 2021-2023, Chapter 7; AFSCME agreements, 2021-2023 and 2023-2025, Appendix M; MAPE agreements, 2021-2023 and 2023-2025, Appendix K; MMA agreements, 2021-2023, Appendix I, and 2023-2025, Appendix H; and Minnesota Management and Budget, *Commissioner's Plan*, 2021-2023 and 2023-2025, Chapter 6, and *Managerial Plan*, 2021-2023 and 2023-2025, Chapter 6.

²⁴ Minnesota Management and Budget, Human Resources/Labor Relations Policy 1409, *Family and Medical Leave Act (FMLA)*, issued December 1, 2014, revised December 16, 2015. An employee may take FMLA-qualifying leave continuously, intermittently, or on a reduced leave schedule. Employees are required to exhaust their accrued sick leave hours for conditions that qualify for sick leave usage under the applicable labor agreements or plans. After exhausting accrued sick leave hours, the employee may choose, and the agency must grant, the use of accrued vacation or compensatory time while taking FMLA leave. All paid time counts toward the 12 weeks of FMLA-qualifying leave. Employees who do not meet the requirements for taking paid leave remain entitled to take unpaid FMLA leave.



OLA

Nonpayroll Expenditures

During the scope of the audit, the Office of the State Auditor (OSA) had \$3,332,550 in nonpayroll expenditures. Exhibit 3 shows the nonpayroll expenditures by type.

Exhibit 3

Nonpayroll Expenditures, July 1, 2021, through December 31, 2023

Nonpayroll Expenditures	Amount
Other Goods and Services	\$1,419,706
Space Rentals	1,309,790
Equipment	336,511
Professional/Technical Services Contracts	236,743
Employee Expense Reimbursements	53,449
Expenditure Reductions ^a	(24,933)
Total	\$3,331,266

^a Employee-paid parking fees totaling \$24,161 are included in this total. OSA collects parking fees from employees through the state's payroll system, which reduces the rent expense incurred by the office for leasing parking spaces. The remaining \$772 consists of vendor refunds and expense reimbursement refunds issued to the office. We analyzed these expenditures to verify that vendors, invoice descriptions, and amounts appeared reasonable, but we did not test them.

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

Equipment and Other Goods and Services

During the scope of the audit, OSA made 1,089 payments totaling \$1,756,217 for various types of other goods and services and equipment. These included purchases on state contracts, such as office supplies and computer equipment, and other purchases made through purchasing orders, such as employee training. We tested a random sample of 66 payments as well as 32 additional payments we identified in our analysis and found no significant issues.

Space Rentals

During the scope of the audit, OSA paid \$1,309,790 for office or parking space rent. Of this amount, the office paid \$1,239,647 for building leases in six cities: Duluth, Mankato, Marshall, Moorhead, Rochester, and St. Paul. The office paid the remaining \$70,143 for a parking lease at the St. Paul location. We tested all of the expenditures for rent and analyzed all of the expenditures for parking spaces, and found no issues.

Asset Management

OSA maintains assets, including capital assets and sensitive items, needed for its operations. State policy defines a capital asset as an item with “a normal useful life expectancy exceeding two years...[that] maintains its identity while in use.”²⁵ Sensitive items are items “that could be easily sold and are most often subject to pilferage or misuse.”²⁶ State policy requires a complete physical inventory of capital assets and sensitive items to be conducted at least biennially.²⁷ In addition to the state policy, the office has a policy that requires an annual inventory of capital assets.²⁸ The office uses a capital asset system to track its assets.

OSA’s policy also requires an asset number be assigned and tracked in the capital asset system for:

- Items with a purchase price over \$1,000.
- Items that contain data storage of not-public data.
- Items that the office’s staff determine to be susceptible to theft.

Finally, OSA’s policy requires the finance director or deputy auditor to approve any disposal of assets.²⁹

Acquisitions

During the audit period, OSA made 70 acquisitions totaling \$336,511 for various assets. We tested a sample of 13 purchases and subsequently expanded testing for the remaining samples based on errors we found in our initial sample.³⁰

²⁵ Minnesota Department of Administration, *Property Management Reporting and Accountability Policy*, issued May 1, 2014.

²⁶ *Ibid.* Sensitive items include items such as firearms and other weapons; computers, including network servers, portable printers, scanners, projectors, cellular phones, software with an acquisition cost over \$5,000 and less than \$30,000; and cameras, televisions, and other video equipment with an acquisition cost over \$500 and less than \$5,000.

²⁷ Minnesota Department of Administration, *Property Management Reporting and Accountability Policy*, issued May 1, 2024.

²⁸ Minnesota Office of the State Auditor, Accounting Policies and Procedures, *Capital Assets*, issued July 15, 2010. OSA’s capital assets include items that contain not public information or items that are potentially susceptible to theft.

²⁹ *Ibid.*

³⁰ We did not test 1 of 70 purchases because it was already included in the capital asset system.

FINDING 1

The Office of the State Auditor did not assign asset numbers to all of its capital asset acquisitions, nor did it record those assets in its capital asset system, as required by its policy.

OSA did not assign six acquisitions an asset number in accordance with its policy.³¹ The six items consisted of three desks, a mail sorter, a secure area network, and an audio-conferencing device.

The office agreed that these items needed an asset number assigned to them and indicated it has not conducted recent trainings on the inventory policy to ensure that staff are aware of the policy requirements. Additionally, the office did not always identify acquisitions that required an asset number when it approved the acquisition documentation for payment. Assets that are not properly numbered or recorded in the capital asset system are more susceptible to loss or theft.

RECOMMENDATIONS

- **The Office of the State Auditor should assign asset numbers to all capital asset acquisitions and record those assets in its capital asset system.**
- **The Office of the State Auditor should strengthen internal controls over assets to ensure it assigns asset numbers to all of its capital asset acquisitions and records all capital assets in its capital asset system.**

Inventory

Through December 2023, OSA had 912 assets recorded in its capital asset system totaling over \$1.38 million. The office recorded assets that included, but were not limited to, office furniture, computers, phones, and other information technology (IT) equipment.

FINDING 2

The Office of the State Auditor did not manage its asset inventory in compliance with state or office policies.

OSA did not conduct any physical inventories of its assets during the scope of the audit. The most recent physical inventory the office performed, which was only partially completed, occurred in February 2020. Employees told us they had difficulties completing an inventory partly due to the COVID-19 pandemic and moving employees from working in the office to telecommuting full time. As of June 2024, the office indicated it was starting a physical inventory.

³¹ Minnesota Office of the State Auditor, Accounting Policies and Procedures, *Capital Assets*, issued July 15, 2010.

Since OSA had not conducted a complete physical inventory during the audit period, we performed additional procedures to determine the accuracy of the office's inventory. We tested a random sample of 40 items on OSA's inventory and identified 5 items that the office did not accurately maintain in its capital asset system:

- For three of the five items, the office failed to update the capital asset system to indicate that it had disposed of the items. Employees said they erroneously omitted these items on disposal forms and supervisors failed to recognize these items were not on the disposal forms when approving the disposals. As a result, the capital asset system was not updated to reflect the accurate status of these items.
- For two of the five items, the office did not update records to indicate that it changed the asset tracking number. Employees explained that the office originally scheduled these assets for disposal, but it subsequently reassigned and repurposed the assets for a new use.³² Consequently, both the old and new assigned inventory numbers remained in the capital asset system for these items, implying that the office had twice as many of these items than it actually owned.

As a result of OSA not completing its physical inventory during the audit period, the office did not identify or correct these errors. Inaccurate asset inventory records increase the risk of assets being misappropriated without detection. Conducting periodic physical inventories of assets, documenting the results of those inventories, and updating asset inventory records based on those results is necessary to ensure the accuracy of asset inventory records.

Despite the office not conducting physical inventories during the audit period, we determined that the office had resolved the prior audit finding related to the separation of duties for maintaining assets in its capital asset system.³³

RECOMMENDATIONS

- **The Office of the State Auditor should conduct and document a full physical inventory of assets annually, to comply with both state and office policies.**
- **The Office of the State Auditor should update its capital asset system to reflect the results of its annual inventories and investigate discrepancies between its physical inventory and capital asset system.**

Disposals

During our audit period, OSA disposed of 177 capital assets it no longer needed. The majority of the items disposed of were computers and other IT equipment. We tested a random sample of 29 disposals and found no issues.

³² OSA had already physically removed the original assigned asset numbers from the assets in preparation for disposal. Therefore, the office needed to assign new asset numbers once it determined to repurpose the assets.

³³ Office of the Legislative Auditor, Financial Audit Division, *Office of the State Auditor: Internal Controls and Compliance Audit* (St. Paul, 2021). In the prior audit, we found that OSA did not adequately separate duties for the individual who had a majority of the assets assigned to them and also had administrative access to the capital asset system.

Professional/Technical Services Contracts

During the scope of the audit, OSA paid \$236,743 on 37 professional/technical services contracts. The majority of the contracts were for services related to IT systems or training. We tested a random sample of seven contracts and an additional contract based on our analysis, and we found no issues.

Employee Expense Reimbursements

OSA reimburses expenses incurred by employees for legitimate state business. During the scope of the audit, the office paid 350 employee expense reimbursements, totaling \$53,449. We tested a random sample of 40 reimbursements and 5 additional reimbursements based on our analysis and found no significant issues.



OLA

Receipts

The Office of the State Auditor (OSA) collected \$13,117,187 in receipts over the course of the audit period. Audit fees were the largest category at \$12,992,941, comprising 99 percent of total receipts. Exhibit 4 shows receipts by type.

Exhibit 4
Receipts, July 1, 2021, through December 31, 2023

Receipts	Total
Audit Fees	\$12,992,941
Seminar Fees	100,082
Other Receipts ^a	24,164
Total	\$13,117,187

^a "Other Receipts" consists of \$24,000 in accounting software fees, \$119 in interest on delinquent accounts, and \$45 in refunds. We did not test these receipts, as they were less than 1 percent of total receipts.

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

Audit Fees

OSA performs financial and compliance audits of local governments, including counties, towns, schools, and other political subdivisions, and bills those clients for its audit services. Every year, the office evaluates, and adjusts if needed, the hourly rates it charges clients for services performed by its auditors, legal counsel, and investigators.³⁴ During the scope of the audit, the office collected \$12,992,941 from 349 clients for audit services provided. We reviewed the office's procedures for analyzing its hourly rates and verified that the office evaluated its rates each year. We also tested 40 random samples and 1 judgmental sample based on our analysis of 1,002 billings and found no significant issues.

Deposits

During the scope of the audit, OSA collected \$6,388,020 in receipts received by check through the mail. This total included \$6,387,178 in audit fees or other receipts, and \$842 in refunds. We randomly sampled 40 of the 257 check deposits in our audit period. We checked the accuracy of the recorded deposits and verified that the office deposited all check receipts in the bank. We found no significant issues.

³⁴ During calendar year 2023, OSA invoiced clients based on ten different OSA job positions; hourly rates ranged from \$42 to \$124.

Seminar Workshop Fees

OSA provides annual continuing professional education (CPE) training for its Audit Practice Division staff, as well as for local government accounting professionals. The office collects registration fees from nonemployees for its CPE training. In addition, the office tracks registration costs for its employees related to internal training it conducts to cover payments related to the CPE training.³⁵ We tested the fees for all seven seminars, totaling \$100,082, and found no issues.

³⁵ Minnesota Statutes 2024, 16A.721.

Information Technology Security Controls

Information technology (IT) security controls are an important aspect of safeguarding the security, accuracy, and reliability of information systems and data. By establishing robust IT controls, organizations strengthen their overall IT governance and protect critical assets.

The Office of the State Auditor (OSA) is a constitutional office and is therefore outside of the scope of the state's centralized information technology department—Minnesota Information Technology Services (MNIT).³⁶ Because of this, the office has its own Chief Information Officer and IT staff; OSA's use of MNIT's centralized IT services, such as data centers, network services, and consolidated e-mail, are optional.³⁷ The office must also develop and implement its own technical and information security programs, including policies, standards, and procedures.³⁸

Our audit looked at controls within the following information security areas:

- Information security program and risk management
- Inventory and control of IT hardware and software assets
- Security awareness training
- Identity and access management
- Physical security
- Security logging and monitoring
- Network, data, and communication protections

Overall, we found IT security controls that are typical for a small or medium-sized organization that has limited resources to dedicate towards protecting IT assets. As a result, certain IT controls are not as robust as those found in larger enterprises with dedicated IT security resources. Our conclusions for each security area reviewed—and any findings and recommendations for improvement—are discussed below.

³⁶ Minnesota Information Technology Services, *Information Security and Risk Management Applicability Standard*, Version 1.11, revised October 1, 2023.

³⁷ OSA procures some network and telephone services from Minnesota Information Technology Services.

³⁸ U.S. National Institute of Standards and Technology (NIST), Special Publication 800-12, Rev. 1, *An Introduction to Information Security*, June 2017, Chapter 5, addresses best practices for development and implementation of policies, standards, procedures, and guidelines.

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:

- Policies, standards, and procedures.
- Information security resources.
- A classification of information assets.
- A risk assessment process.

Best practices recommend that organizations develop an information security program that describes the required security controls, roles and responsibilities, and risks addressed by the program.³⁹ Best practices also recommend that organizations such as OSA establish policies and procedures designed to ensure the protection of information and systems.⁴⁰ Finally, best practices recommend that organizations conduct periodic assessments to determine the sufficiency of their security program and perform monitoring to identify and address any vulnerabilities found.⁴¹

FINDING 3

The Office of the State Auditor has not implemented an information security program that aligns with best practices.

Although OSA had basic security policies and procedures in place that were directed toward staff, the office lacked more specific policies, standards, and procedures directed toward its information technology operations. For example, policies and procedures prohibit OSA employees from storing OSA data on any personal devices. These policies and procedures also discuss appropriate use of IT assets, and require employees to physically secure laptop computers. However, the office did not have policies, standards, or procedures to define requirements related to (1) appropriate risk and vulnerability management; (2) system patch management; (3) security awareness training; (4) password complexity; or (5) security logging and monitoring.

When properly written, security policies, standards, and procedures should articulate management's operational and security expectations. For example, these documents might include expectations for passwords, encryption levels, system testing, and system maintenance. Absent such direction in the policies and procedures, OSA IT staff and its contractors often have been left to determine for themselves what is required.

³⁹ U.S. National Institute of Standards and Technology (NIST), Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, sec. 3.13, 203-221.

⁴⁰ *Ibid.*, Chapter 3, 16-373. The first control within each NIST family outlines the need for policies and procedures.

⁴¹ *Ibid.*, sec 3.16, 238-245.

Further, OSA has not completed any comprehensive security controls assessments to test the effectiveness of its current controls. Security control assessments (such as penetration tests and secure configuration scans) improve cybersecurity by evaluating the current level of controls. If control gaps are identified—whether by office staff, information security professionals, or internal or external auditors—OSA management can decide to either accept the risk resulting from the deficiency, or develop remediation plans to mitigate the control gaps.

While not as rigorous as detailed security control assessments, OSA told us it has performed undocumented risk assessments on a limited basis to support various IT projects. Risk assessments identify threats and vulnerabilities to the IT system that could occur; they also determine the likely impact on an organization's operations, assets, internal staff, external partners, the public, and other organizations. While risk assessments consider what could go wrong, security control assessments look to identify gaps in controls that allow for a greater probability of a risk becoming reality.

Finally, OSA has not conducted necessary vulnerability monitoring. The office's vulnerability management practices only include patch-management processes. While patch management may remediate some security vulnerabilities, it does not replace vulnerability monitoring; which assesses whether the security patches adequately protect against known vulnerabilities.

For security purposes, OSA must also pay attention to the “support status” of its existing hardware and software. Vendors may stop publishing security patches for unsupported systems and software, thus leaving those systems vulnerable to known security flaws. During our audit, we observed that OSA was using certain hardware and software that vendors no longer supported, thus putting its systems at risk. Scanning the environment with a vulnerability management tool would help the office to identify security flaws and risks to address, such as missing patches or unsupported products.

When we discussed these concerns with OSA staff, they indicated that, as a smaller office, they do not have the resources needed to develop and implement robust security assessments and monitoring. However, even small organizations with limited IT and cybersecurity expertise can take steps toward protecting their IT systems.

RECOMMENDATION

The Office of the State Auditor should implement an information security program that aligns with best practices. As part of its implementation, the office should:

- **Establish expectations and requirements for its information technology operations and security within office policies, standards, and procedures.**
- **Conduct security control assessments of its information assets.**
- **Develop and implement a plan to regularly track information technology vulnerabilities.**

Inventory and Control of IT Hardware and Software Assets

Asset management is the process of procuring, tracking, maintaining, and disposing of an asset owned by an organization. Managing IT assets, in particular, is an important part of IT security. In fact, best practices describe the first and most important step in an effective security program as “know your environment.”⁴² Hence, best practices recommend that organizations establish and maintain an accurate, detailed, and up-to-date inventory of all hardware and software that has the potential to store or process data.⁴³ Having a current inventory allows an organization to monitor and protect its IT assets while preventing unauthorized assets—such as an unauthorized computer connected to the network, or unapproved software—from entering the environment.

While general asset tracking historically focuses on the asset’s existence, valuation, and location, maintaining an inventory of IT assets goes beyond a register of physical devices. IT asset inventory should include assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Best practices prescribe that an organization should include the following information as part of its IT asset inventory:

- IP and MAC addresses for network components, servers, and virtual infrastructure⁴⁴
- Operating system version
- Software version
- Installation date
- Last patched date
- Current vendor support status
- Classification of data transmitted, stored, or processed by the asset
- Interrelationships with other IT assets⁴⁵

⁴² Center for Internet Security, *A Guide to Defining Reasonable Cybersecurity*, May 2024, sec. 5, 12.

⁴³ *Ibid.*, Appendix H, Controls 1.1 and 2.1, 39-40.

⁴⁴ An IP address (Internet Protocol address) is a numerical label assigned to a device connected to a computer network. A MAC address (media access control address) is a 12-digit hexadecimal number assigned to each device connected to the network.

⁴⁵ Center for Internet Security, *A Guide to Defining Reasonable Cybersecurity*, May 2024, Appendix H, Controls 1.1 and 2.1, 39-40; U.S. National Institute of Standards and Technology (NIST), Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, sec. 3.5, 107-110; and COBIT 2019 Framework: Governance and Management Objectives (Schaumberg, IL: ISACA, 2018), BAI10.01, 215.

We examined the extent to which OSA IT inventory records included best practices recommended information and were complete. We identified 375 technology-related IT assets and 55 active software products.⁴⁶

FINDING 4

The Office of the State Auditor's inventory of information technology hardware and software did not contain important maintenance and security-related information.

Although OSA maintains capital asset information for its hardware, the records did not contain sufficient information to meet IT maintenance and security program recommendations.⁴⁷ For example, OSA's IT inventory records did not include IP or MAC addresses, base operating systems, interrelationships with other IT assets, or the support status of the products.

By not maintaining a comprehensive record of all IT assets and their relationships, OSA may find it more difficult to (1) manage and access relevant information, (2) provide detailed insights into its IT infrastructure, and (3) assess the impact of proposed changes on its IT environment. Maintaining detailed information about IT hardware and software assets can also help the office in mitigating risks associated with outdated, unsupported products. Finally, without a complete inventory of authorized IT assets, the office may find it more difficult to detect unauthorized hardware and software that may come into its environment.

In response to our questions, OSA acknowledged that its IT asset inventory did not include all relevant information. OSA noted, however, that risks are somewhat mitigated, as it is a smaller organization, without a vast number of IT assets, and with long-time IT staff who have a good understanding of the office's IT environment.

RECOMMENDATION

The Office of the State Auditor should maintain an inventory of information technology assets that includes information prescribed by best practices.

Best practices also recommend that organizations replace system components when support for the components is no longer available from the developer, manufacturer, or vendor.⁴⁸

⁴⁶ Our audit focused on hardware and software related to networks, remote access, directory services, and workstations (e.g., work computers, laptops, and desktops).

⁴⁷ OSA's asset inventory records included an asset number; asset description, including make, model, and serial number; asset location; and asset acquisition data and cost.

⁴⁸ U.S. National Institute of Standards and Technology (NIST), Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, Control SA-22, sec. 3.17, 290.

FINDING 5

The Office of the State Auditor has hardware and software that is outdated and no longer supported by its vendors or manufacturers.

OSA has roughly 45 different servers, workstations, printers, and networking equipment that are more than 10 years old; 7 of these items are at least 20 years old. In most cases, the vendors or manufacturers are no longer supporting the outdated hardware and software. Unsupported hardware and software can result in increased maintenance costs, reduced operational efficiency, and heightened risk of system failures or security breaches.

OSA was aware of many of its aged hardware and software and told us that these assets generally met its business needs. The office told us it had plans to replace some—but not all—of its hardware and software.

RECOMMENDATION

The Office of the State Auditor should establish and implement a plan to replace its outdated hardware and software.

Security Awareness Training

Best practices recommend that organizations implement a security awareness training program with the goal of training all staff of potential threats and how to avoid situations that might put the organization's systems and data at risk.⁴⁹ These best practices recommend organizations conduct training when staff are first hired and, at a minimum, annually thereafter.⁵⁰ To gain an understanding of OSA's security awareness program, we reviewed current practices and reviewed employee security training records.

FINDING 6

The Office of the State Auditor did not conduct annual security awareness training for its employees.

As discussed previously, OSA did not have formal information security policies that required its employees to complete security awareness training. Despite no formal requirements, the office did enroll its approximately 80 staff in an online course on security awareness during Fiscal Year 2024. However, there were no records of security awareness training for fiscal years 2022 or 2023. While best practices recommend annual security awareness training, OSA employees had only completed training in one of the three years of our audit scope. OSA told us that while it did not require formal security awareness trainings, the office routinely reminded staff of good cybersecurity practices during staff meetings.

⁴⁹ Center for Internet Security, *A Guide to Defining Reasonable Cybersecurity*, May 2024, Appendix H, Control 14, 64.

⁵⁰ *Ibid.*, Appendix H, Control 14.1, 64.

RECOMMENDATIONS

- **The Office of the State Auditor should establish requirements for its information security awareness program.**
- **The Office of the State Auditor should provide security awareness training to its employees on an annual basis.**

Identity and Access Management

Identity and access management includes processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for IT assets and software.

OSA has a formal policy and defined procedure in place for removing access when an employee leaves the office. We tested all 20 individuals who had separated from the office between July 1, 2021, and March 14, 2024, and concluded that the office deactivated all associated user accounts for these individuals in a timely manner.

As discussed previously, OSA did not have a formal policy or standard that defined user account authentication requirements, such as password complexity, password length, or multifactor authentication (MFA).⁵¹ As a result, we compared the office's implemented authentication criteria to best practices.⁵² Best practices implementation includes, at a minimum, [REDACTED]

[REDACTED]

FINDING 7

The Office of the State Auditor did not always follow best practices when authenticating users that access its information technology assets and software.⁵⁵

OSA generally followed best practices for authenticating its general users. However, the office authenticated administrative accounts using the same criteria as a general user

⁵¹ Multifactor authentication requires two or more methods to authenticate a user prior to gaining access. To get access, a user needs (1) something they know (like a password), (2) something they have (like a phone, a special key, or an additional one-time password or PIN), and (3) something they are (like a fingerprint).

⁵² Center for Internet Security, *A Guide to Defining Reasonable Cybersecurity*, May 2024, Appendix H, Controls 5 and 6, 50-52.

[REDACTED]

[REDACTED]

⁵⁵ In accordance with *Minnesota Statutes* 2024, 13.37, subd. 2, we have removed from the public version of our report language from Finding 7 that we deemed likely to substantially jeopardize the security of OSA systems. We discussed the specific details with OSA.

and, in some instances, administrative passwords did not expire. Administrative passwords should be more restrictive and complex for several key reasons:

- **Higher Privileges.** Administrative accounts have elevated privileges that allow those users to make significant changes to systems, including installing software, accessing sensitive data, and managing user accounts. If these accounts are compromised, the potential damage is much greater.
- **Target for Attacks.** Administrators are prime targets for cyber attackers. Hackers often use sophisticated methods to decipher passwords. Complex passwords make it significantly harder for these attacks to succeed.
- **Unauthorized Access.** Stronger passwords help prevent unauthorized access to critical systems. This is crucial for maintaining the integrity and security of the entire network.

By enforcing more complex and restrictive passwords for administrative accounts, OSA can better protect its critical infrastructure and sensitive information from potential threats. OSA had configured a special security group to authenticate its administrative accounts; however, the office did not add individual administrative accounts to this special group.

In addition to concerns regarding administrative passwords, we found that OSA had not

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] The office could reduce its IT security risk by implementing tighter authentication requirements for its administrative accounts and [REDACTED]

OSA had performed some testing [REDACTED] to access some applications. However, the office told us that challenges [REDACTED] have stalled implementation. [REDACTED]

RECOMMENDATIONS

- **The Office of the State Auditor should require more complex passwords for accounts with broad access.**
- **The Office of the State Auditor should** [REDACTED]
[REDACTED]
[REDACTED]

As part of our audit, we also reviewed whether OSA regularly reviews user access permissions. Best practices suggest that access controls to IT assets and software be reviewed on a recurring schedule—at least annually—to validate that all privileges are authorized.⁵⁷ We found no significant issues.

⁵⁷ Center for Internet Security, *A Guide to Defining Reasonable Cybersecurity*, May 2024, Appendix H, Control 6.8, 52.

Physical Security

Best practices recommend that organizations implement physical security controls to protect organizational assets from known environmental threats—such as floods, fire, wind, and excessive heat and humidity—and potential threats from individuals or groups.⁵⁸

We reviewed existing physical access controls and inspected OSA’s main facility and data center. We found no significant issues.

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.

Best practices recommend that an organization collect, review, and retain logs of events and activities that occur in an IT system.⁵⁹ These best practices recommend logging on all systems to reconstruct computer events such as:

- Actions taken by accounts with administrative privileges.
- Access to all log data, including initializing, stopping, pausing, or deleting of the logs.
- Login attempts.
- System log-offs.
- Password changes.
- Changes to database or application records, where the application has been bypassed to produce the change.
- System and application alerts and error messages.
- System and application shutdowns and restarts.
- Security policy modifications.⁶⁰

⁵⁸ U.S. National Institute of Standards and Technology (NIST), Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, sec. 3.11, 179-193.

⁵⁹ *Ibid.*, sec. 3.3, 65-82; and Center for Internet Security, *A Guide to Defining Reasonable Cybersecurity*, May 2024, Appendix H, Control 8, 54-55.

⁶⁰ *Ibid.*

Best practices further recommend that organizations actively monitor logs and protect them from unauthorized access, use, modification, or deletion.⁶¹ Finally, because system logs are generated in multiple servers, databases, applications, and infrastructure devices, and because system logs can become very large, best practices recommend consolidating these logs into a centralized log management tool that can simplify analysis and better detect malicious activities.⁶²

FINDING 8

The Office of the State Auditor does not have a comprehensive security logging and monitoring program in place to detect and respond to security threats.

OSA has utilized local logging within specific applications and devices for troubleshooting; however, it does not have a comprehensive security log management process, nor does it have a monitoring program.

Without a security logging and monitoring program, OSA may find it more difficult to identify and respond to security threats. Additionally, the office may lack analysis capabilities to identify who did what if a serious event were to occur. Logs provide a detailed record of system activities, which is crucial for investigating security breaches and understanding how they occurred. Finally, consolidated logging could also assist the office with identifying operational issues and inefficiencies.

OSA staff we interviewed were not fully aware of all of the security requirements to manage and monitor logs as defined by best practices. However, implementing logging and monitoring strategies is essential for maintaining a secure and efficient IT environment.⁶³

RECOMMENDATION

The Office of the State Auditor should implement a comprehensive security logging and monitoring program.

⁶¹ U.S. National Institute of Standards and Technology (NIST), Special Publication 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, sec. 3.3, 65-82; and Center for Internet Security, *A Guide to Defining Reasonable Cybersecurity*, May 2024, Appendix H, Control 8, 54-55.

⁶² Center for Internet Security, *A Guide to Defining Reasonable Cybersecurity*, May 2024, Appendix H, Control 8.9, 55.

⁶³ We also benchmarked OSA's security log management program to best practices prescribed by the federal government for federal agencies; Office of Management and Budget, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, Memorandum M-21-31, August 27, 2021.

Network, Data, and Communication Protections

Network, data, and communication protections safeguard an organization's information technology assets and data from unauthorized access, use, disclosure, modification, and destruction. To prevent unauthorized access and potential threats, best practices recommend that organizations establish, implement, and actively manage network devices to safeguard incoming and outgoing traffic.⁶⁴ In particular, these best practices recommend organizations implement controls such as:

- Establishing and maintaining architecture diagram(s) and other network system documentation.
- Ensuring network infrastructure is kept up-to-date.
- Establishing and maintaining a secure network architecture.
- Deploying network intrusion detection and prevention solution.
- Collecting network logs to review and alert upon.

Best practices further recommend that organizations deploy and maintain antimalware software on all IT assets and encrypt sensitive data in transit and while at rest—most importantly, data stored on end-user devices and removable media.⁶⁵

To manage its network, OSA relies heavily upon a vendor to help support its network components on an as-needed basis. We reviewed the network architecture and processes used by the office and its vendor to maintain and monitor its network and data flow.

FINDING 9

The Office of the State Auditor does not follow best practices to detect, respond to, and prevent potential threats to its network.

While OSA had some basic network defense strategies in place to help protect against security threats—such as using antimalware and encryption strategies, implementing firewalls, and segmenting its networks—we found its processes to be limited.

Managing and monitoring the network for ongoing threats has not been part of OSA's routine processes. The office has not maintained architecture diagram(s) and other network documentation. Further, the office has used ad hoc processes, rather than routine scheduled procedures, to help ensure its network infrastructure was protected and kept up-to-date. In particular, some network devices had not been patched in nearly five years. Finally, we found minimal operating processes to conduct comprehensive network monitoring and defend against certain security threats. For example, while OSA's network firewall had built-in network intrusion detection and prevention

⁶⁴ Center for Internet Security, *A Guide to Defining Reasonable Cybersecurity*, May 2024, Appendix H, Controls 12 and 13, 59-63.

⁶⁵ *Ibid.*, Appendix H, Controls 3.6, 3.9, 3.10, and 10.1, 44-45 and 57.

functionality, the office was not actively using these features. Additionally, because of infrequent updates to the firewall's intrusion rules, some new attack methods may have gone unnoticed. Ad hoc network management processes such as these increase the office's risk of network mismanagement and increase the risk of bad actors exploiting vulnerable network services and access points.

Due to its size and lack of an overall best practices security program, OSA has not yet implemented these recommended network management practices. Additionally, we observed some confusion on network maintenance responsibilities that may also have contributed to some hardware not regularly being updated.

RECOMMENDATIONS

- **The Office of the State Auditor should maintain and update network documentation annually, or when significant changes occur.**
- **The Office of the State Auditor should ensure its network infrastructure is kept up-to-date.**
- **The Office of the State Auditor should implement necessary network intrusion detection and prevention capabilities.**

STATE OF MINNESOTA



Julie Blaha
State Auditor

Suite 500
525 Park Street
Saint Paul, MN 55103

January 27, 2025

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

Dear Legislative Auditor Randall:

Thank you for the opportunity to respond to the findings included in the report on the internal control and compliance audit of the Office of the State Auditor (OSA) for the period from July 1, 2021, through December 31, 2023. The OSA appreciates the thoroughness of the Office of the Legislative Auditor's review and its recommendations.

Most of the findings in the report relate to information technology policies and practices. The OSA recognizes the importance of strong information technology controls. As part of the 2024-2025 budget, the OSA received funding for a Chief Information Officer position dedicated to overseeing the OSA's technology functions. The OSA filled the Chief Information Officer position in April 2024, and the Chief Information Officer has already started to implement many of the recommendations included in the report.

Under the Chief Information Officer's leadership, the OSA has already started the process of updating its hardware, software, and network infrastructure. In addition, the OSA recently hired two additional technology staff members to assist with implementation of technology projects, maintain technology assets and related records, and allow additional staff time for information security and monitoring activities.

Below are the Office of the State Auditor's responses to the audit findings included in the report, the OSA staff member primarily responsible for resolving each finding, and the OSA's estimated date the finding will be considered resolved:

Finding 1: The Office of the State Auditor did not assign asset numbers to all of its capital asset acquisitions, nor did it record those assets in its capital asset system, as required by its policy.

Response: Current OSA accounting staff are aware of the policy requirements, but the OSA will train new staff on the requirement to assign asset numbers to all capital asset acquisitions. Since the OSA assigns asset numbers when the capital asset is purchased (i.e., a purchase order issued), the OSA will implement a second verification of the asset number when the asset is received.

Person Responsible for Resolution: Matthew Lindemann, Director of Budget & Finance

Expected Date of Resolution: June 30, 2025

Finding 2: The Office of the State Auditor did not manage its asset inventory in compliance with state or office policies.

Response: The OSA will complete a full physical inventory of assets by the end of FY2025. If the physical inventory of assets identifies discrepancies, the OSA will investigate the discrepancies and update the capital asset system as appropriate.

Person Responsible for Resolution: Matthew Lindemann, Director of Budget & Finance

Expected Date of Resolution: June 30, 2025

Finding 3: The Office of the State Auditor has not implemented an information security program that aligns with best practices.

Response: In April 2024, the OSA hired a Chief Information Officer dedicated to leading the OSA's technology functions. This position will continue to develop the OSA's information security program. The OSA updated its security policies in the summer of 2024. The OSA plans to establish additional technology policies, standards, and procedures in FY2025.

Person Responsible for Resolution: Kathy Fraser, Chief Information Officer

Expected Date of Resolution: June 30, 2025

Finding 4: The Office of the State Auditor's inventory of information technology hardware and software did not contain important maintenance and security-related information.

Response: The OSA created a server and product inventory list that includes operating system, software version, and life cycle status. These inventory lists, along with the hiring of additional technology staff, will allow the OSA to keep its hardware and software updated and mitigate risks.

Person Responsible for Resolution: Kathy Fraser, Chief Information Officer

Expected Date of Resolution: Completed

Finding 5: The Office of the State Auditor has hardware and software that is outdated and no longer supported by its vendors or manufacturers.

Response: The OSA plans to replace its suite of Microfocus products, which are outdated and no longer supported, later this year. This project will significantly improve security and operational efficiencies. The OSA also plans to replace its phone system during this timeframe.

Person Responsible for Resolution: Kathy Fraser, Chief Information Officer

Expected Date of Resolution: December 31, 2025

Finding 6: The Office of the State Auditor did not conduct annual security awareness training for its employees.

Response: The finding relates to FY2022 and FY2023. In both FY2024 and FY2025, OSA staff completed security awareness training as part of the required annual training through the State of Minnesota's Enterprise Learning Management (ELM) system. The OSA continues to communicate cybersecurity threats and best practices to staff throughout the year.

Person Responsible for Resolution: Kathy Fraser, Chief Information Officer

Expected Date of Resolution: Completed

Finding 7: The Office of the State Auditor did not always follow best practices when authenticating users that access its information technology assets and software.

Response: The OSA has a project planned for FY2025 to strengthen its security posture. As part of this project, the OSA will improve authentication processes, implement stronger password requirements, and tighten controls for administrative accounts. The OSA will also leverage its investment in M365 to implement advanced security capabilities, such as Microsoft Intune, to enhance security.

Person Responsible for Resolution: Kathy Fraser, Chief Information Officer

Expected Date of Resolution: June 30, 2025

Finding 8: The Office of the State Auditor does not have a comprehensive security logging and monitoring program in place to detect and respond to security threats.

Response: In the fall of 2024, the OSA invested in software to monitor, detect, and prevent threats from executing on computer devices on the network. The software includes patch management, vulnerability assessment, endpoint detection and response (EDR), and managed detection and response (MDR). In addition, the OSA hired an IT Support Specialist that will allow for improved monitoring and maintenance of its network.

Person Responsible for Resolution: Kathy Fraser, Chief Information Officer

Expected Date of Resolution: Completed

Finding 9: The Office of the State Auditor does not follow best practices to detect, respond to, and prevent potential threats to its network.

Response: The OSA agrees with the importance of network security as evidenced by the OSA's recent actions. As discussed in the OSA's responses to other findings, the hiring of additional staff, process maturity, and software investments will allow the OSA to be proactive in detecting, responding to, and preventing threats to its network.

Person Responsible for Resolution: Kathy Fraser, Chief Information Officer

Expected Date of Resolution: December 31, 2025

The OSA is committed to resolving the above findings and further strengthening our sound financial and technology practices. Thank you again for your office's review and recommendations.

Sincerely,

A handwritten signature in black ink, appearing to read "Julie Blaha".

Julie Blaha
State Auditor



OLA



OLA

Financial Audit Staff

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

Audit Directors

Ryan Baker, CFE
Jordan Bjonfald, CPA
Kayla Borneman, CPA
Mark Mathison, CISA, CISSP, CPA (inactive)
Heather Rodriguez
Valentina Stone, CPA
Scott Tjomsland, CPA
Zach Yzermans, CPA

Audit Coordinators

Joe Sass, CISA

Audit Team Leads

Shannon Hatch, CFE
Gabrielle Johnson, CPA
Holly Runia

Senior Auditors

Tyler Billig, CPA
Nicholai Broekemeier
Deb Frost, CISA
Lisa Makinen, CPA
Alec Mickelson
Duy (Eric) Nguyen
Crystal Nibbe, CFE
Sheena Kurth
Erick Olsen
Rob Riggins, CISA, CISSP
Zakeeyah Taddese
Emily Wiant

Auditors

Joseph Anderson
Ria Bawek
Jonathan Brandtner
Gabrielle Gruber
Dylan Harris
Nicole Heggem
Andrea Hess
Braden Jaeger
Dustin Juell, CompTIA Security+
Christian Knox
Benjamin Path
Cary Sumague
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