Office of the Auditor General
Performance Audit Report

Central Reservation System for Recreational Resources

Department of Natural Resources

August 2016

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

751-0591-16

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit
Central Reservation System (CRS) for Recreational Resources
Department of Natural Resources (DNR)

Report Number:
751-0591-16

Released:
August 2016

CRS is a commercial off-the-shelf software purchased by DNR to allow individuals to reserve State campground and harbor sites for lodging or other recreational activities. CRS manages the daily inventory of over 14,500 campsites, lodges, and harbor slips with over one million nights reserved annually. Customers can make reservations via the Internet, by telephone, or at State parks. CRS is also used at State parks to process payments for goods and services made by cash, credit card, and e-check. During fiscal years 2014 and 2015, CRS processed gross sales of $41.2 million and $48.4 million, respectively.

Audit Objective			**Conclusion**
Objective #1: To assess the effectiveness of DNR's access controls over CRS.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
DNR did not fully establish and implement access controls over CRS, increasing the risk of unauthorized access, use, and modification of CRS data. Eleven (27%) of 41 selected users had access rights in excess of those necessary to perform their jobs. Thirteen (32%) of the 41 users no longer needed access (Finding #1).		X	Agrees

Audit Objective			**Conclusion**
Objective #2: To assess the effectiveness of DNR's application controls over CRS.			Effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
DNR did not require the CRS vendor to conduct and provide a Service Organization Controls (SOC) 1, type 2 report in accordance with the CRS contract (Finding #2).		X	Agrees

A copy of the full report can be
obtained by calling 517.334.8050
or by visiting our Web site at:
www.audgen.michigan.gov

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

OAG
Office of the Auditor General
Doug A. Ringler, CPA, CIA
Auditor General
201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • www.audgen.michigan.gov

August 23, 2016

Mr. Keith Creagh, Director
Department of Natural Resources
Constitution Hall
Lansing, Michigan

Dear Mr. Creagh:

I am pleased to provide this performance audit report on the Central Reservation System for Recreational Resources, Department of Natural Resources.

We organize our findings and observations by audit objective. Your agency provided preliminary responses to the recommendations at the end of our fieldwork. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and submit it within 60 days of the date above to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

TABLE OF CONTENTS

CENTRAL RESERVATION SYSTEM FOR RECREATIONAL RESOURCES

INTENTIONALLY BLANK PAGE

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

ACCESS CONTROLS OVER CRS

BACKGROUND

Department of Natural Resources (DNR) staff, vendor staff, and customers use the Central Reservation System (CRS) to reserve State campground and harbor sites for lodging and other recreational activities.

Access controls* limit or detect inappropriate access, which is important to ensure the availability, confidentiality, and integrity of data.

The Federal Information System Controls Audit Manual* (FISCAM) is a methodology developed by the U.S. Government Accountability Office (GAO) for performing information system control audits of governmental entities in accordance with professional standards.

AUDIT OBJECTIVE

To assess the effectiveness* of DNR's access controls over CRS.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- CRS contains moderately sensitive data.
- DNR established and implemented authentication controls in accordance with State policy, such as password complexity requirements and user account lockout after 5 invalid log-in attempts.
- Reportable condition* related to improved CRS access controls (Finding #1).

** See glossary at end of report for definition.*

FINDING #1

Improvements are needed to CRS access controls.

DNR did not fully establish and implement access controls over CRS, increasing the risk of unauthorized access, use, and modification of CRS data.

FISCAM states that user access should be limited to individuals with a valid business purpose, access authorization forms should be maintained, access rights should prevent conflicting transactions and activities, and system owners and security* managers should periodically monitor user access.

DNR did not:

a. Use standard authorization forms to document business owner approval of the specific access rights granted to users.

   Documenting this authorization helps ensure that only appropriate individuals obtain access and that the rights assigned are appropriate.

b. Employ the principle of least privilege* as required by Department of Technology, Management, and Budget (DTMB) Technical Standard 1335.00.03.

   We selected 41 CRS users and noted that 11 (27%) were granted rights in excess of those necessary to perform their jobs. In addition, 13 (32%) of the 41 users were not current DNR, vendor, or municipal employees and no longer needed access to CRS.

c. Deactivate accounts of departed users in a timely manner as required by DTMB Technical Standard 1335.00.03.

   Of 40 CRS users selected from a population of user accounts deactivated during our audit period, DNR took between 7 and 295 days to deactivate 21 (53%) of the accounts, with an average of 24 days. Promptly deactivating the accounts of departed users helps ensure that only authorized personnel have access to CRS.

d. Ensure segregation of duties* through the proper assignment of access rights as required by DTMB Technical Standard 1335.00.03.

   We reviewed 13 central office users and determined that 7 (54%) had been granted access rights that conflict with their assigned job functions. Effective segregation of duties helps prevent the possibility that a single person could be responsible for critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner.

** See glossary at end of report for definition.*

e. Routinely monitor audit logs for inappropriate user account modifications in accordance with DTMB Technical Standard 1335.00.03.

   DNR informed us that its review of audit logs, which tracks user account modifications, is limited to undocumented periodic spot checks. Without routinely monitoring audit logs, inappropriate user account changes may go undetected.

f. Periodically review user access rights every 120 days in accordance with DTMB Technical Standard 1335.00.03 to ensure that rights remain appropriate.

   DNR informed us that user access is reviewed by the field administrators biannually. However, DNR did not formally document its review.

RECOMMENDATION

We recommend that DNR fully establish and implement access controls over CRS.

AGENCY PRELIMINARY RESPONSE

DNR provided us with the following response:

DNR agrees with the recommendation to establish and implement access controls over CRS and will seek to implement the controls over the next year.

APPLICATION CONTROLS OVER CRS

BACKGROUND

Application controls* help to ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

AUDIT OBJECTIVE

To assess the effectiveness of DNR's application controls over CRS.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- CRS application and Web portal contained edit checks to ensure that only complete and valid data was input into CRS.
- DNR established and implemented data processing controls, which ensured the completeness and accuracy of data processed through CRS.
- DNR established and implemented data output controls, which ensured the completeness and accuracy of data output from CRS.
- Reportable condition related to the need for a Service Organization Controls (SOC) 1, type 2 report (Finding #2).

** See glossary at end of report for definition.*

FINDING #2

DNR did not require the CRS vendor to conduct and provide a SOC 1*, type 2 report in accordance with the CRS contract.

SOC 1, type 2 report needed.

SOC reports are internal control* reports on the services provided by a service organization and provide valuable information that users need to assess and address the risks associated with an outsourced service. A SOC 1, type 1 engagement is conducted by an independent auditor to report on management's description of a service organization's system and the suitability of the design of controls. The auditor may also test and report on the operating effectiveness of those controls, which results in a type 2 engagement.

DNR should require that the vendor employ an independent auditing firm to annually conduct a SOC 1, type 2 attestation engagement.

The CRS contract requires that the vendor employ an independent auditing firm to annually conduct a SOC 1, type 2 attestation engagement. The contract requires that the vendor obtain an auditor's opinion regarding whether the vendor's description of its system was fairly presented, internal control over financial reporting was suitably designed to achieve the related control objectives, and controls were operating effectively. The contract also specifies that the State reserves the right to request the vendor to employ an independent firm to conduct a SOC 2*, type 2 engagement if CRS experiences any form of data breach, becomes unavailable, or experiences processing integrity issues that jeopardize the State or its customers.

Although DNR received a SOC 1 report, the report did not include an auditor's opinion regarding the operating effectiveness of the controls, which is a key component of a SOC 1, type 2 report.

DNR should require the vendor to annually conduct a SOC 1, type 2 engagement. In addition, DNR should periodically assess the need to request a SOC 2, type 2 report, which would provide an assessment of the security, availability, processing integrity, confidentiality, and privacy of CRS.

RECOMMENDATION

We recommend that DNR require the CRS vendor to conduct and provide a SOC 1, type 2 report in accordance with the CRS contract.

AGENCY PRELIMINARY RESPONSE

DNR provided us with the following response:

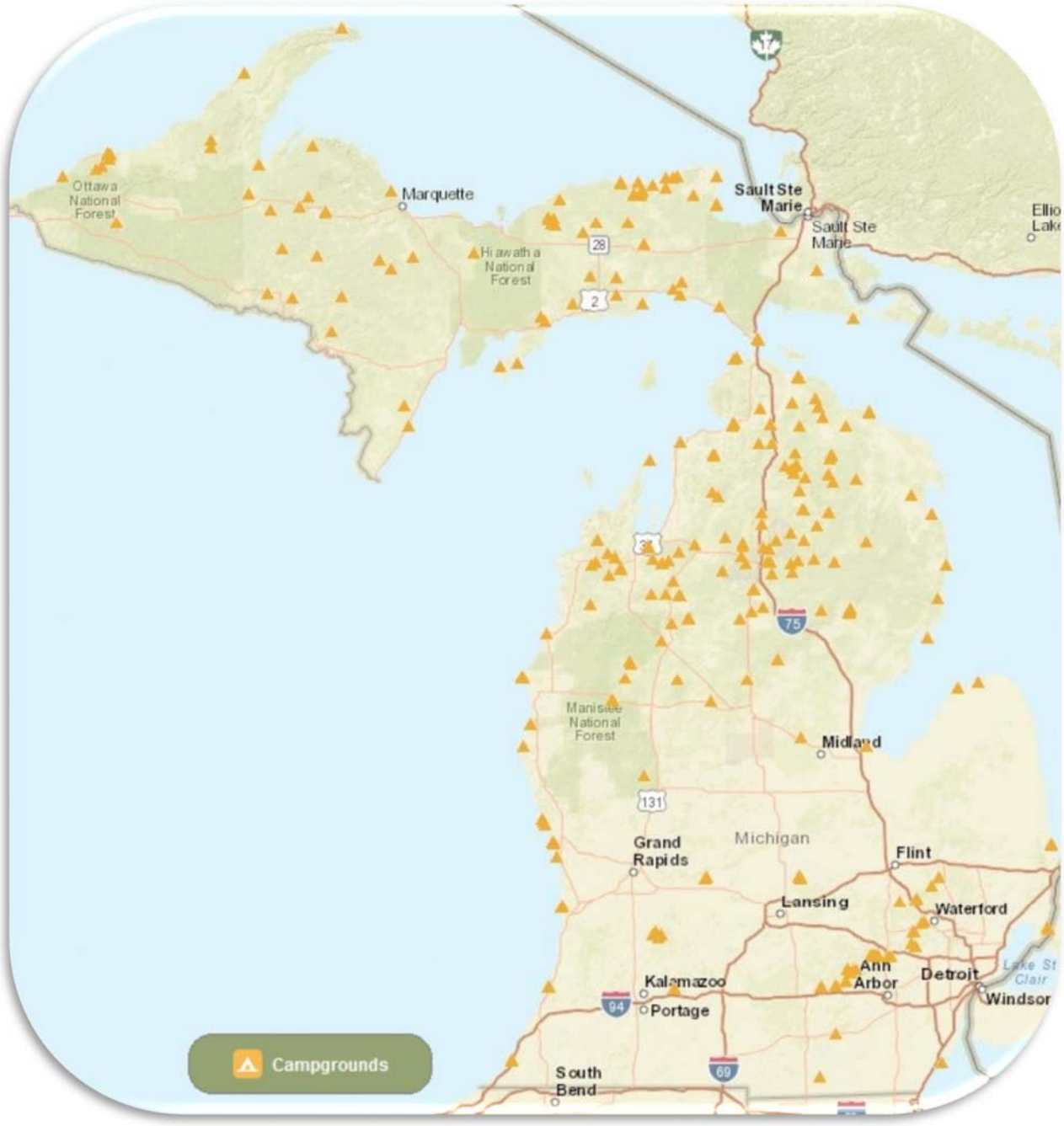
DNR agrees with the recommendation to require the CRS vendor to conduct and provide a SOC 1 type 2 report within the next available review cycle.

** See glossary at end of report for definition.*

SUPPLEMENTAL INFORMATION

UNAUDITED
Exhibit #1

CENTRAL RESERVATION SYSTEM
Department of Natural Resources
Map of State Campgrounds
As of April 2016



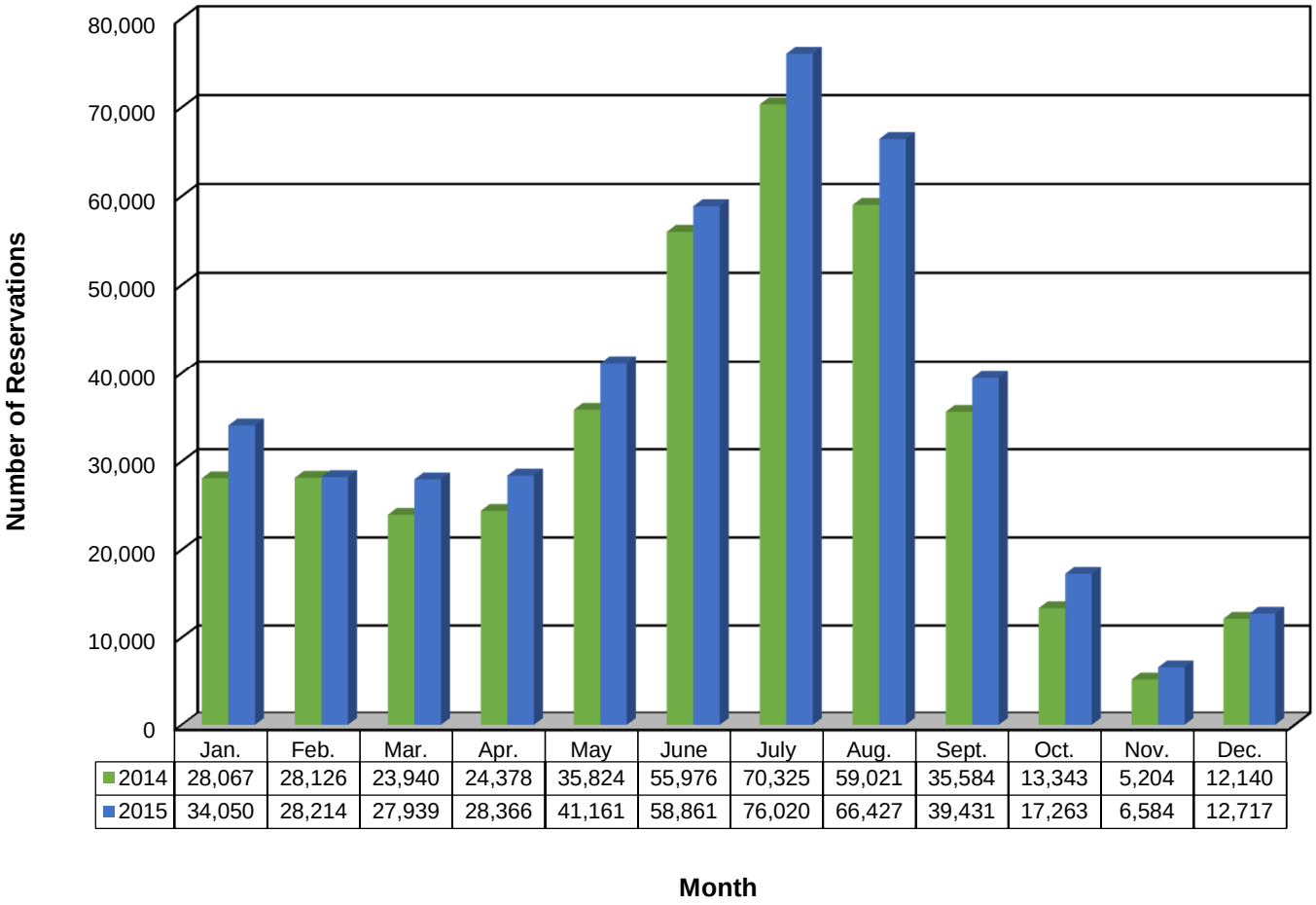
Source: www.michigan.gov/dnr/

CENTRAL RESERVATION SYSTEM
Department of Natural Resources
Map of State Harbors
As of April 2016

Source: www.michigan.gov/dnr/

UNAUDITED
Exhibit #3

CENTRAL RESERVATION SYSTEM
Department of Natural Resources
Number of Reservations by Month
Calendar Years 2014 and 2015



	Jan.	Feb.	Mar.	Apr.	May	June	July	Aug.	Sept.	Oct.	Nov.	Dec.
2014	28,067	28,126	23,940	24,378	35,824	55,976	70,325	59,021	35,584	13,343	5,204	12,140
2015	34,050	28,214	27,939	28,366	41,161	58,861	76,020	66,427	39,431	17,263	6,584	12,717

Source: The Office of the Auditor General prepared this exhibit using data obtained from CRS.

SYSTEM DESCRIPTION

CRS was purchased by DNR to allow individuals to reserve State campground and harbor sites for lodging or other recreational activities. The application is utilized by over 900 State, vendor, and municipal employees.

A daily inventory of over 14,500 campsites, lodges, and harbor slips are managed through CRS. Customers can make reservations via the Internet, by telephone, or at State parks with over one million nights reserved annually.

CRS is also used at State parks to process payments for goods and services made by cash, credit card, check, e-check, and gift card. During fiscal years 2014 and 2015, CRS processed gross sales of $41.2 million and $48.4 million, respectively.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the program and other records of DNR's Central Reservation System. We conducted this performance audit* in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered the period October 1, 2013 through April 30, 2016.

METHODOLOGY

We conducted a preliminary survey of CRS to formulate a basis for defining our audit objectives and scope. This included gaining an understanding of DTMB policies and procedures for State of Michigan information technology systems. During our preliminary survey, we:

- Interviewed DNR management and staff to obtain an understanding and a walk-through of CRS.
- Reviewed DNR and DTMB access and application control policies applicable to CRS.
- Reviewed system documentation.
- Reviewed the vendor's SOC 1 report for CRS.
- Obtained an understanding of DNR's processes for:
    - Granting user access to CRS.
    - Determining what roles/privileges are assigned to users.
    - Ensuring data output from CRS is complete and accurate.

** See glossary at end of report for definition.*

OBJECTIVE #1

To assess the effectiveness of DNR's access controls over CRS.

To accomplish this objective, we:

- Performed site visits at select State parks and harbors to obtain an understanding of how user access is controlled at each location.
- Obtained a list of active CRS users and assessed whether:
    - Access authorization procedures and authentication parameters complied with DTMB policy.
    - DNR periodically recertified active user accounts.
    - Roles and privileges assigned to users employed the principle of least privilege.
    - Segregation of duties was maintained through assigned access authorizations.
- Obtained a list of inactive CRS users and assessed whether access was promptly deactivated after user departure.

OBJECTIVE #2

To assess the effectiveness of DNR's application controls over CRS.

To accomplish this objective, we:

- Validated that edit checks for the CRS application and Web portal ensured that only complete and valid data was accepted as an input to the system.
- Reviewed select reservation and sales transactions to ensure that CRS accurately calculated the sales amount in accordance with DNR published rate tables.
- Validated that select reservation business rules were properly enforced by CRS.
- Reviewed reconciliations of electronic payment data output from CRS for completeness and accuracy.
- Validated select cash deposit reports from CRS with bank deposit slips to ensure completeness and accuracy.

CONCLUSIONS

We base our conclusions on our audit efforts and the resulting material conditions* and reportable conditions.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve State government operations. Consequently, we prepare our performance audit reports on an exception basis.

AGENCY RESPONSES

Our audit report contains 2 findings and 2 corresponding recommendations. DNR's preliminary response indicates that it agrees with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion at the end of our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

SUPPLEMENTAL INFORMATION

Our audit report includes supplemental information that relates to our audit objectives (Exhibits #1 through #3). Our audit was not directed toward expressing a conclusion on this information.

** See glossary at end of report for definition.*

GLOSSARY OF ABBREVIATIONS AND TERMS

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
application controls	Controls that are directly related to individual computer applications. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.
CRS	Central Reservation System.
DNR	Department of Natural Resources.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
Federal Information System Controls Audit Manual (FISCAM)	A methodology published by the U.S. Government Accountability Office (GAO) for performing information system control audits of federal and other governmental entities in accordance with *Government Auditing Standards*.
internal control	The organization, policies, and procedures adopted by management and other personnel to provide reasonable assurance that operations, including the use of resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of assets against unauthorized acquisition, use, or disposition.
material condition	A matter that, in the auditor's judgment, is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.
performance audit	An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and

	operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.
principle of least privilege	The practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.
reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
segregation of duties	Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.
SOC 1 report	A report prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16 in which an independent auditor reports on management's description of a service organization's system and the suitability of the design of controls (a type 1 report). The auditor may be engaged to also test and report on the operating effectiveness of those controls (a type 2 report).
SOC 2 report	A report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy in which an independent auditor reports on management's description of a service organization's system and the suitability of the design of controls (a type 1 report). The auditor may be engaged to also test and report on the operating effectiveness of those controls (a type 2 report).

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank


OAG
Office of the Auditor General
Independent
Objective
Transparent