Report 18-3
February 2018

# State of Wisconsin

## Fiscal Year 2016-17 Financial Statements

STATE OF WISCONSIN



Legislative Audit Bureau

**Report 18-3**
**February 2018**

# State of Wisconsin
## Fiscal Year 2016-17 Financial Statements

### Joint Legislative Audit Committee Members

| Senate Members: | Assembly Members: |
|---|---|
| Robert Cowles, Co-chairperson | Samantha Kerkman, Co-chairperson |
| Chris Kapenga | John Macco |
| Alberta Darling | John Nygren |
| Kathleen Vinehout | Melissa Sargent |
| Mark Miller | Terese Berceau |

**Report 18-3**
**February 2018**

# LEGISLATIVE AUDIT BUREAU

**State Auditor**
Joe Chrisman

**Special Assistant to the State Auditor**
Anne Sappenfield

**Financial Audit Directors**
Kendra Eppler
Sherry Haakenson
Carolyn Stittleburg

**Assistant Financial Audit Directors**
Lisa Kasel
Erin Scharlau

**IT Audit Manager**
Colin Shogren

**Publications and Design Coordinator**
Susan Skowronski

The Bureau is a nonpartisan legislative service agency responsible for conducting financial audits and performance evaluations of state agencies. The Bureau's purpose is to provide assurance to the Legislature that financial transactions and management decisions are made effectively, efficiently, and in compliance with state law and that state agencies carry out the policies of the Legislature and the Governor. 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.*

**Team Leaders**
Shellee Bauknecht
Bruce Flinn
Jenny Frank
Jacob Gasser
Brian Geib
Kendra Glander
Nathan Heimler
Rachael Inman
Amanda Murkley
Katie Natzke
Emily Pape
Joshua Petersen

**Auditors**
Emily Albrecht
Jeffrey Beckett
Kimberly Cantwell
Bridget Cull
Martha Czerniakowski
Aaron Erdmann
Tom Fornander
Rita Klawitter
Michael Kuen
Tenzin Kunsang
Jan McAllister
Heather Murray
Lucas Nelson
Thi Nguyen
Kimberly Olson
Jake Poulos
Matt Rossi
Keri Routhieaux
BreeAnn Schlenske
Dominic Schuh
Phillip Stapel
Matthew Terpstra
Joseph Westby
Elizabeth Wilson
Brandon Woller
Fei Xiong
Stephanie Yost

Contact the Bureau at 22 East Mifflin Street, Suite 500, Madison, Wisconsin 53703; *AskLAB@legis.wisconsin.gov;* or (608) 266-2818.

# CONTENTS



# OPINIONS PUBLISHED SEPARATELY

The financial statements and our opinions on them are included in the State of Wisconsin's Comprehensive Annual Financial Report (CAFR) for the fiscal year ended June 30, 2017

STATE OF WISCONSIN | Legislative Audit Bureau

22 East Mifflin St., Suite 500 ▪ Madison, WI 53703 ▪ (608) 266-2818 ▪ Hotline: 1-877-FRAUD-17 ▪ www.legis.wisconsin.gov/lab

Joe Chrisman
State Auditor

February 14, 2018

Senator Robert Cowles and
Representative Samantha Kerkman, Co-chairpersons
Joint Legislative Audit Committee
State Capitol
Madison, Wisconsin 53702

Dear Senator Cowles and Representative Kerkman:

We have completed our financial audit of the State of Wisconsin as of and for the fiscal year ended June 30, 2017, and issued unmodified opinions dated February 13, 2018, on the State's financial statements. These financial statements were prepared by the Department of Administration (DOA) in accordance with generally accepted accounting principles (GAAP) and are included in the State's fiscal year (FY) 2016-17 Comprehensive Annual Financial Report (CAFR), which may be found on DOA's website.

State agencies, except the Department of Transportation (DOT), implemented the State's new enterprise resource planning system (STAR) on October 1, 2015, and this implementation affected the timing of financial reporting for FY 2015-16. STAR implementation for DOT occurred on July 1, 2016, and affected the timing of financial reporting for FY 2016-17.

The CAFR helps to describe the State's fiscal condition and contains information on over 90 funds. In the remainder of this letter, 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; explain the State's disclosure of tax abatements; and describe our findings related to internal controls over financial reporting.

## General Fund

As reported on a GAAP basis, the General Fund's fund balance was a deficit of $1.6 billion as of June 30, 2017, as shown on page 44 of the CAFR. In its Management's Discussion and Analysis on page 29, DOA noted that total General Fund revenue, which was derived from taxes and federal revenues, increased by $513.1 million and totaled $25.5 billion for FY 2016-17. Total General Fund expenditures and transfers increased by $332.3 million primarily due to increases in school aids payments and Medical Assistance costs, and totaled $25.3 billion for FY 2016-17.

## Transportation Fund

On a GAAP basis, the balance of the Transportation Fund decreased from $717.3 million as of June 30, 2016, to $582.4 million as of June 30, 2017, as shown on page 44 of the CAFR. In its Management's Discussion and Analysis on page 31, DOA noted that the majority of the

Transportation Fund's balance (96.2 percent) was "restricted" on the Balance Sheet due to the November 2014 constitutional amendment related to uses of the Transportation Fund. Total transportation-related expenditures decreased by $115.1 million to $2.4 billion in FY 2016-17. The expenditures reported in the Transportation Fund were funded largely by motor fuel taxes, registration fees, and federal revenues.

## Long-term Debt

The State's long-term debt decreased from $13.7 billion as of June 30, 2016, to $13.6 billion as of June 30, 2017, as shown in the Management's Discussion and Analysis on page 34. The amount of outstanding annual appropriation bonds increased and the amount of outstanding revenue bonds decreased. During FY 2016-17, $1.3 billion in new general obligation bonds and notes were issued, of which $484.4 million was for transportation projects.

## Disclosure of Tax Abatements

The Governmental Accounting Standards Board issued a tax abatement disclosure requirement that first affected financial reporting for the State in FY 2016-17. Wisconsin Statutes authorize tax abatements that result in a reduction in the amount of tax revenue the State would otherwise collect. The State disclosed those abatement programs that affected tax revenues for the State in FY 2016-17, including five programs administered by the Wisconsin Economic Development Corporation and one program administered by the Wisconsin Historical Society. As reported in Note 26, state tax revenues were reduced by $78.2 million in FY 2016-17 as a result of abatement agreements under these programs.

## Findings Related to Internal Control over Financial Reporting

We identified internal control weaknesses during our audit that are required to be reported under *Government Auditing Standards*. Specifically, we identified one material weakness and eight significant deficiencies in internal control. The Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters, which begins on page 7, discusses each concern and includes the responses and corrective action plans from management of the responsible agency.

We continued to identify weaknesses in information technology (IT) security policies and procedures that resulted in weaknesses in the administration of STAR. Although DOA took steps to reduce the inappropriate or excessive access we identified in report 17-4, we continued to identify concerns with security administration over STAR and we report a material weakness in internal control (Finding 2017-007). We also report a significant deficiency in internal control related to concerns with STAR access at the Department of Revenue and include recommendations for improvement (Finding 2017-002).

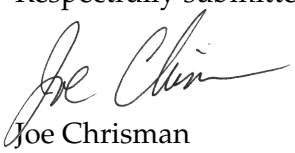
We also continued to identify weaknesses in the University of Wisconsin (UW) System's (Finding 2017-003) and DOA's (Findings 2017-004 and 2017-005) IT security policies and procedures, which we consider to be significant deficiencies in internal control. We include recommendations for UW System Administration and DOA to address their respective control

deficiencies. The recommendations for UW System Administration (Finding 2017-003) were also included in the Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters for UW System's financial statements (report 18-2).

Other significant deficiencies in internal control over financial reporting were identified at DOA related to cash (Finding 2017-001) and the Environmental Improvement Fund (Finding 2017-006). We also report significant deficiencies in internal control over financial reporting at DOT related to capital assets (Finding 2017-008) and the use of certain data from STAR (Finding 2017-009). We include recommendations for DOA and DOT to address their respective control deficiencies.

We appreciate the courtesy and cooperation extended to us by DOA and other state agencies during the audit. During the FY 2017-18 audit, we will follow up on the progress of state agencies in implementing our recommendations.

Respectfully submitted,



Joe Chrisman
State Auditor

JC/CS/ss

# Auditor's Report ■

STATE OF WISCONSIN | Legislative Audit Bureau

22 East Mifflin St., Suite 500 ▪ Madison, WI 53703 ▪ (608) 266-2818 ▪ Hotline: 1-877-FRAUD-17 ▪ www.legis.wisconsin.gov/lab

Joe Chrisman
State Auditor

**Report 18-3**

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

Honorable Members of the Legislature The Honorable Scott Walker, 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, 2017, and have issued our report thereon dated February 13, 2018.

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 Comprehensive Annual Financial Report (CAFR) for the fiscal year ended June 30, 2017.

Our report includes a reference to other auditors who audited the financial statements of the Environmental Improvement Fund, the College Savings Program Trust, the Wisconsin Housing and Economic Development Authority, the University of Wisconsin Hospitals and Clinics Authority, and the University of Wisconsin Foundation, as described in our report on the State of Wisconsin's basic financial statements. The financial statements of the Environmental Improvement Fund, the College Savings Program Trust, the Wisconsin Housing and Economic Development Authority, and the University of Wisconsin Hospitals and Clinics 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 University of Wisconsin 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 University of Wisconsin Foundation.

## 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 to determine the

audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the State's internal control. Accordingly, we do not express an opinion on the effectiveness of the State's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent 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. However, we identified certain deficiencies in internal control that we consider to be material weaknesses or significant deficiencies.

We consider the deficiency in internal control, described in the accompanying Findings and Responses Schedule as Finding 2017-007, to be a material weakness. We consider the deficiencies in internal control, described in the accompanying Findings and Responses Schedule as Findings 2017-001 through 2017-006 and 2017-008 through 2017-009, to be significant deficiencies. Because the University of Wisconsin (UW) System's financial activity is also reported separately from the State's CAFR, Finding 2017-003 was also included in the Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters for UW System's financial statements (report 18-2).

## 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 determination of financial statement amounts. 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

Agency-specific responses, including corrective action plans, to the findings identified in our audit are described in the accompanying Findings and Responses Schedule. The responses and

corrective action plans were not subjected to the 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

Joe Chrisman
State Auditor

February 13, 2018

# FINDINGS AND RESPONSES SCHEDULE

This schedule includes one material weakness and eight significant deficiencies related to internal control over financial reporting that are required to be reported by auditing standards generally accepted in the United States of America and *Government Auditing Standards*. Findings 2016-004, 2016-005, 2016-006, and 2016-007 from the prior year (report 17-4) were resolved. Repeat findings from report 17-4 are indicated with an asterisk (*).

## Finding 2017-001: Internal Controls over Financial Reporting for Cash at the Department of Administration

*Criteria:*

The Department of Administration (DOA) State Controller's Office (SCO) is the custodian of the State's cash assets and has a complex and broad set of responsibilities that includes implementing proper internal controls to ensure cash assets are properly managed and are properly reported for financial reporting purposes. This responsibility includes ensuring accuracy in the preparation of the Monthly Statement of Receipts and Disbursements by Fund, which is used by some agencies for financial reporting. In addition, SCO is responsible for working with its staff and state agencies to ensure errors in cash balances that have not been corrected in the State's accounting and payroll system, STAR, by financial statement reporting dates are appropriately adjusted in the financial statements.

*Condition:*

In our audit of SCO's internal controls over cash, we identified an error in the preparation of the Monthly Statement of Receipts and Disbursements by Fund for June 2017. We found that total receipts for the Transportation Fund were understated by $4.8 million. This error caused an understatement of ending pool shares and an overstatement of check float as presented on the monthly statement. Further, after we brought these errors to its attention, SCO identified an additional error of $290,000 in receipts of the Hospital Assessment Fund.

In addition, in conducting our audit work related to the State's General Fund financial statements to be presented in the State's CAFR, we questioned a $38.2 million increase in a liability that, after discussion with SCO staff, was determined to be the result of an error in the cash balance for the General Fund as of June 30, 2017. The error had been appropriately identified as a reconciling item in the bank reconciliation process and was corrected on STAR in fiscal year (FY) 2017-18. However, SCO staff did not ensure the error was considered for FY 2016-17 financial reporting. This error resulted in a $38.2 million overstatement of the General Fund cash balance as of June 30, 2017.

Further, after we discussed these errors with SCO staff, we were informed that SCO had identified a third error that occurred during the implementation of the STAR payroll module, Human Capital Management (HCM), in FY 2015-16. This error resulted in a $7.3 million understatement of the General Fund cash balance on the June 30, 2017 financial statements.

Finally, as part of our audit of the bank reconciliation, we raised questions regarding an outstanding receipt of $9.6 million that was deposited in the bank in March 2017, but was not

yet recorded in STAR as of June 30, 2017. SCO staff researched this reconciling item and identified that it related to a deposit that had been made to a disbursement account. This error resulted in a $9.6 million understatement of the General Fund cash balance on the June 30, 2017 financial statements.

These errors in the presentation of the General Fund financial statements in the State's CAFR were corrected, and SCO informed the relevant agencies of the errors for consideration in financial reporting.

***Questioned Costs:***

None.

***Context:***

In conducting our audit of the State's CAFR, we test the controls over cash within SCO, including testing the bank reconciliation and preparation of the Monthly Statement of Receipts and Disbursements by Fund. SCO is responsible for ensuring there are proper controls over cash, including controls to ensure cash is reported accurately for financial reporting. This could include taking steps to communicate errors to other state agencies or to the SCO Financial Reporting Section, which has responsibility for compiling the State's CAFR.

***Effect:***

There is an increased risk of errors in the reporting of cash balances in the State's financial statements. The net effect on the specific errors described in the condition was a $21.3 million overstatement of the General Fund cash balance as of June 30, 2017. Further, the net effect of the errors overstated ending pool shares and understated check float as reported on the June 2017 Monthly Statement of Receipts and Disbursements by Fund.

***Cause:***

Errors in a query used to prepare the Monthly Statement of Receipts and Disbursements by Fund contributed to some of the errors. In addition, SCO staff did not always understand the effects of the errors on financial reporting and, therefore, did not take steps to communicate them to the appropriate agencies.

## ☑ Recommendation

*We recommend the Wisconsin Department of Administration State Controller's Office implement a process to communicate errors and other adjustments to cash balances in a timely manner to the appropriate agency staff and to the State Controller's Office Financial Reporting Section to ensure consideration of the implications on financial statement presentation.*

**Response from the Wisconsin Department of Administration:** The Department of Administration agrees with the recommendation.

**Corrective Action Plan from the Wisconsin Department of Administration:** This is to provide a Corrective Action Plan to address the concerns raised in Finding 2017-001: Internal Controls over Financial Reporting for Cash.

No later than January 31, 2018, the State Controller's Office will develop and implement procedures to communicate errors and other adjustments to cash balances in a timely manner to the appropriate agency staff and to the State Controller's Office Financial Reporting Section to ensure consideration of the implications on financial statement presentation.

---

## Finding 2017-002: STAR Finance Access Concerns at the Department of Revenue

*Criteria:*

HCM and Finance are two components of STAR, the State of Wisconsin's enterprise resource planning system. STAR HCM provides integrated human resources and payroll business functions. STAR Finance provides accounting functions and serves as the basis for the financial information used in preparing the State's financial statements.

Security for STAR is based on roles and permission lists. Users are assigned to roles that provide access to STAR based on the permissions granted to each role. Although DOA is responsible for creating and configuring the overall security for STAR, including the set up and maintenance of roles and permission lists, the Department of Revenue (DOR) is responsible for determining and authorizing the roles its employees are assigned to, including ensuring that assigned roles or other controls appropriately separate job duties. DOR is also responsible for removing access when necessary.

*Condition:*

DOR staff did not remove STAR Finance access for terminated employees in a timely manner. We reviewed 62 employees assigned to more than two roles in STAR Finance and found 21 were no longer employed by DOR. In addition, 2 of those 21 individuals were assigned roles in STAR Finance that created separation of duties conflicts, and one of these individuals was employed by another state agency after leaving DOR.

*Questioned Costs:*

None.

*Context:*

We reviewed employees with access to STAR Finance for DOR and assessed whether they were current DOR employees. Because most employees are provided two basic roles within STAR Finance and these roles are considered to be of lower risk, our review focused on those employees assigned to more than two roles due to the increased risk potential.

*Effect:*

There is an increased risk of inappropriate transactions being processed in STAR Finance that could result in misstatement of the financial statements and/or misappropriation of assets. This risk is increased for those employees assigned to roles that create separation of duties conflicts and for terminated employees who are now employed by another agency and would not be prevented from using a computer at the current employing agency to access STAR Finance and process transactions for DOR.

*Cause:*

DOR staff believed that DOA had implemented a process to automatically remove access to STAR Finance when access was removed to STAR HCM.

**☑ Recommendation**

*We recommend the Wisconsin Department of Revenue:*

- *review access to STAR Finance and seek changes as needed to ensure terminated employees do not retain access; and*

- *develop and implement procedures to ensure access is removed in a timely manner when employees terminate employment.*

**Response from the Wisconsin Department of Revenue:** The Department agrees with the finding and recommendations.

**Corrective Action Plan from the Wisconsin Department of Revenue:** This memo is the Wisconsin Department of Revenue's corrective action plan for the finding and recommendations made by the Legislative Audit Bureau (LAB) in the interim memo dated November 30, 2017, regarding the STAR Finance Access Concerns (Finding 2017-002).

DOR Corrective Action Plan

The Department plans to take the following corrective actions:

- DOR will perform a reconciliation between STAR HCM and STAR Finance to determine if any terminated employees still have STAR Finance access that did not get removed by the automatic removal process. STAR Finance access will be removed for those terminated employees no later than December 31, 2017.

- In a two-phased process, the responsibility for maintenance of STAR Finance and STAR HCM accesses will be transferred to the Department's Security Support Unit in the Division of Technology Services (DTS). This change will ensure that STAR system access is treated similar to all other system accesses in DOR.

    - By February 23, 2018, DTS Security will have procedures in place for removing STAR Finance and STAR HCM access in a timely manner for terminated employees consistent with existing procedures for removing all other system access.

    - By April 27, 2018, DTS Security will have procedures in place for adding & changing roles for employees in STAR Finance and STAR HCM.

- The Security Support Unit in the Division of Technology Services (DTS) conducts periodic review of agency system accesses to ensure former employees have had their system accesses removed. STAR HCM and STAR Finance will be added to the list of systems for this periodic review by March 31, 2018.

## Finding 2017-003: Information Technology Controls at the University of Wisconsin System*

*Criteria:*

The UW System consists of 13 four-year universities, 13 two-year colleges, UW-Extension, and UW System Administration. UW institutions operate in a highly computerized environment and are responsible for maintaining confidential and sensitive information, such as student data. UW System Administration maintains the Shared Financial System (SFS), which is UW System's accounting system, and the Human Resource System (HRS), which is UW System's payroll and personnel system. These systems are used by all UW institutions. In addition, each institution maintains its own student information system (SIS) to administer federal student financial aid programs, as well as other computer applications. To provide proper internal control, information technology (IT) security policies and procedures are necessary to ensure software and data stored and processed by the institutions are protected from accidental or intentional misuse or destruction. In addition, IT controls should be established to prevent inappropriate or inadvertent access to systems and data.

In developing systemwide IT security policies and procedures, UW System Administration consulted policies and procedures from UW institutions and other educational institutions, as well as using the National Institute of Standards and Technology (NIST) *Special Publication 800-63* and *Special Publication 800-171*. NIST publications provide a framework for establishing a well-controlled IT environment and are most effective when implemented for all critical IT areas. The UW Information Assurance Council, which is made up of IT, legal, and audit staff representing different institutions, including UW System Administration, was established to identify and analyze risks related to IT security, develop policies to address these risks, and review the performance of the UW System IT security program. Chancellors and chief information officers at each institution are responsible for ensuring compliance with the new policies.

*Condition:*

We have reported weaknesses in UW System's IT security policies, procedures, and controls during our FY 2014-15 and FY 2015-16 audits. We made recommendations for UW System Administration to develop systemwide IT security policies and procedures, assist UW institutions in implementing timely corrective actions related to our institution-specific concerns, and develop procedures for assessing the level of protection provided for UW systems and data.

In response to our prior-year recommendations, the UW System Board of Regents approved, in December 2015, a high-level policy on information security that required UW System to develop and maintain a comprehensive IT security program. Further, five systemwide IT policies were established in September 2016 through the UW Information Assurance Council. These policies covered the following areas: authentication, data classification, security awareness, incident response, and acceptable use. However, UW System Administration has not taken significant steps to develop IT policies and procedures to cover other critical areas under the NIST framework and to meet the requirements of the Board of Regents policy to develop a comprehensive IT security program.

In response to our institution-specific recommendations from prior years, we found institutions were working to address the concerns we noted in our prior audits in several areas. For example, institutions were implementing password controls in an effort to comply with UW System Administration policies and procedures. However, many of these corrective actions were completed late during FY 2016-17, and we also identified new areas of concern. We determined that the detailed results of our review were too sensitive to communicate publicly. Therefore, we communicated these results in confidential interim memoranda to the institutions involved.

In addition, UW System Administration staff indicated that UW System Administration's Office of Internal Audit is in the process of performing IT audits at each UW institution to test compliance with UW System Administration IT security policies and procedures. Finally, UW System Administration indicated that it is in the process of developing procedures to assess the overall level of protection provided for UW systems and data. UW System Administration indicated that procedures will be implemented by December 2017.

***Questioned Costs:***

None.

***Context:***

We reviewed UW System's new IT security policies and procedures and assessed them in comparison to NIST standards. We interviewed the Vice President for Administration, the Chief Information Officer, and the Chief Information Security Officer for UW System Administration. We tested various IT controls at several UW institutions. We did not audit the IT security policies and procedures at all UW institutions or the IT controls over all computer applications used by the institutions. However, we believe there is a potential that similar weaknesses may exist at those institutions or in those applications that we did not review.

***Effect:***

Although it can be difficult to determine how IT concerns such as those we identified affect the financial statements and material federal compliance areas, ineffective general IT controls in areas such as these may permit controls over individual systems to operate improperly and may allow financial statement misstatements and noncompliance to occur and not be detected.

Weaknesses in IT security policies, procedures, and controls increase the risk that unauthorized or erroneous transactions could be processed or changes could be made to accounting, payroll, and student data. In addition, failure to provide an appropriate level of protection for UW systems and data increases the risk that personally identifiable information could be accidentally or maliciously exposed. Finally, ineffective or inconsistent general IT controls may lead to increased risks of cyberattacks and loss of data or intellectual property, which could lead to a significant financial loss.

***Cause:***

UW System Administration, working with the UW Information Assurance Council, has not agreed on the next areas of systemwide IT security policy and procedure development. The resources and time needed by the institutions to implement the current IT security policies and

procedures were noted as reasons for delays in the further development of systemwide IT security policies and procedures.

IT staff at each UW institution are responsible for ensuring IT security policies, procedures, and controls are properly developed and maintained. Those institutions that have smaller IT staff may find challenges in meeting these responsibilities, maintaining proper separation of duties, and monitoring sufficiently all security policies and procedures. In addition, with changing technologies, monitoring and assessment of current processes are necessary to evaluate changing data security risks.

### ☑ Recommendation

*In addition to recommendations we made to individual University of Wisconsin institutions, we recommend UW System Administration continue to work with the UW Information Assurance Council and individual institutions to:*

- *continue development and maintenance of a comprehensive IT security program, including developing systemwide IT security policies and procedures across the remaining critical IT areas as recommended by National Institute of Standards and Technology publications;*

- *provide guidance and training to the institutions regarding information technology security policies and procedures, as needed;*

- *assist the institutions in implementing timely corrective actions related to our institution-specific recommendations; and*

- *complete development of and implement procedures for assessing the level of protection provided for UW systems and data.*

**Response from the University of Wisconsin System:** UW System Administration agrees with the recommendations.

**Corrective Action Plan from the University of Wisconsin System:** In regard to finding 2017-003, UW System Administration agrees with the assessment that additional steps should continue to be taken to develop IT policies and procedures to cover other critical areas under the NIST framework and to meet the requirements of the Board of Regents policy to develop and maintain a comprehensive information security program. UW System Administration will work with the UW Information Assurance Council to address the recommendations as follows:

| Action Item | Anticipated Date |
|---|---|
| Continue development and maintenance of a comprehensive IT security program including developing systemwide IT security policies and procedures across the remaining critical IT areas as recommended by National Institutes of Standards and Technology publications | |
| Develop a UW System Information Security Program document, accompanied by a 12-month work plan. | April 30, 2018 |
| Create additional systemwide, NIST-based information security policies to support the Information Security Program. Include in the 12-month work plan the next set of policies to be developed. | Based on Information Security Program schedule |
| Provide guidance and training to the institutions regarding information technology security policies and procedures, as needed | |
| Develop documentation which provides comprehensive guidance to all UW institutions on suggested methods to implement information security policies and procedures. | April 30, 2018 |
| Conduct monthly reviews, during which UW System institutions will share best practices, identify ways to most effectively use available resources, as well as receive guidance from UW System on resources which can be used to implement policies. | January 30, 2018 (start date) |
| Assist the institutions in implementing timely corrective actions related to our institution-specific recommendations | |
| Engage monthly with the UW System institutions, advising them of potential ways to address audit recommendations and confirming progress as planned. Lead in aligning resources with institution priorities to address audit recommendations. | January 30, 2018 (start date) |
| Complete development of and implement procedures for assessing the level of protection provided for UW systems and data | |
| Complete external UW System Information Security Assessment to establish a baseline for assessing the level of protection provided for systems and data. | March 30, 2018 |
| Use results of external Information Security Assessment to establish an order of priority in which to address deficiencies of data and systems protection, across UW System institutions and consistent with the Information Security Program. | April 30, 2018 |
| Provide an advanced General Data Protection Regulation readiness assessment to assist UW System institutions with awareness of the regulations; actions to comply with the regulations; and assessments to monitor progress. | June 30, 2018 |
| Establish an ongoing program to assess the level of protection provided for UW systems and data. | June 30, 2018 |

## Finding 2017-004: Department of Administration Division of Enterprise Technology Security Concerns*

*Criteria:*

Section 16.97, Wis. Stats., specifies DOA's responsibilities for the State's IT services, including DOA's responsibility to ensure that all state data processing facilities develop proper privacy and security procedures and safeguards. As part of DOA, the Division of Enterprise Technology (DET) provides a variety of services to state agencies, including:

- managing the mainframe computer for all agencies and managing servers for DOA and other executive branch agencies, including the departments of Corrections, Health Services, Children and Families, Natural Resources, and Revenue;

- housing servers for agencies that manage their own devices including the departments of Workforce Development and Public Instruction; and

- maintaining DOA-related systems and performing programming and security functions, including maintaining the infrastructure for STAR, which includes statewide accounting and payroll functions.

Because the mainframe computer and servers contain financial data and confidential information, it is important that DET manage and maintain a secure environment. Managing a secure environment involves developing, approving, and following appropriate policies, standards, and procedures.

As defined by DET, IT policies are formal, brief, high-level statements or plans that reflect an agency's general beliefs, goals, rules, and objectives for a specific subject area. Standards are mandatory actions or rules designed to support policies. Procedures are a documented series of steps that align with policies and standards. Well-written policies, standards, and procedures provide staff with a consistent methodology for performing their job functions.

DET uses the federal NIST framework as a guide to develop policies, standards, and procedures. Because of the diverse requirements of the agencies DET supports, its policies, standards, and procedures must comply with Wisconsin Statutes, as well as requirements of other laws and standards, such as the Internal Revenue Service, Criminal Justice Information Services, Health Insurance Portability and Accountability Act, Payment Card Industry Data Security Standard, and Family Educational Rights and Privacy Act.

It is also important that DET establish settings that enforce its policies, standards, and procedures. Settings are technical configurations that enforce controls for a computer or group of computers. For instance, password settings can enforce password length, which is prescribed by DET's policies and standards. Implementation of settings enforces the controls that are in place and, therefore, ensures that approved standards are being followed.

***Condition:***

We first reported concerns regarding a lack of policies, standards, and procedures over the DET data center operations during the FY 2014-15 audit. We recommended DET develop policies, standards, and procedures and address specific concerns we identified with IT practices and settings. DET has taken some steps to address these concerns including:

- developing and approving DET security policies;

- developing and approving 18 DET security standards;

- drafting 10 additional DET security standards, which are expected to be approved during FY 2017-18;

- developing plans and timelines to document and approve procedures for all DET sections that will comply with policies and standards; and

- developing plans and timelines to address specific security concerns we identified and working to remedy the specific concerns.

Although DET has taken steps to implement corrective actions related to our recommendations, we continue to identify concerns. First, we found that DET has not finalized all standards to support DET policies. Additionally, we found DET has not sufficiently communicated the approved policies and standards to DET staff. For example, staff of two DET sections were not aware of a new standard that was approved in October 2016 and, therefore, the staff did not review the settings in place and determine if changes were necessary.

Second, DET has not developed written procedures to comply with the DET policies and standards, and current practices and settings were not reviewed to ensure compliance with approved policies and standards.

Third, DET has not resolved all of the specific security concerns that we communicated in a March 2017 interim memorandum.

***Questioned Costs:***

None.

***Context:***

We reviewed the policies and standards developed by DET, discussed the status of DET's efforts to implement its prior-year corrective action plan, and tested security settings and practices.

Most state agencies use computer systems that are located on servers maintained in the DET data centers and are relied on to process checks, account for cash receipts, prepare financial statements, and administer federal grant programs.

***Effect:***

The lack of standards and procedures affects the level of security provided by DET. We continued to identify multiple areas of concern, which we specifically communicated to DET in March 2017.

Failure to properly manage and maintain a secure environment at the DET data centers could result in inappropriate access, which could result in the issuance of erroneous or fraudulent checks or the inappropriate viewing of confidential data.

Further, because DET hosts and supports a significant and growing number of executive branch agencies and systems at its data centers, risks at the data centers can affect the computing resources of a significant portion of the State. For example, since many agencies' systems and data are located at DET data centers, if a data center or the state network becomes compromised, there is an increased risk that harm could come to any of the systems or data of the agencies that use the data center or network.

***Cause:***

Although DET has agreed with our recommendations, the development and approval of policies and standards has been and continues to be a significant time commitment. Further, because DET's plan was to begin reviewing practices and settings after it had established its policies and standards, as of the end of FY 2016-17, DET had not yet began reviewing its practices and settings. Finally, for policies and standards that have been finalized and

published, DET has not adequately communicated to staff that new policies and standards exist and need to be followed.

### ☑ Recommendation

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

- *implement its plan to establish standards and procedures according to its proposed timeline;*
- *review current practices and settings to ensure controls conform to the approved policies, standards, and procedures, and make changes as appropriate; and*
- *assess the risks related to the concerns identified in this and previous security reviews and address the high-risk concerns immediately.*

**Response from the Wisconsin Department of Administration:** The Department of Administration agrees with the recommendations.

**Corrective Action Plan from the Wisconsin Department of Administration:**

| LAB Recommendation | DOA Corrective Action | Anticipated Corrective Action Date |
|---|---|---|
| 1. We recommend the Department of Administration, Division of Enterprise Technology (DET) implement its plan to establish standards and procedures according to its proposed timeline; | The Department will continue to execute its plan as follows: | |
| | ▪ Document and approve all the identified IT security standards (based on NIST 800-53r4). Currently DET has completed and approved all but one of the standards, which is currently under review. | In process with anticipated completion 1/26/2018 |
| | ▪ Complete the Analysis of existing procedures and create the prioritized list of procedures that need to be created or updated for implementation of the IT Security Standards. | In process with anticipated completion 2/28/2018 |
| | ▪ Updated or created procedures written and approved. | Begin 3/1/2018 with anticipated completion 2/28/2019 |
| | ▪ Implement approved IT standards and procedures. | Begin implementation as they are approved with anticipated completion 2/28/2020 |

| | | |
|---|---|---|
| 2. We recommend DET review current practices and settings to ensure controls conform to the approved policies, standards, and procedures, and make changes as appropriate; and | ▪ Document the process for the continuous review of approved IT controls settings/practices to ensure compliance with DET policies, standards and procedures.<br><br>▪ Conduct initial review of approved IT controls settings/practices to ensure compliance with DET policies, standards and procedures. | Begin on or before 2/28/2020 with anticipated completion 6/30/2020<br><br>Begin on or before 2/28/2020 with anticipated completion 12/31/2020 and annually thereafter. |
| 3. We recommend DET assess the risks related to the concerns identified in this and previous security reviews and address the high-risk concerns immediately. | DET has assessed the risk and initiated projects to address the high-risk concerns. | Projects are underway with various completion dates based on project time lines with anticipated completions between 6/30/2018 and 1/14/2020. |

## Finding 2017-005: Executive Branch Agency Information Technology Policies and Standards

*Criteria:*

Wisconsin Statutes give DOA responsibility for the State's IT services. For example, s. 16.971 (2), Wis. Stats., specifies DOA shall:

- in cooperation with executive branch agencies, establish policies, procedures, and planning processes for the administration of IT services, which executive branch agencies must follow;
- ensure the policies, procedures, and processes address the needs of agencies, other than the Board of Regents of the UW, to carry out their functions; and
- monitor adherence to these policies, procedures, and processes.

Further, s. 16.971 (2), Wis. Stats., requires DOA to provide oversight and monitoring of state agency IT operations, including the responsibility for 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.

NIST recommends organizations regularly perform vulnerability scanning to identify vulnerabilities and to remediate and minimize the opportunity for attacks to the organization's networks and systems. In addition, NIST recommends organizations conduct regular external and internal penetration tests to identify vulnerabilities and areas that may be used to exploit the organization's networks and systems.

Finally, Executive Order 99, which was issued on April 26, 2013, established the Information Technology Executive Steering Committee (ITESC) with the purpose of aligning enterprise IT deployment with statewide business goals. One of ITESC's stated goals is to create and maintain enterprise IT policies.

***Condition:***

During the FY 2015-16 audit, we recommended DOA develop plans and timelines in cooperation with executive branch agencies for the establishment, approval, and implementation of policies and standards that apply to all executive branch agencies and develop timelines and plans for providing oversight and monitoring of all executive branch agency IT operations, as required by s. 16.971 (2), Wis. Stats. DOA agreed with the recommendations and developed a corrective action plan. DOA indicated:

- it would finalize DET-specific policies and standards by June 30, 2017, and would use these policies and standards as a starting point for the development of executive branch agency IT policies and standards;

- it would meet with ITESC by June 15, 2017, to discuss the development of executive branch agency IT policies and procedures and DOA's responsibilities for oversight and monitoring of executive branch agency IT operations;

- ITESC would identify individuals to represent each agency in the development of statewide policies and standards by July 31, 2017;

- ITESC would identify individuals to represent each agency in the development of plans and timelines for monitoring and oversight of executive branch agencies' IT operations by October 31, 2017; and

- it would develop a plan and timeline by December 15, 2017, for development of agency policies and standards.

During FY 2016-17, DET finalized its policy handbook and successfully completed its first annual review of the policy handbook. Additionally, DET developed and approved 18 standards and drafted 10 additional standards that staff indicated were going through DET's review process and are expected to be approved in FY 2017-18.

However, as of completion of our audit fieldwork in November 2017, DOA had not met with ITESC to specifically discuss the recommendations in the Bureau memo related to the development of executive branch agency IT policies and procedures, nor had DOA taken any of the additional steps noted in its corrective action plan. DOA continues to be in noncompliance with state statutes regarding its responsibilities for development of executive

branch agency IT policies and standards and oversight and monitoring of IT operations at executive branch agencies.

In addition, we are concerned that DOA has not completed a comprehensive risk assessment to identify security concerns and vulnerabilities at the DET data centers. DOA hired an external firm to perform a risk assessment of the data center operations in 2012. However, this risk assessment was limited to DET-specific operations, and no additional comprehensive risk assessment has been performed since that time. A comprehensive risk assessment may include identifying all systems and data in the network and completing regular vulnerability assessments and penetration testing of the state's network and systems in the state's network. The risk assessment should include executive branch agency systems and networks that are housed within the state data centers as they can create risks to all the other systems housed within the data centers.

DOA cannot properly assess the criticality of all servers and systems within the state's network. Although DOA performs monthly vulnerability scans of the servers at the DET data centers to identify needed patches, it does not regularly complete penetration tests to identify and further evaluate the risk of the identified vulnerabilities.

Finally, DOA does not have comprehensive information regarding the level of vulnerability assessments and penetration testing completed by individual executive branch agencies. Therefore, DOA may not be aware of vulnerabilities that could affect the state's network or of steps executive branch agencies are taking that could reduce risk.

***Questioned Costs:***

None.

***Context:***

We interviewed the DOA Chief Information Officer, the DOA Chief Technology Officer, the DOA Chief Information Security Officer, and other DOA staff to gain an understanding of the steps that have been taken to develop executive branch agency IT policies and standards and monitoring and oversight of executive branch agency IT operations.

State agencies use computer systems that are located on servers maintained in the DET data centers and are relied on to process checks, account for cash receipts, prepare financial statements, and administer federal grant programs.

***Effect:***

A lack of policies and standards that apply to all executive branch agencies can lead to weaknesses in the state's network. Because there are interconnections across agencies in the state's network, weaknesses at one agency can affect other agencies' security.

Additionally, failure to monitor executive branch agencies' environment and practices can also lead to weaknesses in the state's network, known or unknown, because there is no assurance that all systems are meeting a minimum level of security for the State's IT environment, as determined by the policies and 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 staff have indicated to us that agency management is resistant to the development of IT policies and standards that apply to all executive branch agencies. For example, DOA staff have indicated that some agencies believe requirements to establish statewide policies and standards apply only to statewide systems, such as STAR. Additionally, DOA has indicated that agencies have been resistant to ITESC approved projects. For example, ITESC has approved a project to implement statewide web content filtering. However, DOA has noted little progress on the project, attributing some of the delays to significant resistance from agencies. Finally, despite its statutory responsibilities, DOA has not taken steps to use its authority to provide greater assurances on the security over the state's DET data centers, as well as oversight over agency-owned systems.

### ☑ Recommendation

*We recommend the Wisconsin Department of Administration:*

- *review and revise its plans and timelines for the establishment, approval, and implementation of policies and standards that apply to all executive branch agencies, including meeting with the Information Technology Executive Steering Committee by April 30, 2018;*

- *develop and implement a plan to complete vulnerability assessments and penetration testing across all devices and networks within the Division of Enterprise Technology data centers by December 31, 2018, and resolve any concerns needing immediate attention; and*

- *complete a comprehensive risk assessment across all executive branch agencies by December 31, 2018, including identifying all systems and data in the state's network and determining an appropriate level of vulnerability assessments and penetration testing to be completed on a regular basis of the network and systems within the network to identify and evaluate security concerns.*

**Response from the Wisconsin Department of Administration:** The Department of Administration agrees with the recommendations.

**Corrective Action Plan from the Wisconsin Department of Administration:**

| LAB Recommendation | DOA Corrective Action | Anticipated Corrective Action Date |
|---|---|---|
| 1. We recommend DOA review and revise its plans and timelines for the establishment, approval, and implementation of policies and standards that apply to all executive branch agencies, including meeting with the Information Technology Executive Steering Committee by April 30, 2018; | DOA will review and revise its plans and timelines for the establishment, approval, and implementation of policies and standards that apply to all executive branch agencies, including meeting with the Information Technology Executive Steering Committee. | Review has been initiated with anticipated completion 4/30/2018 |
| 2. We recommend DOA develop and implement a plan to complete vulnerability assessments and penetration testing across all devices and networks within the DET Data Centers by December 31, 2018, and resolve any concerns needing immediate attention; and | Since vulnerability assessments and penetration testing are two separate functions, DOA will address these as separate plans and implementations as follows:<br><br>Vulnerability Assessments will be conducted as the top priority to identify and address common vulnerabilities related to patching and configuration issues.<br><br>▪ Develop the plan for implementing vulnerability assessments across all devices and networks within the DET Data Centers<br><br>▪ Implement a life cycle for vulnerability assessment across all devices and networks within DET Data Centers including process for review of results, prioritization of identified issues and tracking of remediation activity.<br><br>Penetration Testing will be conducted after the common vulnerabilities have been addressed.<br><br>▪ Develop the plan for penetration testing across all devices and networks within the DET Data Centers.<br><br>▪ Implement penetration testing across all devices and networks within the DET Data Centers including process for review of results, prioritization of identified issues and tracking of remediation activity. | <br><br><br><br><br><br>4/30/2018<br><br><br><br>Begin 4/30/2018 with anticipated completion to be determined, based on plan.<br><br><br><br><br><br>Begin 4/30/2018 with anticipated completion 07/31/2018<br><br><br>Begin 7/31/2018 with anticipated completion to be determined, based on plan. |

| | | |
|---|---|---|
| 3. We recommend DOA complete a comprehensive risk assessment across all executive branch agencies by December 31, 2018, including identifying all systems and data in the state's network and determining an appropriate level of vulnerability assessments and penetration testing to be completed on a regular basis of the network and systems within the network to identify and evaluate security concerns. | DOA will develop a plan and timeline to identify executive branch agency systems and data in the state's network and determine the appropriate level of vulnerability assessments and penetration testing to be completed on a regular basis. | Begin 07/31/2018 with anticipated completion 12/31/2018 |
| | ▪ Implementation of vulnerability assessments of the identified systems and data including a process for review of results, prioritization of identified issues and tracking of remediation activity. | Begin 12/31/2018 with anticipated completion to be determined, based on plan. |
| | ▪ Implementation of penetration testing of the identified systems and data including a process for review of results, prioritization of identified issues and tracking of remediation activity. | Begin post vulnerability remediation with anticipated completion to be determined, based on plan. |

## Finding 2017-006: Financial Reporting Controls at the Department of Administration

*Criteria:*

The Capital Accounting Services Section (Capital Accounting) within DOA SCO is responsible for preparing financial statements for several funds, including the Bond Security and Redemption Fund (BSRF) and the Environmental Improvement Fund (EIF), and for preparing government-wide entries for reporting in the State of Wisconsin's CAFR. Capital Accounting is responsible for preparing the financial statements and government-wide entries in accordance with generally accepted accounting principles (GAAP). In addition, Capital Accounting prepares financial statements for the EIF to be included in the EIF's separately issued financial report. The BSRF and EIF financial statements and the government-wide entries are provided to the SCO Financial Reporting Section (FRS) for use in compiling the CAFR. FRS is responsible for reviewing financial statements and government-wide entries provided by the state agencies or other sections within DOA and working with those entities to adjust the financial statements or entries, as needed.

It is important to ensure financial statements appropriately reflect the financial activity and balances for the reporting period, and that this presentation is in accordance with GAAP to help readers of the financial statements have an accurate understanding on which to base decisions.

*Condition:*

In preparing the stand-alone EIF financial statements, which are audited by an external firm, Capital Accounting reported the surrender of an investment in general obligation subsidy bonds belonging to the EIF as a Special Item.

When FRS incorporated the EIF stand-alone financial statements into the State's CAFR, it changed the presentation of the Special Item to instead reflect transfers between the BSRF and the EIF. The revised financial statements for the BSRF and the EIF no longer clearly reflected the surrender of the EIF's investment in general obligation subsidy bonds and the cancellation of the debt by the State, but rather made it appear that the debt was paid off.

***Questioned Costs:***

None.

***Context:***

To evaluate the appropriate reporting for the transaction to surrender the investment in the general obligation subsidy bonds and the subsequent cancellation of the debt, we reviewed the stand-alone financial report for the EIF, obtained additional information from the external auditor, assessed GAAP requirements, and discussed the cancellation of the debt with DOA Capital Finance, Capital Accounting, FRS, and the State Controller.

The BSRF accounts for and reports financial resources that are restricted, committed, or assigned to expenditure for principal and interest, and accounts for financial resources that are being accumulated for future principal and interest. The EIF accounts for financial resources generated and used for clean water projects. Federal capitalization grants, interest earnings, revenue bond proceeds, and general obligation bond proceeds are the primary funding sources for the EIF.

***Effect:***

As a result of the adjustments made by FRS to the EIF financial statements when compiling the State's CAFR, the Special Item account was no longer presented and the following accounts were misstated in the EIF financial statements in the CAFR:

- Transfers Out was overstated by $148.9 million; and
- Investment and Interest Income was overstated by $20.5 million.

The related adjustments made by FRS to the BSRF resulted in the following misstatements in those financial statements:

- Debt Service—Principal expenditures was overstated by $148.9 million; and
- Transfers In was overstated by $148.9 million.

Finally, as a result of these misstatements, the entity-wide financial statements were also misstated because the statements did not reflect a Special Item.

After we discussed these concerns with them, FRS agreed to correct the financial statements. The corrections were to report, in the CAFR, the Special Item on the EIF financial statements and a Special Item on the entity-wide financial statements.

*Cause:*

The cancellation of general obligation bonds is an infrequent and complex event that contributed to the misstatements on the EIF and BSRF financial statements. The research performed by FRS on the surrender of the EIF's investment in general obligation subsidy bonds and the related cancellation of the debt by the state was not sufficient to properly assess the transaction for financial reporting purposes.

**☑ Recommendation**

*We recommend the Wisconsin Department of Administration State Controller's Office take steps, including conducting adequate research, to ensure the proper presentation of the financial activity and balances from stand-alone financial statements in the State of Wisconsin's Comprehensive Annual Financial Report.*

**Response from the Wisconsin Department of Administration:** The Department of Administration agrees with the recommendation.

**Corrective Action Plan from the Wisconsin Department of Administration:** This is to provide a Corrective Action Plan to address the concerns raised in Finding 2017-006: Financial Reporting Controls at the Department of Administration. Thank you for bringing this issue to my attention.

The Department of Administration, State Controller's Office will immediately take steps, including conducting adequate research, to ensure the proper presentation of the financial activity and balances from stand-alone financial statements in the State of Wisconsin's CAFR.

## Finding 2017-007: STAR Security Concerns*

*Criteria:*

Section 16.97, Wis. Stats., specifies DOA's responsibilities for the State's IT services. One important IT service provided by DOA is the development and maintenance of the accounting and payroll computer systems for the State of Wisconsin. DOA implemented a new enterprise resource planning system, called STAR, in three phases between October 1, 2015, and July 1, 2016.

ITESC, which consists of the State of Wisconsin Chief Information Officer and the deputy secretaries of the departments of Administration, Children and Families, Corrections, Health Services, Natural Resources, Revenue, Transportation, Workforce Development, and Agriculture, Trade and Consumer Protection was responsible for approving all major decisions during the implementation of STAR. This included policy decisions, such as the decision to consolidate vendor payments; and implementation decisions, such as the decision to approve or deny each requested customization to STAR.

To provide proper internal control, IT security policies and procedures are necessary to ensure data stored and processed in STAR are protected from accidental or intentional misuse or destruction. IT controls should be established to prevent inappropriate or inadvertent access to STAR and its related databases and to provide staff with a consistent methodology for

performing their job functions. Finally, the NIST *Special Publication 800-53r4* discusses the importance of creating policies and procedures, ensuring proper separation of duties, and maintaining a standard for access that seeks to provide least privilege for a user, which requires that only the minimum necessary rights are assigned to complete a task.

***Condition:***

As part of our audit of STAR for the State of Wisconsin's financial statement audit for FY 2015-16, we reported weaknesses in policies, standards, and procedures related to security. We made recommendations for DOA to develop a timeline and plans by June 30, 2017, for:

- developing policies, standards, and procedures over security administration;
- ensuring controls over the administration of access conform to the policies, standards, and procedures;
- completing a comprehensive review of access, limiting or adjusting access as necessary, and implementing compensating controls when separation of duties cannot be adequately achieved; and
- providing for regular review and updates to the policies, standards, and procedures to ensure a well-controlled environment.

In addition, we recommended DOA implement its plan and report quarterly on its progress to ITESC.

In response to our prior-year recommendations, the DOA STAR Program Office adopted the security administration policies developed by DOA DET in the DET *IT Security Policy Handbook*. These policies are based on the NIST security framework.

In addition, DOA developed security procedures in the *STAR Security Administration Handbook*, which was implemented on June 19, 2017. We performed a limited evaluation and testing of the new procedures since they were implemented at the end of our audit period. In many of the areas of testing during our FY 2016-17 audit, we noted that DOA had taken steps to reduce the excessive or inappropriate access identified during the prior-year audit. However, we continued to identify concerns with security administration for STAR Finance, STAR HCM, and the related databases. We determined that the detailed results of our review were too sensitive to communicate publicly. Therefore, we communicated the results in confidential interim memoranda to DOA SCO and the DOA STAR Program Office.

***Questioned Costs:***

None.

***Context:***

We completed testing of security administration over the STAR Finance and STAR HCM applications and the related databases. We interviewed staff in the DOA STAR Program Office, DOA SCO, and the DOA Division of Personnel Management to gain an understanding of the security administration policies and procedures, and the steps taken to address prior-year

recommendations. In addition, we performed queries to test access to accounts and roles in STAR, and we requested documentation to test in other areas of security administration.

STAR functions include processing vendor payments, accounting for cash receipts, tracking and maintaining employee information, tracking employee time, and processing payroll. STAR is used by SCO and most state agencies to report financial information, monitor budgets, administer federal grants, process payroll, process transactions, and manage assets.

***Effect:***

Although it can be difficult to determine how IT concerns such as those we identified affect the financial statements and material federal compliance areas, ineffective general IT controls in areas such as these may permit controls over individual systems to operate improperly and may allow financial statement misstatements and noncompliance to occur and not be detected.

Weaknesses in IT security controls increase the risk that unauthorized or erroneous transactions could be processed or changes could be made to accounting, payroll, and other data. In addition, failure to provide an appropriate level of protection for systems and data increases the risk that personally identifiable information could be accidentally or maliciously exposed.

***Cause:***

DOA continues to develop its procedures and controls over the STAR environment. It has not prioritized a comprehensive review of security, which will be important to ensuring access is appropriate in the STAR environment. Further, a focused effort on the development of controls and procedures to align with the DET policies it has adopted will strengthen STAR security.

**☑ Recommendation**

*We recommend the Wisconsin Department of Administration:*

- *develop and implement procedures for a review of access by March 30, 2018, including access by users, STAR Program Office staff, and system accounts; adjust access as appropriate as a result of the reviews; and maintain documentation of the access reviews;*

- *by June 29, 2018, establish a plan and timeline to review its security practices and settings for STAR, document procedures and ensure controls over the applications conform to the policies in the Division of Enterprise Technology IT Security Policy Handbook, and document justifications for any exemptions from the established policies; and*

- *take corrective actions related to the specific recommendations in the confidential interim memoranda provided during the audit.*

**Response from the Wisconsin Department of Administration:** The Department of Administration agrees with the recommendations.

**Corrective Action Plan from the Wisconsin Department of Administration:** This is to provide the Department of Administration's (DOA's) Corrective Action Plan to address the concerns raised in

Finding 2017-007: STAR Security Concerns. Below are the specific recommendations of the Legislative Audit Bureau (LAB), and the corresponding DOA corrective actions. Thank you for bringing these matters to my attention.

LAB Recommendation #1
Develop and implement procedures for a review of access by March 30, 2018, including access by users, STAR Program Office staff, and system accounts; adjust access as appropriate as a result of the reviews; and prepare and maintain documentation of the access reviews.

DOA Corrective Actions
No later than March 30, 2018, DOA will develop and implement procedures for a review of STAR system access including access by users, STAR Program Office staff, and system accounts; adjust access as appropriate as a result of the reviews; and prepare and maintain documentation of the access reviews.

LAB Recommendation #2
By June 29, 2018, establish a plan and timeline to review its security practices and settings for STAR, document procedures and ensure controls over the applications conform to the policies in the DET IT Security Policy Handbook, and document justifications for any exemptions from the established policies.

DOA Corrective Actions
No later than June 29, 2018, DOA shall establish a plan and timeline to review its security practices and settings for STAR, document procedures and ensure controls over the applications confirm to the policies in the DET IT Security Policy Handbook, and document justifications for any exemptions from the established policies.

LAB Recommendation #3
Take corrective actions related to the specific recommendations in the confidential interim memoranda provided during the audit.

DOA Corrective Actions
DOA will take corrective actions related to the specific recommendations in the confidential interim memoranda provided during the audit.

---

## Finding 2017-008: Financial Reporting for Capital Assets at the Department of Transportation

*Criteria:*

Generally accepted accounting principles (GAAP) require capital assets of governmental funds to be reported in the government-wide statement of net position. This statement includes those capital assets for which the DOT is responsible, such as infrastructure and land. To properly report capital assets, DOT must analyze a variety of data related to expenditures incurred during the year, disposals that occurred during the year, and projects in progress or completed during the year. Such analyses help DOT to determine the items that should be capitalized and to assess the classification of these items for financial reporting purposes based on GAAP requirements.

The determination of capital asset amounts to be reported is considered to be an estimate, and the analyses completed to produce this estimate are complex. Producing this estimate was further complicated for FY 2016-17 because DOT implemented the State's enterprise resource planning system, STAR, for FY 2016-17. Completing the analyses needed for financial reporting purposes required DOT, for the first time, to obtain appropriate data from STAR and determine how to properly use this data.

***Condition:***

DOT did not sufficiently understand the process for completing the analyses and how its components related to the determination and reporting of capital assets amounts for financial reporting purposes. In determining the capital assets amounts for FY 2016-17, DOT did not appropriately analyze data, determine the items that should be capitalized, or assess the classification of these items. This resulted in a variety of errors in the completed analyses, including:

- expenditures for land purchases during the current year should have been capitalized but were not;
- only current year expenditures were capitalized for projects that had been in progress and were considered to be completed during the year when the total expenditures for those projects should have been capitalized;
- amounts that should have been classified as bridge assets were instead classified as road assets; and
- amounts for projects were expensed during the year when the projects remained in progress.

***Questioned Costs:***

None.

***Context:***

DOT submits financial information to DOA SCO, which is responsible for preparing the State's CAFR. The Statement of Net Position included in the CAFR reports capital assets for governmental activities of $24.0 billion for FY 2016-17, of which approximately $20.3 billion represents capital assets reported by DOT. Our review focused on the analyses DOT completed to determine the items to report as capital assets and assess the classification of these items for financial reporting purposes. DOT's analyses are complicated because of the many long-term projects that maintain existing capital assets, result in new capital assets, or are not considered to be capital assets for financial reporting purposes. For capitalized assets, DOT's assessment of which asset classification applies, such as land, roads, or bridges, involves communication among various DOT staff and some level of judgment.

*Effect:*

Errors that we identified in the amounts reported for capital assets for Governmental Activities on the Statement of Net Position included:

- infrastructure assets were understated by $112.9 million because ongoing projects completed during the year were not capitalized;
- infrastructure assets were overstated by $13.2 million because assets were considered to be disposed of during the year but were not;
- other nondepreciable assets were understated by $11.9 million because ongoing projects were considered to be disposed of during the year when they should not have been;
- other nondepreciable assets were understated by $8.2 million because expenditures were not identified as being related to projects in progress that would be capitalized;
- other nondepreciable assets were overstated by $6.5 million because projects that should have been disposed of during the year were not; and
- other nondepreciable assets were understated by $1.1 million because land purchases during the year were not appropriately capitalized.

In addition, although it did not affect the capital assets amounts reported in the financial statements, DOT inaccurately classified $27.2 million as bridges that should have been classified as roads.

DOT corrected the $112.9 million understatement of infrastructure in the FY 2016-17 financial statements and plans to correct for the other less significant errors when financial reporting information is prepared for FY 2017-18. However, because of the concerns identified related to DOT's completion of the analyses, there is increased potential that additional errors exist and were not identified.

*Cause:*

Although multiple factors contributed to DOT's inaccurate analyses and preparation of financial reporting information related to capital assets, DOT may not have adequately planned for some of these factors. As noted, DOT needed to obtain, for the first time, much of the data required to complete its analyses from STAR. DOT also experienced turnover, including in positions key to completing the analyses and preparing the financial information related to capital assets. In addition, DOT's written documentation for completing the analyses and preparing the financial information was not adequate to enable staff to successfully complete the analyses. The existing documentation had also not been updated to reflect DOT's use of STAR. DOT staff also indicated that there was not sufficient time for the analyses and financial information prepared to be adequately reviewed due to pressure from DOA to submit the required information. These circumstances were further exacerbated because DOT used multiple spreadsheets to analyze the data and prepare the financial information and automation was not used to link information among them when applicable.

## ☑ Recommendation

*We recommend the Wisconsin Department of Transportation take steps to improve financial reporting for capital assets, including:*

- *updating, by May 31, 2018, its written documentation related to preparing the financial information, including documentation related to completing the underlying analyses as well as identification and incorporation of checks for reasonableness;*

- *training staff responsible for completing the analyses and preparing the financial information in order to ensure these staff understand the work overall and the relevance and relationship of each component of the work to the work overall;*

- *establishing and documenting a secondary review process of the analyses and the financial information prepared; and*

- *automating the analyses and preparation of the financial information, where possible.*

**Response from the Wisconsin Department of Transportation:** We agree with the recommendations as written.

**Corrective Action Plan from the Wisconsin Department of Transportation:** This is to provide the Department of Transportation's (WisDOT's) Corrective Action Plan to address findings regarding Financial Reporting for Capital Assets. Below are specific recommendations of the Legislative Audit Bureau (LAB) and the corresponding WisDOT corrective actions.

LAB Recommendation #1
Update written documentation by May 31, 2018 related to preparing the financial information, including documentation related to completing the underlying analyses as well as identification and incorporation of checks for reasonableness.

WisDOT Corrective Actions
No later than May 31, 2018, WisDOT will update written documentation related to preparing the financial information and completing the underlying analyses. WisDOT will also identify and incorporate checks for reasonableness into documentation.

LAB Recommendation #2
Training staff responsible for completing the analyses and preparing the financial information in order to ensure these staff understand the work overall and the relevance and relationship of each component of the work to the work overall.

WisDOT Corrective Actions
No later than September 1, 2018, WisDOT will train staff responsible for preparing the financial information and completing the analyses. Training will ensure staff understand the relationship of each component to the work overall. Training will also include the secondary review process identified in LAB Recommendation #3.

LAB Recommendation #3
Establishing and documenting a secondary review process of the analyses and the financial information prepared.

WisDOT Corrective Actions
No later than May 31, 2018, WisDOT will establish and document a secondary review process.

LAB Recommendation #4
Automating the analyses and preparation of the financial information, where possible.

WisDOT Corrective Actions
WisDOT will look at current processes and identify opportunities to automate the preparation of financial information, where possible. Any automations identified will be implemented by September 1, 2018.

---

## Finding 2017-009: Department of Transportation Use of Project Costing Data

*Criteria:*

DOT first implemented the State's enterprise resource planning system, STAR, for FY 2016-17, and several conversion entries were made to bring financial information into STAR. STAR is made up of multiple modules that serve different purposes. For example, the STAR general ledger (GL) module maintains information about expenditure and other transactions on a fiscal year basis. Another STAR module, project costing (PC), maintains information about activity related to particular projects. Although the PC module also includes expenditure information, it was designed to track activity on a life-to-date basis for a project and not specifically on a fiscal year basis for financial reporting purposes. DOA requires DOT to regularly complete reconciliations between STAR modules, including between the GL and PC modules, and resolve variances identified.

Data from the STAR GL module are used by DOA SCO to prepare beginning trial balances. DOT prepares various adjustments that, when added to the beginning trial balance, form the financial statements for the Transportation Fund. In addition, DOT is responsible for preparing other financial information used by SCO in preparing other financial statements and information included in the State's CAFR. For FY 2016-17, DOT prepared certain adjustments and financial information based on data in the PC module. DOT also used data in the PC module for other purposes. It would be expected that DOT would take steps to ensure data obtained from the PC module are reasonable and appropriate for financial reporting or other intended uses, including that it is consistent with data in the GL module.

*Condition:*

DOT did not take sufficient steps to ensure data obtained from the PC module were reasonable and appropriate for financial reporting or other intended uses. We noted three specific areas of concern. First, DOT did not complete reconciliations between the data in the GL and PC modules for May 2017 or June 2017, and did not complete a reconciliation between the data in the GL and PC modules for FY 2016-17 as a whole. Second, DOT did not take steps to ensure the data it

obtained and used from the PC module were reasonable and appropriate for certain financial reporting or other intended uses. Third, DOT performed certain correcting entries in STAR that did not contain sufficient detail to associate them with the relevant projects.

***Questioned Costs:***

None.

***Context:***

DOT determined it would use certain data from the PC module for financial reporting and other purposes because the PC module more readily provided the information that DOT needed. For example, DOT used current year and life-to-date cost data from the PC module to complete its analyses of capital assets. DOT also used data from the PC module to determine the amount of general obligation bond proceeds to request. We gained an understanding of DOT's use of data from the PC module for certain financial reporting and other purposes and assessed the reasonableness of DOT's use of data from the PC module.

***Effect:***

DOT cannot be assured that data obtained from the PC module were appropriate and accurate for financial reporting or other purposes. Without such assurance, adjustments and other financial or other information derived from these data could be incorrect. For example, financial statement amounts could be misstated or the amount of general obligation bond proceeds requested may not be appropriate.

***Cause:***

Multiple factors may have contributed to DOT not taking sufficient steps to ensure data obtained from the PC module were reasonable and appropriate for its intended uses. As noted, DOT implemented STAR and used STAR data for the first time for FY 2016-17. DOT made corrections to its conversion entries in STAR, but did not include sufficient detail when processing these entries. DOT worked with consultant experts during the year, but the consultants left prior to DOT preparing all of the adjustments and financial reporting information. DOT also experienced turnover of various staff, including accounting staff. In addition, DOT indicated that priority was placed on completing year-end procedures for the GL over completing the May and June 2017 reconciliations between data in the GL and PC modules because GL data would be used for financial reporting. Further, it was not clear whether DOT had fully realized the importance of ensuring that the data obtained from the PC module were appropriate to use for financial reporting purposes.

**☑ Recommendation**

*We recommend the Wisconsin Department of Transportation take steps to ensure data obtained from the project costing module are reasonable and appropriate for financial reporting or other intended uses. At a minimum, these steps should include regularly completing reconciliations between data in the project costing and general ledger modules, further correcting the conversion entries to include the relevant project-level detail, and assessing the reasonableness and appropriateness of data used from the project costing module.*

**Response from the Wisconsin Department of Transportation:** We agree with the recommendations as written.

**Corrective Action Plan from the Wisconsin Department of Transportation:** This is to provide the Department of Transportation's (WisDOT's) Corrective Action Plan to address findings regarding Use of Project Costing Data. Below are specific recommendations of the Legislative Audit Bureau (LAB) and the corresponding WisDOT corrective actions.

LAB Recommendation #1
Ensure data obtained from the project costing module is reasonable and appropriate for financial reporting or other intended uses. At a minimum, these steps should include regularly completing reconciliations between data in the project costing and general ledger modules, further correcting the conversion entries to include the relevant project-level detail, and assessing the reasonableness and appropriateness of data used from the project costing module.

WisDOT Corrective Actions
WisDOT will implement a monthly check to ensure monthly project costing to general ledger module reconciliations are completed as well as the year-end reconciliation. By May 31, 2018, WisDOT will complete the correction of conversion entries with DOA to include the relevant project-level detail. WisDOT will also work to assess the reasonableness and appropriateness of data used from the project costing module.

■ ■ ■ ■