



STATE OF WISCONSIN  
**Legislative Audit Bureau**  
NONPARTISAN • INDEPENDENT • ACCURATE

Report 22-26  
December 2022

# State of Wisconsin

## FY 2021-22 Financial Statements



## **Joint Legislative Audit Committee Members**

### Senate Members:

Robert Cowles, Co-chairperson  
Dale Kooyenga  
Howard Marklein  
Melissa Agard  
Tim Carpenter

### Assembly Members:

Vacant, Co-chairperson  
John Macco  
Mark Born  
Dianne Hesselbein  
Francesca Hong

# State of Wisconsin

## FY 2021-22 Financial Statements



STATE OF WISCONSIN

Legislative Audit Bureau

NONPARTISAN • INDEPENDENT • ACCURATE

Report 22-26  
December 2022

## Legislative Audit Bureau

---

**State Auditor**

Joe Chrisman

**Deputy State Auditor  
for Financial Audit**

Carolyn Stittleburg

**Financial Audit**

**Directors**

Sherry Haakenson

Erin Scharlau

**Assistant Financial**

**Audit Directors**

Brian Geib

Lisa Kasel

**Publications Designer  
and Editor**

Susan Skowronski

The Legislative Audit Bureau supports the Legislature in its oversight of Wisconsin government and its promotion of efficient and effective state operations by providing nonpartisan, independent, accurate, and timely audits and evaluations of public finances and the management of public programs. Bureau reports typically contain reviews of financial transactions, analyses of agency performance or public policy issues, conclusions regarding the causes of problems found, and recommendations for improvement.

Reports are submitted to the Joint Legislative Audit Committee and made available to other committees of the Legislature and to the public. The Audit Committee may arrange public hearings on the issues identified in a report and may introduce legislation in response to the audit recommendations. However, the findings, conclusions, and recommendations in the report are those of the Legislative Audit Bureau.

---

The Bureau accepts confidential tips about fraud, waste, and mismanagement in any Wisconsin state agency or program through its hotline at 1-877-FRAUD-17.

For more information, visit [www.legis.wisconsin.gov/lab](http://www.legis.wisconsin.gov/lab).

**Team Leaders**

Nathan Heimler  
Jennifer Multerer  
Matt Rossi  
Keri Routhieaux  
BreeAnn Schlenske  
Bridget Wieser  
Brandon Woller

**Auditors**

Kasey Bernard	David Menichini
Sherry Colstad	Matthew Owensby
Nicholas Dorey	William Sieminski
Wilson Gathirimu	Annie Skorupa
Lauren Gingell	Phillip Stapel
Paul Hauser	Alexis Strong
Zachary Johnson	Tyler Vance
Benjamin Kimmell	Ger Vang
Nicole Kulcyk	Elizabeth Wilson
Audrey Manser	Chloe Zhang
Haley Marks	

# Contents

---

<b>Letter of Transmittal</b>	<b>1</b>
<b>FY 2021-22 Annual Comprehensive Financial Report</b>	<b>3</b>
General Fund	3
Transportation Fund	4
Long-Term Debt	5
Unemployment Reserve Fund	5
University of Wisconsin System	5
Findings Related to Internal Control over Financial Reporting	6
Department of Administration	6
Department of Health Services	7
Board of Commissioners of Public Lands	8
University of Wisconsin System	8
Federal Funding for the Public Health Emergency	8
Coronavirus Relief Fund	9
Coronavirus State and Local Fiscal Recovery Funds	11
Federal Medical Assistance Percentage (FMAP)	13
Unemployment Insurance Funding	14
Other Matters of Interest	15
Clearing Appropriations	15
Office of the Commissioner of Insurance Statutory Transfer	16
Unemployment Interest and Penalty Account	17
Fringe Benefit Variance Accounts	17
<b>Auditor's Report</b>	<b>19</b>
Findings and Response Schedule	23
Finding 2022-001: Medical Assistance Program Third-Party Liability	23
Finding 2022-002: Department of Administration/Division of Enterprise Technology Information Security Access Review Process	25
Finding 2022-003: Department of Administration/Division of Enterprise Technology Information Security Policy Exception Process	27
Finding 2022-004: Department of Administration Information Technology Oversight and Monitoring Responsibilities	30
Finding 2022-005: Financial Reporting for the Medical Assistance Program	34
Finding 2022-006: Common School Fund—Service Organization Internal Controls	36
Finding 2022-007: UW System Information Technology Internal Control Deficiencies	38

<b>Corrective Action Plans</b>	<b>41</b>
Finding 2022-001: Medical Assistance Program Third-Party Liability	42
Finding 2022-002: Department of Administration/Division of Enterprise Technology Information Security Access Review Process	44
Finding 2022-003: Department of Administration/Division of Enterprise Technology Information Security Policy Exception Process	45
Finding 2022-004: Department of Administration Information Technology Oversight and Monitoring Responsibilities	46
Finding 2022-005: Financial Reporting for the Medical Assistance Program	48
Finding 2022-006: Common School Fund—Service Organization Internal Controls	50
Finding 2022-007: UW System Information Technology Internal Control Deficiencies	52

## **Response**

---

From the Department of Administration

## **Opinions Published Separately**

---

The financial statements and our opinions on them are included in the State of Wisconsin's Annual Comprehensive Financial Report (ACFR) for the fiscal year ended June 30, 2022.



STATE OF WISCONSIN

# Legislative Audit Bureau

Joe Chrisman  
State Auditor

22 East Mifflin Street, Suite 500  
Madison, Wisconsin 53703

Main: (608) 266-2818  
Hotline: 1-877-FRAUD-17

[www.legis.wisconsin.gov/lab](http://www.legis.wisconsin.gov/lab)  
[AskLAB@legis.wisconsin.gov](mailto:AskLAB@legis.wisconsin.gov)

December 22, 2022

Senator Robert Cowles, Co-chairperson  
Joint Legislative Audit Committee  
State Capitol  
Madison, Wisconsin 53702

Dear Senator Cowles:

We have completed our financial audit of the State of Wisconsin as of and for the fiscal year ended June 30, 2022, and issued unmodified opinions dated December 20, 2022, on the State's financial statements. The financial statements were prepared by the Department of Administration (DOA) in accordance with generally accepted accounting principles (GAAP) prescribed by the Governmental Accounting Standards Board (GASB) and are included in the State's fiscal year (FY) 2021-22 Annual Comprehensive Financial Report (ACFR), which may be found on DOA's website.

The ACFR helps to describe the State's fiscal condition and contains information on the funds administered by the State. In our report, we discuss the financial condition of the General Fund and Transportation Fund, which are the State's two largest governmental funds; quantify the State's long-term debt; provide information on the Unemployment Reserve Fund's and the University of Wisconsin System's financial statements; report seven significant deficiencies in internal control over financial reporting; and provide information on certain other matters we identified during the course of our audit.

We appreciate the courtesy and cooperation extended to us by DOA and other state agencies during the audit. During our FY 2022-23 audit, we will follow up on the progress of state agencies in implementing our recommendations.

A response from DOA follows the corrective action plans.

Respectfully submitted,

Joe Chrisman  
State Auditor

JC/CS/ss





---

General Fund  
Transportation Fund  
Long-Term Debt  
Unemployment Reserve Fund  
University of Wisconsin System  
Findings Related to Internal Control over Financial Reporting  
Federal Funding for the Public Health Emergency  
Other Matters of Interest

---

# FY 2021-22 Annual Comprehensive Financial Report

---

***We provided unmodified  
opinions on the State's  
financial statements as of  
and for the year ended  
June 30, 2022.***

The Department of Administration (DOA) prepares the Annual Comprehensive Financial Report (ACFR), which contains financial statements prepared in accordance with generally accepted accounting principles (GAAP) prescribed by the Governmental Accounting Standards Board (GASB). The ACFR helps to describe the State's fiscal condition and contains information on state funds, including the State's General Fund, the Transportation Fund, the University of Wisconsin (UW) System, the Unemployment Reserve Fund, and the Wisconsin Retirement System. In addition to the financial statements and notes, the ACFR includes Management's Discussion and Analysis, which describes the State's financial performance for the year, and a statistical section, which provides the reader with information to assist in understanding the State's economic condition. The statistical section includes information such as financial trends and debt capacity. We have completed a financial audit of the State's ACFR and have provided unmodified opinions on the State's financial statements as of and for the year ended June 30, 2022.

## General Fund

***As reported on a GAAP  
basis, the General Fund  
total fund balance  
improved from \$1.2 billion  
as of June 30, 2021, to  
\$4.6 billion as of  
June 30, 2022.***

On a GAAP basis, the General Fund total fund balance improved from \$1.2 billion as of June 30, 2021, to \$4.6 billion as of June 30, 2022, as shown on page 44 of the ACFR. The General Fund total fund balance is primarily made up of amounts restricted or committed for specific purposes, and an unassigned amount. The largest component of total fund balance is the unassigned fund balance of \$2.2 billion. The unassigned fund balance represents that, as of June 30, 2022, more resources were available than were spent or obligated in the short term.

***The State's rainy day fund had a balance of \$1.7 billion as of June 30, 2022.***

The second largest component of total fund balance is the committed fund balance, which was \$1.7 billion as of June 30, 2022, and includes the amount held in the statutory Budget Stabilization Fund, also known as the State's rainy day fund. The balance in the Budget Stabilization Fund increased \$3.8 million in fiscal year (FY) 2021-22, primarily from interest income. Even though tax revenues in FY 2021-22 exceeded projections in 2021 Wisconsin Act 58, the 2021-23 Biennial Budget Act, DOA did not make a transfer to the Budget Stabilization Fund for FY 2021-22 because the balance in the Budget Stabilization Fund exceeded the maximum balance allowed under Wisconsin Statutes.

***Total General Fund revenue increased by \$4.8 billion and totaled \$39.3 billion for FY 2021-22.***

On page 31 of Management's Discussion and Analysis, DOA reported that total General Fund revenue increased by \$4.8 billion and totaled \$39.3 billion for FY 2021-22. This increase was largely attributed to an increase of \$1.9 billion in income tax revenues and an increase of \$663.2 million in sales and excise tax revenues. In addition, federal revenues increased by \$2.0 billion, largely related to federal revenues the State received as a result of the public health emergency.

***Total General Fund expenditures increased by \$2.2 billion and totaled \$33.6 billion for FY 2021-22.***

On page 31 of Management's Discussion and Analysis, DOA reported that total General Fund expenditures increased by \$2.2 billion and totaled \$33.6 billion for FY 2021-22. This increase was attributed to grants and aid to individuals and organizations related, in part, to the public health emergency, increases in Medical Assistance expenditures, and increases in aids to schools.

***DOR updated tax withholding tables as of January 1, 2022, which resulted in a reduction in the estimated tax refunds liability as of June 30, 2022.***

The Department of Revenue (DOR) updated the individual income tax withholding tables, effective January 1, 2022. This update reduced the estimated tax refunds liability by \$884.1 million, from \$2.4 billion as of June 30, 2021, to \$1.5 billion as of June 30, 2022. This estimate relates primarily to amounts collected from individuals through payroll withholding and tax filing that will be refunded when individuals file income tax returns in 2023.

***On a GAAP basis, the total fund balance of the Transportation Fund increased from \$1.0 billion as of June 30, 2021, to \$1.3 billion as of June 30, 2022.***

## Transportation Fund

On a GAAP basis, the total fund balance of the Transportation Fund increased from \$1.0 billion as of June 30, 2021, to \$1.3 billion as of June 30, 2022, as shown on page 44 of the ACFR. On page 33 of Management's Discussion and Analysis, DOA noted that the majority of the Transportation Fund's balance (96.7 percent) was restricted by the Wisconsin Constitution to be used for transportation purposes. Primary revenue sources in the Transportation Fund include motor fuel taxes, federal revenues, and registration fees. On page 33 of Management's Discussion and Analysis, DOA noted that total revenues increased by \$103.9 million to a total of \$3.1 billion, primarily as a result of increases in federal revenues and motor fuel taxes. Transportation Fund expenditures increased by \$215.6 million to a total of \$2.9 billion in FY 2021-22.

2021 Wisconsin Act 58, the 2021-23 Biennial Budget Act, required a transfer of \$134.2 million from the General Fund to the Transportation

Fund in FY 2021-22. The transfer was made and was reported as a Transfer In on the Transportation Fund financial statements.

## Long-Term Debt

***The State's long-term debt decreased from \$12.9 billion as of June 30, 2021, to \$12.5 billion as of June 30, 2022.***

On a GAAP basis, the State's long-term debt decreased from \$12.9 billion as of June 30, 2021, to \$12.5 billion as of June 30, 2022, as shown on page 36 of Management's Discussion and Analysis. The State repaid long-term debt in excess of new debt issuances during FY 2021-22, resulting in the decrease in overall debt. As shown on page 36 of Management's Discussion and Analysis, \$1.0 billion in new general obligation bonds and notes were issued during FY 2021-22. This amount includes \$378.2 million for UW System academic facilities and \$315.1 million for transportation projects. The amount of outstanding annual appropriation bonds decreased by \$183.3 million, and revenue bonds decreased by \$78.9 million.

## Unemployment Reserve Fund

***The Unemployment Reserve Fund's net position increased from \$1.2 billion as of June 30, 2021, to \$1.4 billion as of June 30, 2022.***

Wisconsin's Unemployment Insurance (UI) program is accounted for in the State's ACFR in the Unemployment Reserve Fund, which is administered by the Department of Workforce Development (DWD). The Unemployment Reserve Fund collects contributions made by employers and other federal program receipts that accumulate to make payments to employees who have lost their jobs. As shown on page 52 of the ACFR, the Unemployment Reserve Fund's net position increased from \$1.2 billion as of June 30, 2021, to \$1.4 billion as of June 30, 2022, or by \$203.0 million.

***Unemployment benefit payments of \$683.0 million were reported for FY 2021-22, compared to \$3.5 billion for FY 2020-21.***

In Management's Discussion and Analysis on page 34, unemployment benefit payments of \$683.0 million were reported for FY 2021-22, compared to \$3.5 billion for FY 2020-21. This decline reflects the improvement in the unemployment rate from FY 2020-21 to FY 2021-22, along with the end of the federal unemployment insurance benefits related to the public health emergency. Federal assistance contributed \$334.1 million in aid in FY 2021-22, compared to \$2.5 billion in federal assistance in FY 2020-21.

2021 Wisconsin Act 58, the 2021-23 Biennial Budget Act, required a transfer of \$120.0 million from the General Fund to the Unemployment Reserve Fund in the 2021-23 biennium. During FY 2021-22, a \$60.0 million transfer was completed, which was reported as a Transfer In on the Unemployment Reserve Fund financial statements.

## University of Wisconsin System

As required by s. 13.94 (1) (t), Wis. Stats., we performed a financial audit of UW System, which included an audit of UW System's financial statements as of and for the year ended June 30, 2022, and issued as report 22-25. UW System's financial statements are also presented in the State's ACFR. As shown on page 52 of the ACFR, UW System's net

position increased from \$6.0 billion as of June 30, 2021, to \$6.4 billion as of June 30, 2022, primarily as a result of the reporting of a net pension asset and a net other postemployment benefit (OPEB) asset.

## **Findings Related to Internal Control over Financial Reporting**

***We identified seven significant deficiencies in internal control over financial reporting.***

We identified internal control deficiencies during our audit that are required to be reported under *Government Auditing Standards*. Specifically, we identified seven significant deficiencies in internal control. A significant deficiency is a deficiency or a combination of deficiencies in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. In comparison, a material weakness is a deficiency or combination of deficiencies in internal control such that there is a reasonable possibility that a material misstatement of the State's basic financial statements will not be prevented, or will not be detected and corrected, on a timely basis. We did not report any material weaknesses. The Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters, which begins on page 21, discusses each concern and includes the response from management of the responsible agency. The corrective action plans from agency management begin on page 42.

### **Department of Administration**

***We report significant deficiencies in DOA's IT security, including insufficient reviews of access and insufficient IT policy exception procedures.***

Wisconsin Statutes assign DOA responsibility for the State's information technology (IT) services. Under s. 16.971 (2), Wis. Stats., DOA is required to work with executive branch agencies to establish IT policies, procedures, and planning processes. In addition, DOA is required to monitor adherence to these policies, procedures, and processes. We first made recommendations to DOA regarding the establishment of IT policies during our FY 2014-15 audit, seven years ago. In subsequent audits, we have recommended that DOA take steps to identify, assess, and address risks for the State's IT environment. Although DOA has taken steps, we continued to identify deficiencies in DOA's IT security over the operations of the State's data center, including insufficient reviews of access in certain areas (Finding 2022-002) and insufficient IT policy exception procedures (Finding 2022-003).

***DOA continued to be in noncompliance with Wisconsin Statutes that require it to provide oversight and monitoring of executive branch agency IT operations.***

In addition, DOA continued to be in noncompliance with s. 16.971 (2), Wis. Stats., which requires DOA to provide oversight and monitoring of executive branch agency IT operations and adherence to the State of Wisconsin *IT Security Policy Handbook* and related standards (Finding 2022-004). Although DOA completed and published a dashboard of agency compliance with the State of Wisconsin *IT Security Policy Handbook* and related standards, DOA did not take sufficient steps to assess the accuracy of the agency-reported information. Given the connections among agencies in the State's network, IT weaknesses at one agency can affect IT security for other agencies. Therefore, it is important

that DOA and the other state agencies work in cooperation in seeking to resolve deviations from the State of Wisconsin *IT Security Policy Handbook* and related standards.

***We recommend DOA report to the Joint Legislative Audit Committee on the status of its efforts to implement our recommendations.***

Because these audit concerns have not been fully resolved, there continues to be increased risk that the State's IT systems are not being properly controlled. Given that these concerns have continued for several years, DOA should take corrective actions to implement the recommendations we made and report to the Joint Legislative Audit Committee on the status of its efforts to do so.

### **☑ Recommendation**

---

*We recommend the Wisconsin Department of Administration report to the Joint Legislative Audit Committee by March 31, 2023, on:*

- *revisions made to its access review process, and plans for completing reviews by June 30, 2023 (Finding 2022-002);*
- *revisions made to the information security policy exception process, communications made to agencies regarding the revised process and available training, and steps taken to complete the review of deviations from the State of Wisconsin IT Security Policy Handbook and related standards (Finding 2022-003); and*
- *its monitoring plan for reviewing the effectiveness of agency-reported information in its dashboard, and progress made in developing plans for performing vulnerability assessments and updating its risk management program (Finding 2022-004).*

## **Department of Health Services**

***We report two significant deficiencies in internal control over financial reporting at DHS related to the General Fund.***

We identified two internal control deficiencies related to financial reporting for the General Fund at the Department of Health Services (DHS). First, we identified a Medical Assistance (MA) Program payment for outpatient services that was not properly identified and denied because of cost avoidance rules programmed in the Medicaid Management Information System (MMIS) (Finding 2022-001). We recommend that DHS review and update the MMIS cost avoidance rules, identify other payments that may have been improper, return improper payment amounts to the federal government, and perform an assessment and implement additional procedures for review of cost avoidance rules.

Second, we reported concerns with the financial reporting for the MA Program (Finding 2022-005). In FY 2021-22, DHS claimed additional federal funds for the MA Program, as allowed by Section 9817 of the American Rescue Plan Act of 2021. We found DHS did not consider whether the funds derived from the increased federal medical assistance percentage (FMAP) required an adjustment to properly reflect the activity in the General Fund financial statements. We recommend that DHS develop and implement procedures to evaluate the potential effects of changes in the programs it administers and use the additional procedures to evaluate changes that may require further consideration and adjustment for financial reporting.

### **Board of Commissioners of Public Lands**

*We report a significant deficiency in internal control over financial reporting at the Board of Commissioners of Public Lands related to obtaining and reviewing a service organization audit report.*

We identified an internal control deficiency related to the Board of Commissioners of Public Lands (BCPL) assessment of internal controls at a custodian bank it relies on for certain investment transaction processing and safekeeping (Finding 2022-006). We recommend that BCPL complete an assessment of its reliance on the custodian bank and either implement internal controls to ensure the accuracy of information it receives from the custodian bank or obtain and review the effectiveness of the custodian bank's internal controls as reported in a service organization audit report.

### **University of Wisconsin System**

*We report a significant deficiency in internal control over financial reporting at UW System related to policies to require access reviews and obtaining and reviewing service organization audit reports.*

We identified concerns with UW System's internal controls related to a new computer application called ShopUW+, which was implemented in April 2021 (Finding 2022-007). We found that UW System Administration lacked adequate policies for UW institution review of all access related to the new application during FY 2021-22. We also found that UW System Administration had not obtained a service organization audit report to assess the internal controls of a third-party vendor for the new application. We recommend that UW System Administration develop policies to require such access reviews and monitor that they are completed in a timely manner and to obtain and review service organization audit reports for certain third-party vendors.

## **Federal Funding for the Public Health Emergency**

In March 2020, the federal government and the State declared a public health emergency in response to COVID-19. In response to the public health emergency, the federal government enacted several pieces of legislation, including the Coronavirus Aid, Relief, and Economic Security (CARES) Act and the American Rescue Plan Act (ARPA) of 2021.

***Federal legislation to address the public health emergency provided additional federal funding to Wisconsin.***

Under these federal laws, the State received additional federal funding for certain existing programs, including Medical Assistance and the UI program, as well as funding under new programs, including the Coronavirus Relief Fund (CRF), the Education Stabilization Fund, and the Coronavirus State and Local Fiscal Recovery Funds (CSLFRF). As a condition of receiving federal funds, state agencies must meet the audit requirements of the federal Single Audit Act of 1984, as amended, and of the federal Office of Management and Budget *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* (Uniform Guidance). We are currently performing this audit for FY 2021-22 and anticipate its issuance in spring 2023.

Funding to address the public health emergency affected financial reporting in FY 2021-22. As part of our audit of the State's ACFR, we reviewed and summarized information regarding several key areas related to the public health emergency and the State's finances, including:

- the CRF;
- the CSLFRF;
- the revised FMAP; and
- unemployment benefits.

In report 22-25, we discussed UW System's administration of certain portions of the Higher Education Emergency Relief Fund (HEERF), which is a program funded under the federal CARES Act, the Coronavirus Response and Relief Supplemental Appropriations Act, and ARPA.

## **Coronavirus Relief Fund**

***In April 2020, the State was advanced \$2.0 billion in funding under the CRF.***

The CARES Act created the CRF to distribute money directly to state, local, tribal, and territorial governments. The federal government advanced \$2.0 billion in CRF funds to the State of Wisconsin in April 2020 and included certain stipulations, including that the funds must be used for expenses that are incurred in response to the public health emergency between March 1, 2020, and December 30, 2020. Subsequent federal legislation extended the deadline for use of the funds to December 31, 2021. The federal guidelines allowed expenditures to be recorded through September 30, 2022.

***During FY 2021-22, \$280.8 million in expenditures at 32 state agencies was incurred and paid by the CRF.***

As shown in Table 1, DOA reported that \$280.8 million in expenditures at 32 state agencies was incurred and paid by the CRF during FY 2021-22. The majority of the CRF activity was recorded in the General Fund. According to amounts reported by DOA in the State's accounting system, the largest total expenditures were incurred and paid by DOA, which expended \$119.1 million in CRF funds, including \$110.0 million that was paid to local school districts as school aids.

Table 1

**Expenditures Incurred and Paid by the Coronavirus Relief Fund (CRF)<sup>1</sup>**  
FY 2021-22

	Expenditures	Percentage of Total
Department of Administration	\$ 119,080,423	42.4%
Department of Revenue	80,547,882	28.7
Department of Health Services	50,719,552	18.1
Department of Workforce Development	26,282,855	9.4
Department of Natural Resources	875,916	0.3
Department of Transportation	711,877	0.3
Department of Public Instruction	546,752	0.2
Department of Children and Families	406,523	0.1
Department of Safety and Professional Services	314,186	0.1
Wisconsin Historical Society	314,005	0.1
Department of Veterans Affairs	224,699	0.1
Department of Justice	189,171	0.1
Other Agencies <sup>2</sup>	543,547	0.2
<b>Total</b>	<b>\$ 280,757,387</b>	<b>100.0%</b>

<sup>1</sup> As reported by DOA in the State's accounting system for the fiscal year ended June 30, 2022.

<sup>2</sup> Includes 20 other state agencies that had expenditures between negative \$13,506 and \$116,630.

***DOR expended \$80.5 million in CRF funds to provide grants to small businesses and farmers that were adversely affected by the public health emergency.***

DOR expended \$80.5 million in CRF funds to provide grants to small businesses and farmers that were adversely affected by the public health emergency, including \$49.9 million for the Wisconsin Farm Support program, which provided payments to over 20,000 farmers in Wisconsin in FY 2021-22, and \$30.6 million for the Wisconsin Tomorrow Small Business grant program, which provided payments to over 6,000 small businesses in FY 2021-22. In report 22-21, we reviewed DOR's administration of the Wisconsin Tomorrow program.

Finally, DHS expended \$50.7 million in CRF funds including payments for programs for testing and personal protective equipment, and DWD expended \$26.3 million in CRF funds, largely to fund UI administrative costs.

According to amounts reported by DOA in the accounting system, the full amount of CRF funds was expended by September 30, 2022.



## Coronavirus State and Local Fiscal Recovery Funds

***In May 2022, the State was advanced \$1.5 billion in funding under the CSLFRF, including \$207.7 million for local governments.***

ARPA created the CSLFRF to distribute money directly to state, local, tribal, and territorial governments. The State was allocated \$3.0 billion in CSLFRF funding, and was advanced \$1.5 billion in May 2021, including \$205.8 million to be distributed to local governments. In May 2022, the State was advanced \$1.5 billion, including \$207.7 million to be distributed to local governments. The CSLFRF funding included certain stipulations, including that the funds must be used to:

- respond to the public health emergency or its negative economic impacts;
- respond to the needs of workers performing essential work during the public health emergency;
- provide government services to the extent revenue losses due to the public health emergency reduced revenues; and
- make necessary investments in water, sewer, or broadband infrastructure.

Further, federal regulations stipulate that eligible expenditures must be incurred between March 3, 2021, and December 31, 2024, and spent through December 31, 2026.

***During FY 2021-22, \$730.3 million in expenditures at 13 state agencies was incurred and paid by the CSLFRF.***

As shown in Table 2, DOA reported \$730.3 million in expenditures at 13 state entities was incurred and paid by the CSLFRF during FY 2021-22. The majority of the CSLFRF activity was recorded in the General Fund. According to amounts reported by DOA in the State's accounting system, the largest total expenditures were incurred by DOR, DHS, and DOA.

Table 2  
**Expenditures Incurred and Paid by the  
 Coronavirus State and Local Fiscal Recovery Funds (CSLFRF)<sup>1</sup>**  
 FY 2021-22

	Expenditures	Percentage of Total
Department of Revenue	\$333,965,611	45.7%
Department of Health Services	161,868,117	22.2
Department of Administration	117,226,496	16.1
Wisconsin Economic Development Corporation	68,005,745	9.3
Department of Transportation	25,000,000	3.4
Other Agencies <sup>2</sup>	24,199,429	3.3
<b>Total</b>	<b>\$730,265,397</b>	<b>100.0%</b>

<sup>1</sup> As reported by DOA in the State’s accounting system for the fiscal year ended June 30, 2022.

<sup>2</sup> Includes eight other state agencies that had expenditures between \$264,598 and \$8.4 million.

***In FY 2021-22, DOR expended \$334.0 million in CSLFRF funds to provide grants to small businesses and local governments in Wisconsin.***

DOR expended a total of \$334.0 million in CSLFRF funds in FY 2021-22 to assist businesses that had significant losses resulting from the public health emergency, or to allocate funding to smaller local governments in Wisconsin. DOR provided:

- \$53.8 million in grants to over 10,700 small businesses under the Wisconsin Tomorrow Small Business program;
- \$72.3 million in grants to 970 lodging establishments under the Wisconsin Tomorrow Lodging Grant program; and
- \$207.7 million to over 1,500 non-entitlement units of government (NEUs), which are smaller units of general local governments, as designated by the U.S. Treasury.

In report 22-21, we reviewed DOR’s administration of the Wisconsin Tomorrow program.

***In FY 2021-22, DHS reported \$161.9 million in expenditures funded by the CSLFRF.***

According to the state’s accounting system, DHS reported \$161.9 million in expenditures funded by the CSLFRF, including \$66.6 million under the DHS Agency Staffing Resource Assistance Service program, which was created as a temporary strategy to assist nursing homes, long-term care facilities, and assisted living facilities in

mitigating staffing challenges during the public health emergency, and \$57.8 million for COVID-19 testing, contact tracing, and other planning for the public health emergency.

***In FY 2021-22, DOA administered a number of programs to assist local governments and businesses negatively affected by the public health emergency.***

DOA also administered a number of grant programs to assist local governments and businesses negatively affected by the public health emergency. For example, DOA administered a grant program that provided \$15.3 million to school districts for mental health initiatives and \$8.4 million to the City of Milwaukee for a violence prevention program during FY 2021-22. In addition, DOA provided individual grants to various Wisconsin businesses to address revenue losses and expenditures incurred due to the public health emergency, including a total of:

- \$30.9 million in grants to 231 event venues and businesses;
- \$22.2 million in grants to 102 nonprofit organizations in Wisconsin for the Beyond the Classroom grant program;
- \$15.0 million in grants to 118 destination marketing organizations, such as chamber of commerce organizations and convention and visitor bureaus, to promote tourism in Wisconsin; and
- \$10.0 million in grants to 48 privately owned movie theaters.

***As of June 30, 2022, \$1.8 billion in CSLFRF funds remained to be expended.***

The \$1.8 billion in remaining CSLFRF funds is reflected in Cash and Cash Equivalents and Unearned Revenue in the General Fund Balance Sheet as of June 30, 2022. As of December 15, 2022, accounting records show an additional \$9.0 million in expenditures was funded by the CSLFRF. This leaves a remaining balance of \$1.8 billion, including \$23.0 million in interest earnings since FY 2021-22. As we stated in report 22-23, in December 2022 DOA indicated it had plans for using most of the funds.

## **Federal Medical Assistance Percentage (FMAP)**

***In FY 2021-22, the State received \$641.3 million in additional funds for the MA Program as a result of an increase in Wisconsin's FMAP.***

The FMAP is the percentage of MA Program expenditures the federal government will fund for the State. In March 2020, the federal Families First Coronavirus Response Act provided a temporary 6.2 percent increase in Wisconsin's FMAP for benefit payments. The increase in the FMAP is anticipated to be in place until the federal government determines the public health emergency period for COVID-19 has ended. In FY 2021-22, the State received \$641.3 million in additional funding as a result of the increased FMAP.

As of September 2022, DHS reported to the Joint Committee on Finance that it projected a \$504.9 million surplus in the Medical Assistance budget for the 2021-23 biennium. The surplus was partially attributed to the

increased FMAP, which DHS estimated would continue to be available through at least March 2023.

***In FY 2021-22, DHS also claimed and received an additional \$329.2 million in federal funds under the MA Program, as allowed under ARPA.***

During FY 2021-22, DHS claimed and received an additional \$329.2 million in federal funds under the MA Program, as allowed by Section 9817 of ARPA. The claim was calculated based upon an increase in the FMAP by 10 percent for certain home and community-based services provided to participants during the period April 1, 2021, through March 31, 2022. Federal regulations require that the funds derived from the increased FMAP be reinvested in the MA Program and be used to implement or supplement home and community-based services to participants. DHS reinvested \$50.6 million of these funds during FY 2021-22 and reinvestment of the remaining funds will need to occur prior to March 31, 2025. At that time, any unexpended balance is required to be returned to the federal government. Because of the reinvestment requirement, the receipt of these funds does not result in general purpose revenue savings, and the projection of the MA surplus does not include these funds.

## **Unemployment Insurance Funding**

***Federal pandemic unemployment benefits to individuals expired on September 4, 2021.***

Federal benefits established through the federal CARES Act, and extended by the federal Continued Assistance Act and ARPA, to provide benefits under the unemployment benefit programs for individuals whose employment was affected by the public health emergency ended in FY 2021-22. These programs included the Federal Pandemic Unemployment Compensation program and the Pandemic Unemployment Assistance program, both of which expired on September 4, 2021.

***Programs were also established to provide relief to employers, including federal reimbursement of certain unemployment benefits.***

The CARES Act also established programs to provide relief to employers through federal reimbursement of certain regular unemployment benefits. In addition, 2019 Wisconsin Act 185 and 2021 Wisconsin Act 4 provided additional employer relief through:

- the use of the solvency account for regular unemployment benefits provided to employees of taxable employers; and
- the use of funds in the interest and penalty account, which is maintained in the State's General Fund, for regular unemployment benefits provided to employees of reimbursable employers.

***DWD completed its review of regular unemployment benefit payments made during the public health emergency to determine the funding source for these payments.***

During FY 2021-22, DWD completed its review of approximately \$1.5 billion in regular unemployment benefit payments made during the public health emergency to determine whether the payments could be funded by federal reimbursements, be funded by the interest and penalty account, or be transferred to the solvency account. As a result of this review, DWD determined that:

- \$183.7 million was funded through reimbursements from the federal government;
- \$69.8 million was funded through the interest and penalty account in the General Fund; and
- \$1.3 billion was transferred from employer accounts to the Fund’s solvency account.

As of June 30, 2022, the balance of the solvency account was a deficit balance of \$1.7 billion, which when combined with the \$3.1 billion balance in the employer accounts, results in the Unemployment Reserve Fund net position of \$1.4 billion.

## Other Matters of Interest

During our audit work, we identified four issues that did not meet the requirements for reporting under *Government Auditing Standards*, but are matters of interest. These issues included clearing appropriation balances, an Office of Commissioner of Insurance (OCI) transfer, the Unemployment interest and penalty account, and fringe benefit variance accounts. We will follow up on the status of these issues during our FY 2022-23 audit.

### Clearing Appropriations

***DOA is responsible for ensuring expenditures and revenues recorded in clearing appropriations are moved out of clearing appropriations before the end of the fiscal year.***

Statutes provide DOA with the authority to create clearing appropriations, which allow an agency to record expenditures temporarily until the agency determines the correct appropriation to charge. DOA policies in the *Wisconsin Accounting Manual* also allow an agency to record revenues in a clearing appropriation temporarily until the agency determines the correct appropriation to charge. DOA is responsible for ensuring the accounting transactions are completed to move the expenditures or revenues out of the clearing appropriations before the close of the accounting records for the fiscal year.

***As of June 30, 2022, one clearing appropriation had a remaining balance as of June 30, 2022.***

In response to our recommendation in report 21-23, DOA continued its efforts to resolve remaining balances in clearing appropriations. As of June 30, 2022, a negative balance of \$9.4 million remained in a clearing appropriation used by DOA to administer the central fuel procurement program, which allows the state to consolidate fuel purchases for utilities and bargain for better utility rates by providing utilities in bulk. DOA reassessed the nature of this appropriation and it is no longer used in FY 2022-23. Instead, this activity has been moved into a custody appropriation, which more accurately reflects the activity.

***DOJ transferred the \$33.1 million balance from its clearing appropriation to three other DOJ appropriations as of June 30, 2022.***

As we noted in report 21-23, at the end of FY 2020-21, a positive balance remained in a DOJ clearing appropriation as an outstanding court order stated that the amounts could not be transferred out of the clearing appropriation. In March 2022, a final order on the case lifted the outstanding court order regarding the funding in the clearing appropriation. As a result, in FY 2021-22 DOJ transferred the \$33.1 million balance from the clearing appropriation to three other DOJ appropriations, including \$26.7 million to DOJ’s gifts and grants appropriation. The court decision is currently under appeal.

### **Office of the Commissioner of Insurance Statutory Transfer**

***DOA is responsible for maintaining the State’s accounting records and ensuring budgetary controls are enforced.***

DOA is responsible for maintaining the State’s accounting records in the State’s enterprise resource planning system, which is known as STAR, approving all payments, and ensuring budgetary controls are enforced. DOA has procedures in place to track statutorily required lapses and transfers and to monitor that statutorily required lapses and transfers are made by agencies prior to the close of the accounting records each fiscal year.

***A statutorily required transfer of \$1.5 million between two OCI appropriations was not made timely.***

2021 Wisconsin Act 58, the 2021-23 Biennial Budget Act, required OCI to transfer \$1.5 million from its general program operations appropriation to another OCI program revenue appropriation in each year of the biennium. However, neither OCI nor DOA sufficiently assessed whether the transfer for FY 2021-22 was made before the accounting records were closed on September 9, 2022. Subsequent to the close of the accounting records for FY 2021-22, DOA staff realized that the OCI transfer had not occurred when the OCI program revenue appropriation was found to be in an overdraft status.

***In October 2022, DOA re-opened the accounting records for FY 2021-22 to process the statutorily required transfer.***

DOA staff indicated that the specificity of the statutory language in 2021 Wisconsin Act 58, the 2021-23 Biennial Budget Act, would not allow the OCI transfer to be made in FY 2022-23. Therefore, DOA re-opened the FY 2021-22 accounting records on October 9, 2022, and processed a transaction to transfer the funds. It is highly unusual to re-open the accounting records after the records are closed for the fiscal year. DOA officials we spoke with were unaware of this happening in the past. Re-opening a closed accounting period can introduce risk into the process of preparing the financial statements and creates a precedent that could allow for potentially inappropriate manipulation of the accounting records if it becomes a common practice. We recommend that DOA review its existing procedures and add additional procedures to ensure all statutorily required transfers are made before the accounting records are closed each year.

**Unemployment Interest and Penalty Account**

*There is a deficit balance of \$49.2 million in the Unemployment interest and penalty account in the General Fund as of June 30, 2022.*

During FY 2021-22, the Unemployment Reserve Fund received reimbursement totaling \$69.8 million from the interest and penalty account in the General Fund, which is a program revenue appropriation established under s. 20.445 (1) (gd), Wis. Stats. As allowed under 2019 Wisconsin Act 185, this amount was received for a portion of benefit payments made during the public health emergency to former employees of reimbursable employers, which are employers such as the State of Wisconsin that reimburse benefits paid by the Unemployment Reserve Fund for its former employees. As a June 30, 2022, the interest and penalty account in the General Fund was in a deficit, or overdraft, position of \$49.2 million. In a plan submitted to DOA, DWD reported that, based upon a review of the annual historical net revenues received into this account, it will take approximately 24 years before the overdraft would be eliminated.

**Fringe Benefit Variance Accounts**

In processing payroll, DOA is responsible for deducting amounts from employee’s paychecks for health insurance benefits. The Department of Employee Trust Funds (ETF) bills DOA for these amounts and for the employer share of health insurance premiums. When certain changes in benefits occur, such as a new hire, a termination, or a change in benefit type, there can be a timing difference between what is being deducted from an employee’s paycheck and the employer’s share of those benefits, and what ETF bills the agency for these amounts. In these cases, DOA pays the amount billed by ETF and charges the fringe benefit variance account for the amount billed for the employee.

*The balance in the health insurance fringe benefit variance account increased from \$20.5 million as of June 30, 2021, to \$23.4 million as of June 30, 2022.*

DOA is responsible for reviewing the balance in variance accounts and working with state agencies to research and resolve the variances. Although it would not be unexpected to have a balance in the health insurance fringe benefit variance account, the balance would be expected to be resolved in a timely manner and not increase over time. However, as we reported in our FY 2020-21 audit (report 21-23), balances in the health insurance fringe benefit variance account have steadily increased since the implementation of STAR HCM in 2016. The balance in the health insurance fringe benefit variance account as of June 30, 2022, was \$23.4 million, which was an increase of \$2.9 million from the \$20.5 million balance as of June 30, 2021. DOA indicated that there are ongoing efforts to resolve the variance, with the current timeline for resolution being the end of calendar year 2023. It is important that DOA address the variance, as it will become increasingly more difficult to resolve over time. We note that a similar fringe benefit variance account exists for life insurance.







---

# Auditor's Report

---



22 East Mifflin Street, Suite 500  
Madison, Wisconsin 53703Main: (608) 266-2818  
Hotline: 1-877-FRAUD-17[www.legis.wisconsin.gov/lab](http://www.legis.wisconsin.gov/lab)  
[AskLAB@legis.wisconsin.gov](mailto:AskLAB@legis.wisconsin.gov)

## Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters

Honorable Members of the Legislature

The Honorable Tony Evers, Governor

We have audited the financial statements and the related notes of the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the State of Wisconsin, which collectively comprise the State's basic financial statements, as of and for the year ended June 30, 2022, and have issued our report thereon dated December 20, 2022.

We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, which is issued by the Comptroller General of the United States. The basic financial statements and related auditor's opinions have been included in the State of Wisconsin's Annual Comprehensive Financial Report (ACFR) for the fiscal year ended June 30, 2022.

Our report includes a reference to other auditors who audited the financial statements of the Environmental Improvement Fund, the Deferred Compensation Fund, the Wisconsin Housing and Economic Development Authority, the University of Wisconsin (UW) Hospitals and Clinics Authority, and the UW Foundation, as described in our report on the State of Wisconsin's basic financial statements. The financial statements of the Environmental Improvement Fund, the UW Hospitals and Clinics Authority, and the Wisconsin Housing and Economic Development Authority were audited in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*. This report does not include the results of the other auditors' testing of internal control over financial reporting or compliance and other matters that were reported on separately by those auditors. Although the financial statements of the Deferred Compensation Fund and the UW Foundation were audited in accordance with auditing standards generally accepted in the United States of America, they were not audited in accordance with *Government Auditing Standards* and, accordingly, this report does not include reporting on internal control over financial reporting or instances of reportable noncompliance associated with the Deferred Compensation Fund or the UW Foundation.

### Report on Internal Control over Financial Reporting

Management of the State of Wisconsin is responsible for establishing and maintaining effective internal control over financial reporting (internal control). In planning and performing our audit of the financial statements, we considered the State's internal control as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent misstatements, or to detect and correct misstatements on a timely basis. A *material weakness* is a

deficiency or a combination of deficiencies in internal control such that there is a reasonable possibility that a material misstatement of the State's basic financial statements will not be prevented, or that a material misstatement will not be detected and corrected on a timely basis. A *significant deficiency* is a deficiency or a combination of deficiencies in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control, described in the accompanying Findings and Responses Schedule as Findings 2022-001 through 2022-007 that we consider to be significant deficiencies.

### **Report on Compliance and Other Matters**

As part of obtaining reasonable assurance about whether the State's basic financial statements are free from material misstatement, we performed tests of compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

### **Responses to Findings**

*Government Auditing Standards* require the auditor to perform limited procedures on the agency-specific written response to the findings identified in the audit and described in the accompanying Finding and Response Schedule. The corrective action plans begin on page 42. The responses and corrective action plans were not subjected to other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

### **Purpose of This Report**

This report is an integral part of an audit performed in accordance with *Government Auditing Standards* and should be used when considering the State's internal control and compliance. The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the result of that testing, and not to provide an opinion on the effectiveness of the State's internal control or on compliance. Accordingly, this report is not suitable for any other purpose.

LEGISLATIVE AUDIT BUREAU



December 20, 2022

## FINDINGS AND RESPONSES SCHEDULE

This schedule includes seven deficiencies in internal control over financial reporting that we consider to be significant deficiencies. These deficiencies in internal control over financial reporting are required to be reported by auditing standards generally accepted in the United States of America and Government Auditing Standards. Findings 2021-002, 2021-003, and 2021-004 from the prior year (report 21-23) are no longer reportable. Repeat findings from report 21-23 are indicated with an asterisk (\*).

### **Finding 2022-001: Medical Assistance Program Third-Party Liability**

***Background:***

The U.S. Department of Health and Human Services provides funding to the Department of Health Services (DHS) for the Medical Assistance (MA) Program. Funding under the MA Program is used to assist states in maintaining and expanding health care services to certain categories of low-income persons. Services provided to participants include both inpatient and outpatient services that providers bill on a fee-for-service basis. Providers submit claims for services for eligible participants in the MA Program through the Medicaid Management Information System (MMIS), which is administered by the MA Program's fiscal agent. DHS works with the fiscal agent to ensure that the MMIS system is correctly processing claims, changes to the system are approved, and an audit of system controls related to claims is completed annually.

***Criteria:***

Under 42 CFR ss. 433.135 through 433.154, DHS is required to make reasonable efforts to determine the legal liability of third-party insurers for MA Program participants and have processes in place to identify and assess claims to determine if a third-party may be responsible for payment. For example, certain MA Program participants are also eligible for Medicare. If the services provided to a participant could be paid by Medicare, or any other third-party insurer, the claims should first be submitted to the third-party insurer by the provider before the claims are submitted to the MA Program.

To assess the validity of a claim prior to paying a provider the approved fee-for-service rate, DHS has established validity checks within MMIS called edits. These edits include cost avoidance rules, which are a series of rules within MMIS that identify claims meeting specific criteria related to whether a third-party insurer, including Medicare, could be responsible for payment of the services provided. These rules use claim information, including participant information and type of service, to determine if a third-party insurer may be responsible for payment. If the claim meets the criteria identified in these rules, the provider claim is denied. For claims that are denied through the cost avoidance rules, the MA Program may subsequently pay some claims if the third-party insurer ultimately does not cover the services provided to the participant.

***Condition:***

We found one MA Program payment of \$1,956 for outpatient services that was not properly identified and denied under the cost avoidance rules in MMIS. Based upon the outpatient services of this claim, the payment should have been denied because the participant was enrolled in Medicare at the time the service was provided, and Medicare may have been responsible for payment of the service.

***Context:***

During fiscal year (FY) 2021-22, based upon MA Program payment information provided by DHS, a total of \$5.2 billion was paid to providers for fee-for-service claims. During FY 2021-22, there were \$324.5 million in MA Program payments for 586,522 claims for outpatient services. Of the

40 fee-for-service claims we reviewed, seven claims were for outpatient services that had payments totaling \$6,445.

***Questioned Costs:***

For the \$1,956 payment we identified, we question \$1,293 as the estimated federal share. We also question an undetermined amount for other claims DHS paid using MA Program funding during FY 2021-22 for participants also enrolled in Medicare.

***Effect:***

DHS inappropriately used MA Program funding to make a payment for an outpatient claim that may be covered by Medicare, resulting in an improper payment under the MA Program. Further, because the cost avoidance rules are applied to all claims, it is likely there are additional claims for services provided to participants who are also enrolled in Medicare that were improperly paid.

***Cause:***

The improper payment we identified occurred because the cost avoidance rules were not correctly established to deny this type of claim for a participant who was also enrolled in Medicare. According to DHS staff, in 2015 DHS reviewed cost avoidance rules in MMIS related to Medicare in an effort to simplify and clarify the rules. In making and testing changes to these rules, DHS did not identify errors in claims meeting criteria similar to the one selected for testing as a part of our audit. DHS indicated that no further testing specific to these rules was performed after these cost avoidance rules were tested and implemented in 2015.

**Recommendation**

---

*We recommend the Wisconsin Department of Health Services:*

- *review and update the Medicaid Management Information System cost avoidance rules to properly identify and deny payment for claims that may be covered by third-party insurers;*
- *identify payments made during FY 2021-22 that may have been improper due to inaccurate cost avoidance rules and seek to recover these amounts;*
- *return to the federal government recovered payments that may have been improper; and*
- *perform an assessment and implement additional procedures to review changes to cost avoidance rules in the future.*

**Type of Finding:** Significant Deficiency

**Response from the Wisconsin Department of Health Services:** The Wisconsin Department of Health Services agrees with the audit finding and recommendations.

## **Finding 2022-002: Department of Administration/Division of Enterprise Technology Information Security Access Review Process**

### ***Background:***

Under s. 16.971 (2), Wis. Stats., the Department of Administration (DOA) is responsible for the State's information technology (IT) services, including ensuring that all state data processing facilities develop proper privacy and security procedures and safeguards. As a part of DOA, the Division of Enterprise Technology (DET) operates data centers to provide a variety of services to state agencies, including managing the mainframe for all agencies; managing servers for DOA and other executive branch agencies; and maintaining DOA-related systems. In addition, DET performs programming and security functions, including maintaining the infrastructure for STAR, which is the State's enterprise resource planning system that includes accounting, payroll, and purchasing systems used by most state agencies.

We have reported access review concerns related to DET accounts since our FY 2015-16 audit and have made recommendations to DET to review and update access and retain documentation of such reviews. Although DET established a policy and standard regarding access reviews, it did not complete access reviews in accordance with the policy and standards for all hardware and software maintained by DET.

### ***Criteria:***

The Wisconsin Access Control Standard states that the privileges assigned to roles or classes of users must be reviewed annually to validate the need for such privileges. Further, the Standard states that access to privileged accounts must be reviewed at least every six months to determine whether the account is still required and access remains appropriate.

An effective access review process contains the following key elements:

- identification of all active user accounts, both standard and privileged, that should be reviewed;
- a timeline to review identified user accounts within appropriate time frames;
- approval of each user account's access by entity staff at an appropriate level within the entity that understands the user's access requirements; and
- a process to validate that access changes resulting from the review were completed.

In addition, it is important that access review documentation is maintained and that responsibilities for the access review process are communicated to the appropriate entity staff.

### ***Condition:***

During FY 2021-22, DET did not complete access reviews in accordance with the policy and standards for all DOA and DOA-managed user accounts. In addition, DET has not completed access reviews in some areas since we first made a recommendation as part of our FY 2015-16 audit.

### ***Context:***

We reviewed the State of Wisconsin *IT Security Policy Handbook* and related standards and made inquiries of senior management to gain an understanding of the process for reviewing access and to assess progress DET made in addressing our FY 2021-22 recommendations.

As noted, the areas of insufficient access reviews are pervasive across several different types of accounts. Further, these accounts have access to various hardware and software located in the DET data centers, which could affect all executive branch agencies.

***Questioned Costs:***

None.

***Effect:***

Access reviews are important to ensure access remains appropriate based on user responsibilities and the principle of least privilege. Because DET hosts and supports a significant number of executive branch agency systems at its data centers, users with inappropriate access have the ability to affect the computing resources and data of all state agencies with resources connected to the DET network.

***Cause:***

DET indicated that steps were taken in FY 2021-22 to attempt to complete user access reviews. However, DET indicated it was unable to develop clear and reproducible access reports that could be used for a regular access review process. DET indicated that in August 2022, it purchased an access management tool to automate the user access reviews and is developing plans to implement the tool in FY 2022-23. Although automating the access review process could be beneficial, this access management tool cannot be applied to all access types applicable to the DET network environment.

**Recommendation**

---

*We recommend the Wisconsin Department of Administration, Division of Enterprise Technology develop and complete a process by June 30, 2023, to perform access reviews in accordance with the State of Wisconsin IT Security Policy Handbook, including updating access based on the review and retaining documentation of the review and the updates made to access.*

**Type of Finding:** Significant Deficiency

**Response from Wisconsin Department of Administration, Division of Enterprise Technology:** The Wisconsin Department of Administration agrees with the audit finding and recommendation.



## **Finding 2022-003: Department of Administration/Division of Enterprise Technology Information Security Policy Exception Process**

### ***Background:***

Under s. 16.971(2), Wis. Stats., DOA is responsible for the State's IT services, including ensuring that all state data processing facilities develop proper privacy and security procedures and safeguards. Further, statutes require DOA to provide oversight and monitoring of state agency IT operations. As a part of DOA, DET operates data centers to provide a variety of services to state agencies, including managing the mainframe for all agencies; managing servers for DOA and other executive branch agencies; and maintaining DOA-related systems.

DOA implemented the State of Wisconsin *IT Security Policy Handbook*, which includes policies for IT security and the related standards. Executive branch agencies are expected to comply with these policies and standards, or obtain an approved exception to a policy or standard if compliance cannot be achieved. An exception is a known deviation from policies in the State of Wisconsin *IT Security Policy Handbook* and related standards. For example, DOA may approve an exception to allow an agency to deviate from an established IT security policy, such as a password policy.

We reported concerns with the process for requesting an exception during our FY 2018-19 audit and made recommendations to DET to improve its process. During our FY 2020-21 audit, we again made recommendations to DET to improve its exception process. However, DET did not make sufficient progress in addressing our recommendations in this area.

### ***Criteria:***

The compliance section of the State of Wisconsin *IT Security Policy Handbook* and related standards states that if compliance with particular policies or related standards is not feasible or technically possible, or if a deviation from a policy or standard is justifiable to support a business function, executive branch agencies can request an exception through the exception procedures established by the DOA/DET Bureau of Security. Further, the Security Policy and Standards Review and Maintenance section of the State of Wisconsin *IT Security Policy Handbook* and related standards states that the DOA/DET Bureau of Security is responsible for coordinating the review and tracking of exception requests to the IT security policies and standards.

An effective exception process contains the following key elements:

- identification of situations where established processes or configurations do not comply with established policies;
- a process to report exceptions to these policies by entity staff at an appropriate level within the entity;
- an assessment of the exception requested that considers risks to the entity of authorizing the exception and potential compensating controls that could be implemented;
- approval of exceptions at an appropriate level within the entity that understands the policies and risks; and
- regular review of approved exceptions, such as annually, to ensure risks remain acceptable and to consider if changes can be made to alleviate the need for an exception.

In addition, it is important that documentation of exception requests and approvals be maintained and that the responsibilities for the exception process are appropriately communicated.

**Condition:**

In response to recommendations from our FY 2020-21 audit, DET indicated it would review its new dashboard that identifies exceptions to the State of Wisconsin *IT Security Policy Handbook*, as self-reported by executive branch agencies. DET also indicated it would work with executive branch agencies to ensure any exceptions identified in this review were drafted and approved by September 30, 2022. However, as of June 30, 2022, DET completed a preliminary analysis of the dashboard, identified instances of noncompliance, and indicated that meetings were held to assist agencies in becoming compliant with the policies. However, DET did not provide sufficient documentation to support that these meetings were held, the discussions that occurred, and the steps that agencies were taking to become compliant. Further, there were no new exceptions drafted, even though agencies were not following all policies, standards, and procedures in the State of Wisconsin *IT Security Policy Handbook*. We followed up with DET in October 2022, and found that executive branch agencies were asked to draft exceptions and provide them to DET by November 30, 2022.

In response to recommendations from our FY 2020-21 audit, DET had indicated that by March 30, 2022, it would perform an assessment of current exceptions, identify the risks related to approving the exceptions, and consider potential compensating controls. In completing testing during our FY 2021-22 audit, we found DET remediated 2 of 13 policy exceptions we identified during our FY 2020-21 audit and prepared draft exceptions for 3 others.

DET also had indicated that it would review approved exceptions on a quarterly basis to assess if the approval of the exception should continue. Although DET provided a spreadsheet that indicated that it was tracking some exceptions, the documentation did not include evidence that DET consistently communicated with the agency regarding the continued need for the exception or an assessment of the risks related to the exception. For example, in December 2021 DET requested an agency provide additional information regarding an exception. However, DET did not provide a due date for its request. As of October 2022, there was no response from the agency, or documentation that DET had followed up with the agency on its request.

Finally, DET indicated it would review its exceptions procedure and forms, make revisions to ensure exceptions are properly submitted and approved, and communicate relevant procedures and responsibilities to DET and executive branch agencies by March 30, 2022. DET did not complete a review or make updates to its exceptions procedure and forms by March 30, 2022, or before the end of FY 2021-22.

**Context:**

We reviewed the State of Wisconsin *IT Security Policy Handbook* and related standards, made inquiries of DET staff, reviewed approved exceptions, and evaluated the design of the existing exception process.

We evaluated the new dashboard for agency compliance with the State of Wisconsin *IT Security Policy Handbook* and related standards. We compared the dashboard results against the spreadsheet of approved and in progress exceptions. We identified concerns with the exception process across nine policy areas in the State of Wisconsin *IT Security Policy Handbook* and related standards.

Most state agencies use computer systems that are located on the mainframe or on servers maintained in the DET data centers. Therefore, IT weaknesses at one agency can affect IT security for other agencies.

**Questioned Costs:**

None.

**Effect:**

Without a strong information security policy exception process in place, DET does not have an appropriate awareness of areas where policies are not being followed. As a result, weaknesses in the overall security in the state network may not be identified or corrected.

In our review of compliance with nine policies and standards in the State of Wisconsin *IT Security Policy Handbook* and related standards, as reported in the Policy Standards and Procedures dashboard by four executive branch agencies, we identified 34 areas of noncompliance or partial noncompliance with the policies and standards for which there was not an approved exception.

**Cause:**

DET did not have adequate procedures in place for administering the exceptions process and did not develop an efficient training process to address agency staff turnover. Documentation provided by DET indicated that DET did not communicate regularly with executive branch agencies regarding the status of exceptions, establish timelines for agency responses to DET's inquiries, or escalate to senior management when an agency was not responding to DET's inquiries. In addition, DET did not have procedures for escalating executive branch agency noncompliance with the State of Wisconsin *IT Security Policy Handbook* and related standards, to senior management within the particular agency and within DOA.

DET staff indicated that other priorities, including resolving questions and issues arising from other third-party audits of DET, were assessed as higher priority than addressing the recommendations in this area.

**☑ Recommendation**

---

*We recommend the Wisconsin Department of Administration, Division of Enterprise Technology:*

- *complete by January 31, 2023, a review of its existing IT security exception process and make revisions to the process, including developing a procedure for escalating noncompliance with established policies to senior management within the Department of Administration and within the particular executive branch agency;*
- *develop an exception process training program and communicate the relevant training program and exception process procedures and responsibilities to its staff and executive branch agency staff by January 31, 2023; and*
- *complete and document its review and assessment of processes and configurations that do not comply with established policies, complete approvals of exceptions when changes to processes cannot be made timely, maintain documentation of discussions and meetings with agency staff as the review and assessment of exceptions are completed, and complete this review and approval of exceptions by March 31, 2023.*

**Type of Finding:** Significant Deficiency

**Response from the Wisconsin Department of Administration, Division of Enterprise Technology:**

The Wisconsin Department of Administration agrees with the audit finding and recommendations.

## **Finding 2022-004: Department of Administration Information Technology Oversight and Monitoring Responsibilities\***

### ***Background:***

DOA is responsible for the State's IT services, including providing oversight and monitoring of executive branch agency IT operations. We first recommended that DOA develop and implement executive branch agency IT policies and standards and provide oversight and monitoring of executive branch agencies' IT operations seven years ago during our FY 2014-15 audit. During subsequent audits, we recommended that DOA take steps to identify, assess, and address risks for the State's IT environment. These steps were to include completion of a comprehensive risk management program across all executive branch agencies. DOA has taken steps including:

- implementing in FY 2018-19 the State of Wisconsin *IT Security Policy Handbook*, which includes policies for IT security and the related standards with which executive branch agencies are expected to comply;
- developing in FY 2019-20 a risk assessment plan, which contained a plan for improving vulnerability management and completing penetration testing;
- initiating efforts in FY 2020-21 to develop a baseline understanding of agency compliance, with the State of Wisconsin *IT Security Policy Handbook* and related standards; and
- implementing and configuring in FY 2021-22 a new vulnerability management tool.

During our FY 2020-21 audit (report 21-23), we found that DOA did not collect needed information from all executive branch agencies, and DOA did not establish a plan for other important monitoring steps, such as analyzing the effectiveness of the procedures established by executive branch agencies. At that time, we recommended that DOA improve its monitoring program, perform ongoing vulnerability assessments, and update its risk assessment program.

### ***Criteria:***

Wisconsin Statutes give DOA responsibility for the State's IT services. Under s.16.971 (2), Wis. Stats., DOA is required to work with executive branch agencies to establish IT policies, procedures, and planning processes. In addition, statutes require DOA to monitor adherence to these policies, procedures, and processes. Further, statutes require DOA to provide oversight and monitoring of executive branch agency IT operations, which includes ensuring:

- management reviews of IT organizations are conducted;
- all executive branch agencies develop and operate with clear guidelines and standards in the areas of IT systems development and employ good management practices and cost-benefit justifications; and
- all state data-processing facilities develop proper privacy and security procedures and safeguards.

Finally, s. 16.973 (3), Wis. Stats., states that DOA shall facilitate the implementation of statewide initiatives, including the development and maintenance of policies and programs to protect the privacy of individuals who are the subjects of information contained in the agency databases.

National Institute of Standards and Technology (NIST) 800-137 *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* indicates that ongoing monitoring is a critical part of an organization's risk management process. In addition, an organization's overall IT security architecture and accompanying security program should be monitored to ensure that organization-wide operations remain within an acceptable level of risk despite any changes that occur. Key steps in effective monitoring include:

- developing and communicating the policies, procedures, and standards that form the security framework;
- collecting information on the effectiveness of the policies, standards, and procedures;
- analyzing the information collected;
- responding to the results of the analyses; and
- reviewing and updating the monitoring program.

**Condition:**

During our FY 2021-22 audit, we found again that DOA did not have sufficient oversight and monitoring in place to ensure executive branch agency adherence to the State of Wisconsin *IT Security Policy Handbook* and related standards. DOA completed and published a baseline dashboard of agency compliance with the *IT Security Policy Handbook* and related standards, based on information self-reported by executive branch agencies. DOA completed a preliminary analysis of the dashboard, identified instances of noncompliance, and indicated that meetings were held to assist agencies in becoming compliant with the policies. However, DOA did not provide sufficient documentation to support that these meetings were held, the discussions that occurred, and the steps that agencies were taking to become compliant. We include recommendations in Finding 2022-003 for DOA to improve its information security policy exception process that will help address these concerns.

Given its statutory responsibilities, it would be expected that DOA would review agency procedures to assess the accuracy of the self-reported information, and the effectiveness of the procedures established by the executive branch agencies. However, DOA did not take sufficient steps to assess the accuracy of the agency-reported information. DOA indicated that it performed some reviews of agency procedures to assess compliance with the IT policies. However, DOA did not provide documentation to support that these reviews were completed, and DOA indicated it had no plans to conduct additional reviews. In our review of agency compliance with the State of Wisconsin *IT Security Policy Handbook* and related standards, we found that certain controls reported by four agencies in the dashboard as being compliant were not compliant based on our audit work. For example, two agencies assessed their personnel termination status as implemented. However, the agencies' timelines to disable access exceeded the timeline listed in the standard. Another agency assessed its business continuity plan test as implemented. However, upon discussion with the agency, the planned test was canceled due to lack of staff availability.

During FY 2021-22, DOA worked with executive branch agencies to implement a new vulnerability management tool. As of June 30, 2022, 14 of 19 agencies had implemented the new tool. However, a licensure issue resulted in changes to how DOA planned to use the vulnerability tool, at least in the short term. As a result, DOA did not establish plans for how ongoing vulnerability assessments would be performed, or how DOA would respond to those assessments and make changes to the State's IT environment.

Finally, due to the implementation issues with the new vulnerability tool, DOA did not make further progress in the development of its risk assessment plan. In addition, DOA did not update its risk assessment plan to include consideration of the risks related to known deviations from policies in the State of Wisconsin *IT Security Policy Handbook* and related standards. For example, DOA may approve an exception to allow an agency to deviate from an established IT security policy, such as a password policy. Although deviations from the policies have been approved, the deviations may bring additional risk that DOA should consider in its oversight and monitoring of the State's IT environment. In Finding 2022-003, we make recommendations for DOA to improve the information security policy exception process.

***Context:***

State agencies rely on computer systems to complete critical functions, including processing checks, accounting for cash receipts, preparing financial statements, and administering federal grant programs. DOA is responsible for ensuring these computer systems are properly secured. We interviewed key DOA staff to gain an understanding of the steps that were taken by June 30, 2022, to provide oversight and monitoring of executive branch agency IT operations and adherence to the State of Wisconsin *IT Security Policy Handbook* and related standards. We also interviewed key DOA staff to gain an understanding of DOA's plans for utilizing the new enterprise vulnerability management tool to identify vulnerabilities with security patch, configuration, and regulatory compliance issues. We evaluated the baseline dashboard of executive branch agency compliance with the State of Wisconsin *IT Security Policy Handbook* and related standards. We compared the dashboard results against our review of agency compliance with certain IT policies and standards for four executive branch agencies.

Because DOA has responsibility to provide oversight and monitoring over IT operations for executive branch agencies, and because there are connections among agencies in the State's network, IT weaknesses at one agency can affect IT security for other agencies.

***Questioned Costs:***

None.

***Effect:***

For FY 2021-22, DOA did not comply with s.16.971 (2), Wis. Stats., which requires DOA to provide oversight and monitoring of executive branch agency IT operations and adherence to the State of Wisconsin *IT Security Policy Handbook* and related standards. Insufficient monitoring of agency IT environments can lead to vulnerabilities in the State's network, known or unknown, because there is no assurance that all systems are meeting the minimum level of security for the State's IT environment, as established in the State of Wisconsin *IT Security Policy Handbook* and related standards. Weaknesses in the security of the network can lead to inappropriate access to confidential or sensitive data, unauthorized changes to the data within the system, or a failure of the system.

***Cause:***

DOA indicated that executive branch agencies were not always responsive to requests to discuss noncompliance with the State of Wisconsin *IT Security Policy Handbook* and related standards, and the steps needed to address the noncompliance. However, DOA did not have procedures to assist its staff in understanding when and how to escalate to senior management within the particular agency and within DOA when agencies were not responsive.

DOA did not establish a monitoring process to analyze the accuracy of the agency-reported information or to assess the effectiveness of executive branch agency controls. DOA should develop a plan for the review of agency procedures. This plan could include different levels of review based

on an assessment of risk to the State's IT environment and could be cycled to smooth the effort over a period of time.

Finally, DOA indicated that it encountered licensure issues in implementing the new vulnerability management tool, which delayed its comprehensive use of the tool for ongoing monitoring and precluded additional updates to its risk assessment program.

#### ☑ Recommendation

---

*We recommend the Wisconsin Department of Administration, Division of Enterprise Technology comply with its statutory responsibilities to provide oversight and monitoring of executive branch agency adherence to the State's IT policies by:*

- *using its statutory authority to ensure executive branch agencies conform with the State's IT policies and standards or obtain an approved exception by March 31, 2023;*
- *developing and communicating to executive branch agencies by March 31, 2023, a monitoring plan to review the effectiveness of agency-reported information in the dashboard, including how the Department of Administration will report results to the agency and expected timelines for agencies to correct the noncompliance with the State's IT policies and standards or obtain an approved exception;*
- *establishing detailed plans by June 30, 2023, for how it will perform ongoing vulnerability assessments with the new vulnerability management tool, respond to those assessments, and make changes to further strengthen the State's IT environment; and*
- *continuing to update its risk management program including considering the risks related to approved policy exceptions and remediating known vulnerabilities.*

**Type of Finding:** Significant Deficiency

**Response from the Wisconsin Department of Administration, Division of Enterprise Technology:**

The Wisconsin Department of Administration agrees with the audit finding and recommendations.

## Finding 2022-005: Financial Reporting for the Medical Assistance Program

### **Background:**

The financial activity of programs administered by DHS, which includes the MA Program, is reported as part of the State's General Fund in the State's ACFR. The MA Program provides health care services to certain categories of low-income persons. The MA Program is significant to the General Fund and, as a result, consideration of the activity of this program and changes in the program are critical to accurate financial reporting.

In FY 2021-22, DHS claimed additional federal funds for the MA Program, as allowed by Section 9817 of the American Rescue Plan Act of 2021. The claim amount was calculated based upon an increase in the federal medical assistance percentage (FMAP) rate by 10 percent for certain home and community-based services provided to participants during the period April 1, 2021, through March 31, 2022. To claim the increased FMAP rate, DHS made several adjustments primarily related to the allowable portion of monthly capitation payments. These adjustments resulted in the receipt of federal funds totaling \$329.2 million during FY 2021-22. Further, an additional \$75.5 million was received in FY 2022-23 that related primarily to certain services provided to participants on a fee-for-service basis during the period from April 1, 2021, through March 31, 2022.

Federal regulations require the funds derived from the increased FMAP to be reinvested in the MA Program to implement or supplement home and community-based services to participants. DHS is required to return to the federal government any remaining amount that is unexpended as of March 31, 2025. During FY 2021-22, DHS had reinvested \$50.6 million of these funds.

### **Criteria:**

For use in preparing the financial statements of the State's General Fund as reported in the ACFR, DHS is responsible for preparing adjustments in accordance with Governmental Accounting Standards Board (GASB) standards and submitting this information to the Department of Administration State Controller's Office (DOA-SCO). The *Uniform GAAP Conversion Policies and Procedures Manual*, which is published by DOA-SCO, provides guidance to state agencies in preparing adjustments. Using the requirements of the accounting standards promulgated by GASB, Section V-18 of the manual includes requirements related to the appropriate reporting of amounts received related to a federal grant program.

### **Condition:**

DHS did not consider whether the additional funds derived from the increased FMAP required an adjustment to properly report the activity in the General Fund financial statements. At our request, DHS reviewed the process used to claim and receive these funds as well as the federal requirements related to the use of these funds. From this analysis, DHS concluded that the \$75.5 million in federal funds it received in FY 2022-23 should have been accrued both as a receivable and as a federal revenue for FY 2021-22. In addition, because the federal government required the funds to be reinvested in certain MA Program services, the unspent balance of \$278.6 million as of June 30, 2022, as well as the \$75.5 million received in FY 2022-23, should have been reported as a restriction of the General Fund's fund balance in the financial statements.

### **Context:**

We interviewed DHS staff to gain an understanding of the federal requirements related to the receipt of the funds derived from the increased FMAP and reviewed the federal regulations related to the future use of these amounts. We also reviewed claim adjustments processed throughout FY 2021-22 and adjustments subsequent to the end of FY 2021-22 to verify activity related to the funds.



**Questioned Costs:**

None.

**Effect:**

The Intergovernmental Revenue account on the Statement of Revenues, Expenditures, and Changes in Fund Balance and Due from Other Government account on the Balance Sheet were understated by \$75.5 million for the General Fund. In addition, Fund Balance—Restricted was understated by \$354.1 million and Fund Balance—Unrestricted was overstated by \$354.1 in the General Fund Balance Sheet.

**Cause:**

DHS staff responsible for financial reporting discussed MA Program activity with staff responsible for accounting and monitoring the MA Program to identify potential adjustments that may have been needed to the FY 2021-22 General Fund financial statements. These discussions were not sufficient to identify the need for an adjustment related to the receipt and future use of the funds derived from the increased FMAP.

 **Recommendation**

---

*We recommend the Wisconsin Department of Health Services:*

- *develop and implement additional procedures to evaluate the potential effects of changes in the programs that it administers; and*
- *use the additional procedures to evaluate changes that may require further consideration and adjustments for financial reporting purposes.*

**Type of Finding:** Significant Deficiency

**Response from the Wisconsin Department of Health Services:** The Wisconsin Department of Health Services agrees with the audit finding and recommendations.

## **Finding 2022-006: Common School Fund—Service Organization Internal Controls**

### ***Background:***

The Board of Commissioners of Public Lands (BCPL) administers the Common School Fund, which accounts for proceeds from the sale of land granted by the federal government to Wisconsin when it became a state. The state Constitution established that the proceeds from the sale of the public lands be invested and held in perpetuity in the Fund, and the investment income be distributed as library aids to school districts.

2015 Wisconsin Act 60 expanded BCPL's investment authority, which allowed it to consider a broader array of investments for the Common School Fund assets. Prior to this time, the Common School Fund assets were limited to investments in certain municipal bonds and notes. Since that time, BCPL has expanded its investments to include equities and limited partnerships.

### ***Criteria:***

Management is responsible for the proper design, implementation, and maintenance of internal controls relevant to the preparation and fair presentation of financial information that is free from material misstatement. This includes instances in which management contracts with a service organization, which is an organization that provides services to another entity and those services are relevant to the entity's internal controls over financial reporting. For example, an entity may use a service organization to process financial transactions or an entity may outsource some of its accounting functions to a service organization.

When using a service organization, the entity should gain assurances that the internal controls at the service organization are operating effectively because weaknesses in the service organization's internal controls could affect the financial activity of the entity. Such assurances could be gained through a service organization audit, which includes a report on the service organization's internal controls by an independent auditor. One type of audit that may be completed includes an opinion on the fairness of management's description of the internal controls in place at the service organization, whether the auditor believes the service organization's internal controls are suitably designed to achieve the internal control objective, and whether the service organization's internal controls are effective at achieving the internal control objective.

If an entity relying on a service organization does not obtain a service organization audit report, the entity should ensure it has assessed the work being completed by the service organization, and has implemented procedures to ensure the accuracy of processing completed by the service organization and of the information provided by the service organization.

### ***Condition:***

BCPL maintains a service agreement with a custodian bank, which is responsible for conducting purchases and sales of investments as authorized by BCPL. The custodian bank makes wire transfers for capital calls for limited partnership investments, collects income, and keeps cash and investment holdings for the Common School Fund. BCPL also relies on accounting and investment reports prepared by the custodian bank, including reporting the fair value of investments to BCPL, which are used for financial reporting. The custodian bank performs certain services for BCPL that classify it as a service organization.

Although BCPL relies on the custodian bank, it did not document its assessment of its reliance on the custodian bank, it did not obtain a service organization audit report from its custodian bank, nor did it perform other procedures sufficient to reduce risk. For example, BCPL could request its custodian bank to provide a SOC 1, Type 2 service organization audit report, which would provide an independent auditor's opinion on the design and effectiveness of the custodian bank's internal

controls that are important to BCPL's financial reporting. BCPL could also assess the reliance placed on its custodian bank and reduce its risks by performing other procedures, such as reviewing the investment valuation provided by its custodian bank to provide assurance of its accuracy.

**Context:**

We reviewed BCPL's investment records for the Common School Fund and discussed its investment procedures, including the services provided by its custodian bank. When we inquired about the internal controls related to the custodian bank, we learned that BCPL did not obtain a service organization audit report from its custodian bank. The Common School Fund investment assets have increased from \$496.4 million as of June 30, 2015, to \$981.1 million as of June 30, 2022, an increase of \$484.7 million, or 97.6 percent.

**Questioned Costs:**

None.

**Effect:**

The custodian bank may have internal control deficiencies about which BCPL is unaware that could affect the investments or financial reporting for the Common School Fund.

**Cause:**

BCPL staff indicated that the custodian bank would provide a service organization audit report. However, BCPL staff did not know which specific internal controls at the custodian bank were important and, therefore, needed to be tested by a service organization auditor.

Because a service organization audit report provides an opinion on whether internal controls of the service organization are operating effectively, BCPL could obtain a service organization audit report as an additional tool to assess whether its custodian bank has effective internal controls in place and to assess whether any identified deficiencies should be further discussed and addressed with respect to BCPL transactions and holdings. In addition, BCPL could use the service organization audit report to assess whether appropriate and sufficient internal controls are in place at BCPL to complement the internal controls at the custodian bank.

**Recommendation**

---

*We recommend the Wisconsin Board of Commissioners of Public Lands:*

- *complete and document an assessment of its reliance on its custodian bank; and*
- *determine and implement internal controls as appropriate to ensure the accuracy of information it receives from the custodian bank; or*
- *obtain a service organization audit report from its custodian bank, assess and document its review of the effectiveness of the custodian bank's internal controls as reported in the service organization audit report, and assess and document its review of the service organization audit report to ensure appropriate and sufficient internal controls are present at the Board of Commissioners of Public Lands to complement the internal controls at the custodian bank.*

**Type of Finding:** Significant Deficiency

**Response from the Board of Commissioners of Public Lands:** The Wisconsin Board of Commissioners of Public Lands agrees with the audit finding and recommendations.

## **Finding 2022-007: UW System Information Technology Internal Control Deficiencies**

### ***Background:***

In April 2021, the University of Wisconsin (UW) System implemented ShopUW+ (SUW) as a new procure-to-pay procurement system that integrates approval of purchases among all 13 UW institutions. Similar to other systemwide applications, UW System Administration was responsible for administering SUW, including developing systemwide policies and ensuring adequate internal controls. SUW is a cloud-based system, and some SUW activities are integrated with UW System's accounting system, the Shared Financial System (SFS). For example, SUW system roles responsible for providing approvals on UW purchases are authorized by designated individuals at each UW institution. Certain other roles are provisioned through a formal process within SFS. The process to provide SUW approval access, and subsequently monitor this access, was different than with SFS.

### ***Criteria:***

Under s. 36.09 (1), Wis. Stats., the Board of Regents is vested with the primary responsibility for the governance of UW System. In discharging this responsibility, compliance with local, state, and federal regulations is necessary to protect institutional and research data. *UW System Administrative Procedure 1031.B Information Security: Data Protections* requires that information technology systems follow operating system-specific best practices for system management and security. Such best practices include limiting access to those individuals who need access to complete properly separated job duties and periodically reviewing the access provided to ensure it remains appropriate.

According to the National Institute of Standards and Technology (NIST) Cybersecurity Framework and NIST 800-53 Release 5, when an entity uses a cloud-based third-party to process financial transactions or it outsources some of its information technology functions, the entity should consider whether assurances are needed to ensure the third-party internal controls are operating effectively. Weaknesses in the third-party's internal controls could affect the financial activity of the entity. These assurances are typically provided through a service organization audit report, which is a report on the service organization's internal controls by an independent auditor.

A service organization audit report is intended to meet the needs of management of user entities, such as UW System Administration, and user entities' auditors. One type of audit that may be completed includes an opinion on the fairness of management's description of the internal controls in place at a service organization, whether the auditor believes those controls are suitably designed to achieve the internal control objective, and whether the internal controls are effective at achieving the control objective.

### ***Condition:***

We identified two concerns with the internal controls over SUW. First, we found that UW System Administration had not formally documented that UW institutions should periodically review approval access authorized within the SUW application. We also note that these approval roles within SUW were not included in the SFS access review process conducted by UW institutions. UW System Administration provides weekly reports of employee job changes to assist UW institutions in monitoring SUW approval access. Although UW System Administration staff indicated that certain UW institution staff were responsible for conducting a review of this report to monitor SUW-authorized access, there was no established procedure nor any systemwide monitoring to ensure that each UW institution completed such a review. We contacted four UW institutions and only one UW institution identified the weekly job change report provided by UW System Administration as part of their process to review SUW approval access.

Second, UW System Administration did not obtain a service organization audit report from its third-party SUW vendor during FY 2021-22 to provide assurances that the vendor had appropriate internal controls in place and that they were operating effectively. Because UW System Administration did not obtain the annual service organization audit report, it also did not consider the adequacy of certain activities that UW System should have in place to ensure reliance on the third-party vendor's internal controls, such as reviewing SUW access authorized by UW institutions.

***Context:***

We reviewed the SFS and SUW systems, which include internal controls over certain UW institution expenses reported in the FY 2021-22 financial statements and certain federal grant programs. During FY 2021-22, UW System approved \$1.3 billion in payments through access authorized within SUW. We also assessed established UW systemwide policies requiring adequate internal controls and procedures to ensure that each UW institution complied with these policies. In addition, we reviewed a UW System Office of Internal Audit report on certain SUW internal controls that was completed in March 2022. We further discussed the SFS and SUW access review process with UW System Administration and certain UW institutions. We performed transaction testing to review a sample of payments, including those approved through SUW, to ensure the transactions were appropriately approved. We discussed management of service organization audit reports with UW System Administration staff.

***Questioned Costs:***

None.

***Effect:***

Access reviews are important to ensure access remains appropriate based on user responsibilities and the principle of least privilege. Failure to monitor access can lead to inappropriate access to sensitive data or inappropriate transaction approvals. Although it can be difficult to determine how information security concerns affect the financial statements and material compliance areas, ineffective information security controls may permit controls over individual systems to operate improperly and may allow financial statement misstatements and noncompliance to occur and not be detected.

***Cause:***

UW System Administration had emphasized with UW institutions that each UW institution was responsible for granting appropriate access for SUW approvers. However, UW System Administration had not communicated in writing the responsibility of UW institutions to conduct periodic access reviews for SUW approval roles nor did UW System Administration include SUW approval roles in the SFS access review process due to the large number of approvers. UW System Administration is currently working on the Administrative Transformation Program (ATP), which will replace certain systemwide information technology applications, and it currently plans to retain SUW when the ATP project is completed. Therefore, UW System Administration should take further steps to clarify and monitor UW institution review requirements for SUW approval access.

UW System Administration performed a risk assessment in 2019 prior to contracting with the cloud-based third-party vendor to assess the vendor's internal controls, including security provisions. In addition, UW System's contract with the cloud-based third-party vendor provides for a service organization audit report. However, no UW System Administration staff were assigned the responsibility or requirement to annually obtain and review such a report. As the application owner, UW System Administration should obtain and review a service organization audit report at least annually. Because UW System's current ATP project is planning to rely on additional cloud-based third-party vendors to administer aspects of these new systemwide applications, it is important for

UW System Administration to establish systemwide policies to adequately monitor cloud-based third-party vendor internal controls.

**Recommendation**

---

*We recommend the University of Wisconsin System Administration improve its oversight of the ShopUW+ application by:*

- *developing a written requirement for University of Wisconsin institutions to periodically review ShopUW+ approval access and communicating this requirement to all University of Wisconsin institutions;*
- *developing a procedure to monitor the compliance of all University of Wisconsin institutions with the requirement for periodic review of ShopUW+ approval access;*
- *developing a policy to require periodic review of the adequacy of certain cloud-based third-party vendors' internal controls, such as by assigning the responsibility to obtain a service organization audit report and ensuring such reports are reviewed; and*
- *annually obtaining and reviewing relevant service organization audit reports.*

**Type of Finding:** Significant Deficiency

**Response from the University of Wisconsin System Administration:** The University of Wisconsin System Administration agrees with the audit finding and recommendations.

■ ■ ■ ■

---

## **Corrective Action Plans**

---



State of Wisconsin  
**Department of Health Services**

Tony Evers, Governor  
 Karen E. Timberlake, Secretary

DATE: November 16, 2022

TO: Lisa Kasel, Assistant Financial Audit Director  
 Legislative Audit Bureau

FROM: Barry Kasten, Director  
 Bureau of Fiscal Services  
 Department of Health Services

SUBJECT: Corrective Action Plan – Medical Assistance Program Third-Party Liability

Department staff has reviewed the Legislative Audit Bureau's (LAB) interim audit memo for Finding 2022-001: Medical Assistance Program Third-Party Liability. This is the department's Corrective Action Plan.

**Recommendation (2022-001): Medical Assistance Program Third-Party Liability**

*We recommend the Wisconsin Department of Health Services:*

- Review and update the Medicaid Management Information System cost avoidance rules to properly identify and deny payment for claims that may be covered by third-party insurers.

**Wisconsin Department of Health Services Planned Corrective Action:**

DHS has completed an assessment of Medicaid Management Information System (MMIS) cost avoidance rules and will implement changes by December 31, 2022, necessary to properly identify and deny outpatient services when a participant is enrolled in Medicare or other third-party insurance at the time the service was provided.

*We recommend the Wisconsin Department of Health Services:*

- Identify payments made during FY 2021-22 that may have been improper due to inaccurate cost avoidance rules and seek to recover these amounts;
- Return to the federal government recovered payment that may have been improper; and



Memo to Lisa Kasel  
November 16, 2022  
Page 2

**Wisconsin Department of Health Services Planned Corrective Action:**

DHS will attempt to recover \$1,956 in improper payments for outpatient services not properly identified and denied under cost avoidance rules in MMIS by December 31, 2022, and return to the federal government the estimated federal share of \$1,293.

DHS will complete an assessment and identify paid claims by March 31, 2023, where cost avoidance rules were not appropriately applied for outpatient services when a participant was enrolled in Medicare or other third-party insurance with a date of service after July 1, 2021, and return to the federal government recovered payments that were improper.

*We recommend the Wisconsin Department of Health Services:*

- Perform an assessment and implement additional procedures to review changes to cost avoidance rules in the future.

**Wisconsin Department of Health Services Planned Corrective Action:**

DHS will implement processes and procedures by December 31, 2022, for conducting production validation on any configuration changes impacting cost avoidance rules.

**Anticipated Completion Date:** March 31, 2023

Person responsible for corrective action:

Nick Havens, Director  
Bureau of System Management, Division of Medicaid Services  
[Nicholas.Havens@dhs.wisconsin.gov](mailto:Nicholas.Havens@dhs.wisconsin.gov)





**STATE OF WISCONSIN**  
**DEPARTMENT OF ADMINISTRATION**

Tony Evers, Governor  
Kathy Blumenfeld, Secretary-designee  
Trina Zanow, Division Administrator

**Corrective Action Plan**

**Finding 2022-003:** Department of Administration/Division of Enterprise Technology Information Security Policy Exception Process

**Planned Corrective Action:**

<b>LAB Recommendation</b>	<b>DOA/DET Planned Corrective Action</b>	<b>Anticipated Completion Date</b>
Complete by January 31, 2023, a review of its existing IT security exception process and make revisions to the process, including developing a procedure for escalating noncompliance with established policies to senior management within the Department of Administration and within the particular executive branch agency.	DOA/DET will complete a review of its existing IT security exception process and revise the process. The revised process will include developing an escalation procedure for escalating noncompliance with established policies to senior management within the Department of Administration as well as the noncompliant executive branch agency.	January 31, 2023
Develop an exception process training program and communicate the relevant training program and exception process procedures and responsibilities to its staff and executive branch agency staff by January 31, 2023.	DOA/DET will develop an exception process training program and communicate the relevant training program and exception process, procedures and responsibilities to DOA/DET and executive branch agency staff.	January 31, 2023
Complete and document its review and assessment of processes and configurations that do not comply with established policies, complete approvals of exceptions when changes to processes cannot be made timely, maintain documentation of discussions and meetings with agency staff as the review and assessment of exceptions are completed, and complete this review and approval of exceptions by March 31, 2023.	DOA/DET will complete and document a review and assessment of processes and configurations that do not comply with established policies, complete approvals of exceptions when changes to processes cannot be made timely, maintain documentation of discussions and meetings with agency staff as the review and assessment of exceptions are completed, and complete this review and approval of exceptions.	March 31, 2023

Person responsible for corrective action:  
Alan Greenberg, CISO  
Division of Enterprise Technology  
Alan.Greenberg@wisconsin.gov



STATE OF WISCONSIN  
DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor  
Kathy Blumenfeld, Secretary-designee  
Trina Zanow, Division Administrator

Corrective Action Plan

**Finding 2022-004:** Department of Administration Information Technology Oversight and Monitoring Responsibilities

Planned Corrective Action:

LAB Recommendation	DOA Planned Corrective Action	Anticipated Completion Date
We recommend the Wisconsin Department of Administration, Division of Enterprise Technology comply with its statutory responsibilities to provide oversight and monitoring of executive branch agency adherence to the State’s IT policies by:	DOA/DET, provides direct support and monitoring to eleven executive branch agencies for compliance with multiple audits to meet federal regulatory requirements such as IRS Publication 1075, Criminal Justice Information Systems (CJIS), Centers for Medicare and Medicaid (CMS/HIPAA) and Social Security Administration (SSA).  DOA/DET will continue to comply with its statutory responsibilities to provide oversight and monitoring of executive branch agencies by implementing the below recommendations.	March 31, 2023
Using its statutory authority to ensure executive branch agencies conform with the State’s IT policies and standards or obtain an approved exception by March 31, 2023.	DOA/DET will work with executive branch agencies to ensure compliance with the State’s Executive Branch IT policies and standards or obtain an approved exception.	March 31, 2023
Developing and communicating to executive branch agencies by March 31, 2023, a monitoring plan to review the effectiveness of agency-reported information in the dashboard, including how the Department of Administration will report results to the agency and expected timelines for agencies to correct the noncompliance with the State’s IT policies and standards or obtain an approved exception.	DOA/DET will develop and communicate to executive branch agencies a monitoring plan to periodically review the effectiveness of agency-reported information in the IT Policies, Standards and Procedures (PSP) dashboard.  DOA/DET will report results to the agency and will outline expected timelines for agencies to correct the noncompliance with the State’s IT Executive Branch policies and standards or obtain an approved exception.	March 31, 2023  March 31, 2023

Establishing detailed plans by June 30, 2023, for how it will perform ongoing vulnerability assessments with the new vulnerability management tool, respond to those assessments, and make changes to further strengthen the State's IT environment.	DOA/DET will establish plans for performing ongoing vulnerability assessments with the new vulnerability management tool. The plan will include the process to review the vulnerability assessment results and subsequent changes made in the environment to further strengthen the State's IT security posture.	June 30, 2023
Continuing to update its risk management program including considering the risks related to approved policy exceptions and remediating known vulnerabilities.	DOA/DET will continue to update its risk management program including considering the risks related to approved policy exceptions and remediating known vulnerabilities.	Ongoing

Person responsible for corrective action:

Alan Greenberg, CISO  
 Division of Enterprise Technology  
 Alan.Greenberg@wisconsin.gov



State of Wisconsin  
**Department of Health Services**

Tony Evers, Governor  
 Karen E. Timberlake, Secretary

DATE: December 5, 2022

TO: Lisa Kasel, Assistant Financial Audit Director  
 Legislative Audit Bureau

FROM: Barry Kasten, Director  
 Bureau of Fiscal Services  
 Department of Health Services

SUBJECT: Corrective Action Plan – Financial Reporting for the Medical Assistance Program

Department staff has reviewed the Legislative Audit Bureau's (LAB) interim audit memo for Finding 2022-005: Financial Reporting for the Medical Assistance program. This is the department's Corrective Action Plan.

**Recommendation (2022-005): Financial Reporting for the Medical Assistance Program**

*We recommend the Wisconsin Department of Health Services:*

- Develop and implement additional procedures to evaluate the potential effects of changes in the program that it administers; and

**Wisconsin Department of Health Services Planned Corrective Action:**

DHS staff responsible for preparing the financial statements will improve their current procedures by meeting in smaller groups with program accountants annually to identify significant new programs, changes to existing programs, and other notable changes. They will obtain a more complete understanding of the financial reporting process of new programs and ensure that all account balances, including fund balance, are appropriately reported and classified.

*We recommend the Wisconsin Department of Health Services:*

- Use the additional procedures to evaluate changes that may require further consideration and adjustments for financial reporting purposes.

Memo to Lisa Kasel  
December 5, 2022  
Page 2

**Wisconsin Department of Health Services Planned Corrective Action:**

Using the additional procedures put in place, DHS staff will critically analyze changes identified to ensure compliance with Federal and State accounting requirements. DHS staff will ensure all necessary adjustments are made.

**Anticipated Completion Date:** September 30, 2023

Person responsible for corrective action:

Emily Pape, Section Chief  
Cost Allocation & GAAP Reporting Section, Bureau of Financial Services, Division of Enterprise  
Services

[Emily.Pape@dhs.wisconsin.gov](mailto:Emily.Pape@dhs.wisconsin.gov)



101 E. Wilson Street  
 2nd Floor  
 PO Box 8943  
 Madison, WI 53708-8943

608 266-1370 INFORMATION  
 608 266-0034 LOANS  
 608 267-2787 FAX  
 bcpl.wisconsin.gov

Thomas P. German, *Executive Secretary*

## Corrective Action Plan

### Finding 2022-006: Common School Fund—Service Organization Internal Controls

#### Planned Corrective Action:

- BCPL has recognized the value of Service Organization Internal Control (“SOC”) Reports as BCPL first raised this issue with LAB.
- BCPL will annually request from Charles Schwab, a Type 1 and Type 2 SOC Report.
- BCPL staff have already considered their reliance on Schwab and have reviewed the Suggested “Complementary User Entity Control Considerations” identified in Schwab’s SOC Reports.
  - BCPL staff agree that these suggested controls are appropriate for BCPL’s use of Schwab’s services and reliance upon Schwab. BCPL staff asserts that they have been consistently exercising virtually all of these controls for an extended period of time.
  - The only suggested user control that had not been previously adopted by BCPL was a systematic analysis of the publicly traded asset pricing provided by Schwab. In order to obtain additional assurances that the pricing provided by Schwab (or its vendor) on such assets is accurate, BCPL will, on a quarterly basis, BCPL select a sampling of approximately 5% of the publicly traded assets custodied at Schwab and will compare the values of such assets as reported by Schwab against valuations provided by Bloomberg or another nationally recognized financial valuation entity. It should be noted that BCPL had already instituted quarterly pricing reviews of private investment funds custodied at Schwab.
- Annually upon receipt of such SOC Reports, BCPL will distribute copies of such reports to the members of BCPL’s Investment Committee and schedule a committee discussion regarding:
  - BCPL’s reliance upon the services provided by Schwab;
  - BCPL’s control processes compared with the suggested Complementary User Entity Control Considerations set forth in Schwab’s SOC report;
  - Any weaknesses identified in the SOC Reports and any subsequent actions which should be taken by BCPL.
- BCPL shall then document such review and any subsequent actions which should be taken.



*Anticipated Completion Date:*

- BCPL has already requested and received such latest SOC reports described above and provided copies of such Reports to LAB.
- BCPL has already considered their reliance on Schwab and has reviewed the Suggested User Complementary Controls identified in Schwab's SOC 1 Report and furthermore has had virtually all such suggested controls in place for an extended period of time.
- BCPL has already implemented the additional systematic valuation testing identified above for the fiscal quarters ended on June 30, 2022 and September 30, 2022 and shall continue such valuation testing within 15 days after fiscal quarters ending December 31, March 31, June 30 and September 30.
- BCPL has already emailed (and mailed) copies of such latest SOC reports to the members of the BCPL Investment Committee.
- Prior to January 10, 2023, BCPL will schedule the committee discussion described above. BCPL shall document the matters identified above on or before January 15, 2023.

Tom German, BCPL Executive Secretary shall be responsible for implementing this action. His contact information is as follows:

[Tom.german@wisconsin.gov](mailto:Tom.german@wisconsin.gov)

(608) 267-2233



Office of Financial Administration  
608-262-1313 | 608-262-5316 (fax)  
780 Regent Street  
Suite 255  
Madison, WI 53715  
[www.wisconsin.edu/financial-administration/](http://www.wisconsin.edu/financial-administration/)

### Corrective Action Plan

#### **Finding 2022-007: UW System Information Technology Internal Control Deficiencies**

**Planned Corrective Action:** The UW System has adequate processes in place for reviewing access to ShopUW+ but agrees to better document these processes. UW System Administration (UWSA) has revised the disbursement internal control template, which all UW universities use in developing their internal control plans, to document the UW System’s security reviews. UWSA will also update the language surrounding its weekly access reports, to explain their purpose and importance. To monitor this control, the UW System will add a statement to this effect in the universities’ annual delegation agreement and certifications.

UWSA is actively taking steps to mature its third-party risk management practices, including the development of guidance and best practices for UW universities. Current efforts are focused on optimizing available resources to provide the highest return on value.

UWSA currently performs periodic reviews of cloud-based third-party internal controls during pre-contract evaluations and at the time of contract renewals. This includes obtaining and reviewing service organization audit reports, if available. UWSA will evaluate the efficacy of increasing the periodicity of these reviews to an annual basis. UWSA will also evaluate means for communicating identified expectations systemwide, up to and including the creation of a new policy.

*Anticipated Completion Date:* June 30, 2023

Person responsible for corrective action:  
Julie Gordon, Senior Associate Vice President  
Finance, UW System Administration  
jgordon@uwsa.edu

---

## Response

---





STATE OF WISCONSIN  
DEPARTMENT OF ADMINISTRATION

Tony Evers, Governor  
Kathy Blumenfeld, Secretary-designee

---

December 20, 2022

Joe Chrisman, State Auditor  
Legislative Audit Bureau  
22 East Mifflin Street, Suite 500  
Madison, Wisconsin 53703

Dear Mr. Chrisman:

I am writing in response to the Fiscal Year 2021-22 financial audit that the Legislative Audit Bureau recently completed and want to extend our appreciation to you and your staff for your diligent work related to this annual audit. I appreciate how staff from both the LAB and the State Budget and Controller's Office were able to complete this project in a collaborative and productive way.

The Department of Administration (DOA) takes very seriously all issues related to information technology across state government and has been taking steps to improve information technology security across the enterprise. Thus, I want to reiterate our concurrence with the LAB recommendations related to Information Technology oversight and monitoring responsibilities as noted in the audit report.

Further, we will continue to work with state agencies to ensure compliance with policies, procedures, and processes.

Again, thank you for your timely and important work.

Sincerely,

A handwritten signature in black ink that reads "Kathy Blumenfeld". The signature is written in a cursive, flowing style.

Kathy Blumenfeld, Secretary-designee  
Department of Administration