Audit of the Information Security of the Colorado Operations Resource Engine (CORE) System

Information Technology Performance Audit
Public Report
April 25, 2016
Myers and Stauffer LC

MYERS AND STAUFFER LC
CERTIFIED PUBLIC ACCOUNTANTS

THE MISSION OF THE OFFICE OF THE STATE AUDITOR
IS TO IMPROVE GOVERNMENT
FOR THE PEOPLE OF COLORADO

LEGISLATIVE AUDIT COMMITTEE

Representative Dan Nordberg – Chair	Representative Su Ryden – Vice-Chair
Senator Morgan Carroll	Senator Tim Neville
Senator Chris Holbert	Representative Dianne Primavera
Senator Cheri Jahn	Representative Lori Saine

OFFICE OF THE STATE AUDITOR

Dianne E. Ray	State Auditor
Matt Devlin	Deputy State Auditor
Cindi Radke	Audit Manager
Myers and Stauffer, LC	Contractor

AN ELECTRONIC VERSION OF THIS REPORT IS AVAILABLE AT
WWW.STATE.CO.US/AUDITOR

A BOUND REPORT MAY BE OBTAINED BY CALLING THE
OFFICE OF THE STATE AUDITOR
303.869.2800

PLEASE REFER TO REPORT NUMBER 1549P WHEN REQUESTING THIS REPORT

MYERS AND STAUFFER LC
CERTIFIED PUBLIC ACCOUNTANTS

April 25, 2016

Members of the Legislative Audit Committee:

This report contains the results of an information technology performance audit of the Information Security of the Colorado Operations Resource Engine (CORE) System. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Governor's Office of Information Technology and the Department of Personnel & Administration/Office of the State Controller.

We conducted this information technology 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. However, we were not able to fully address one of our audit objectives, which was to "assess the risk areas and control gaps noted from the gap assessment to determine whether the State's information security policy requirements have been designed, implemented, and are operating effectively within the CORE system environment managed by CGI" due to a scope limitation on the shared infrastructure systems we were allowed to assess because of security concerns and restrictions imposed by the CORE third-party service provider.

During our audit work, we identified certain matters that are not included in this audit report that were reported to the Governor's Office of Information Technology and Department of Personnel & Administration/Office of the State Controller management in a separate confidential report dated April 25, 2016. These matters were considered sensitive to protecting state information technology assets.

Myers and Stauffer LC

Myers and Stauffer, LC
Austin, Texas

11044 Research Blvd, Ste C-500 | Austin, TX 78759
PH 512.342.0800 | FX 512.342.0820
www.mslc.com

TABLE OF CONTENTS

REPORT HIGHLIGHTS

AUDIT OF THE INFORMATION SECURITY OF THE COLORADO OPERATIONS RESOURCE ENGINE (CORE) SYSTEM
IT PERFORMANCE AUDIT, APRIL 2016

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY (OIT)
DEPARTMENT OF PERSONNEL & ADMINISTRATION/OFFICE OF THE STATE CONTROLLER (DPA/OSC)

AUDIT CONCERN

The Governor's Office of Information Technology needs to hold the CORE contractor accountable for compliance with Colorado Information Security Policies.

KEY FACTS AND FINDINGS

- OIT is not holding the Contractor accountable for compliance with the Colorado Information Security Policies as required by security policy and as directed by the State Chief Information Security Officer.

BACKGROUND

Governor's Office of Information Technology (OIT):

- Centralized the management of Executive Branch information technology resources, including IT staff.
- Is responsible for documenting policies, procedures, and guidelines for IT services.
- Contracted with CGI, a third-party service provider, for the CORE application and supporting services.

Department of Personnel & Administration/Office of the State Controller (DPA/OSC):

- OSC is a division of DPA that provides statewide accounting, purchasing, and contracting services including providing daily support of CORE, the State's enterprise financial system.
- DPA has the lead role for providing oversight of CGI.

OUR RECOMMENDATIONS

The Governor's Office of Information Technology should:

- Amend the contract as necessary to clearly and unambiguously state that the contractor is required to comply with all current and future updated State of Colorado Information Security Policies.
- Ensure it has a process and effective mechanism in place to assess CGI for compliance with the Security Policies including ensuring that CGI's policies and procedures for CORE comply with the Security Policies.
- Amend the CGI contract as necessary to assign DPA/OSC primary responsibility for contract oversight, while stipulating that OIT should continue to ensure compliance with the Security Policies.

FOR FURTHER INFORMATION ABOUT THIS REPORT, CONTACT THE OFFICE OF THE STATE AUDITOR
303.869.2800 – WWW.STATE.CO.US/AUDITOR

CHAPTER 1

OVERVIEW OF COLORADO OPERATIONS RESOURCE ENGINE (CORE)

CORE is an integrated financial management system that was implemented in Fiscal Year 2015 as an upgrade and replacement of the Colorado Financial Reporting System (COFRS), which was the State's prior financial system of record since Fiscal Year 1991. CORE was implemented in July 2014 and is the financial system of record for Fiscal Year 2015 and beyond. CORE is used to perform many key state financial and business functions such as recording expenditure transactions, paying vendors, recording payroll, supporting the collection of grant revenues, and recording tax revenues. The CORE system and data are critical to the State's financial reporting and business processes.

CORE had approximately 4,114 active users statewide as of July 26, 2015. During Fiscal Year 2015, CORE processed about $41.3 billion in revenue and about $40.1 billion in expenditures. All state agencies use CORE for processing of financial data except the Colorado Department of Transportation and higher education institutions which have implemented their own accounting systems that interface with CORE and transmit summarized accounting information to CORE.

CORE's business owner, the Department of Personnel & Administration/Office of the State Controller (DPA/OSC), worked with the Governor's Office of Information Technology (OIT) to purchase CORE and replace/upgrade COFRS. In doing so, the State of Colorado purchased and implemented CGI Technologies and Solutions, Inc.'s (CGI) Advantage system to meet the State's financial and business computing needs. OIT executed a contract with CGI which included deliverables to 1) procure the CORE system and 2) implement an ongoing maintenance contract for CORE.

The CORE application is hosted at CGI's Phoenix Data Center (Data Center) with State users within the Colorado State Network connecting to the application through one of two State managed routers. Additionally, authorized users who are not on the Colorado State Network such as higher education institutions, can connect to the CORE application through a secure web application (Zscaler), which is managed by OIT. See Figure 1 below.

CGI and its service auditor annually issue a Service Organization Control 1 (SOC 1), Type 2 report. This Type 2 report is issued in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 16 (SSAE 16). The report focuses on controls at CGI that are relevant to an audit of a user entity's financial statements, and it includes management's description of CGI's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period. Specifically, CGI's SOC 1, Type 2 report covers its Tier 1, Technology Management, services provided at its Data Center only. In addition to supporting the technical infrastructure for the State's CORE system, the Data Center service delivery organization is responsible for the development and delivery of infrastructure services for numerous other clients across the U.S.

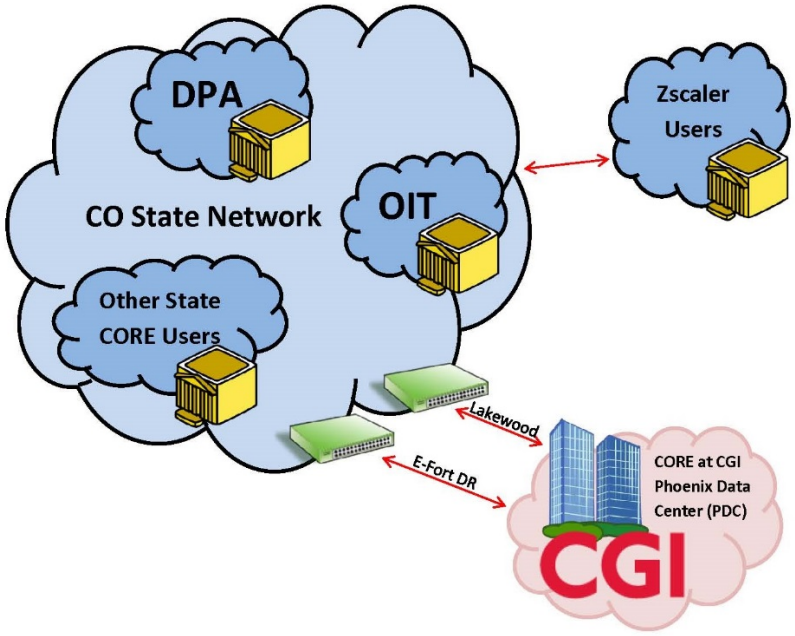

Figure 1 – High Level Depiction of CORE architecture.

While OIT was involved in much of the project management of the CORE implementation, DPA/OSC outlined the business logic, rules, and processes to be incorporated within the new CORE system. Upon CORE implementation in July 2014, DPA/OSC, OIT, and CGI began performing information technology (IT) functions for the CORE system. The Colorado Information Security Policies (CISPs or Security Policies) have been updated since the signing of the CGI CORE contract as illustrated in Figure 2.

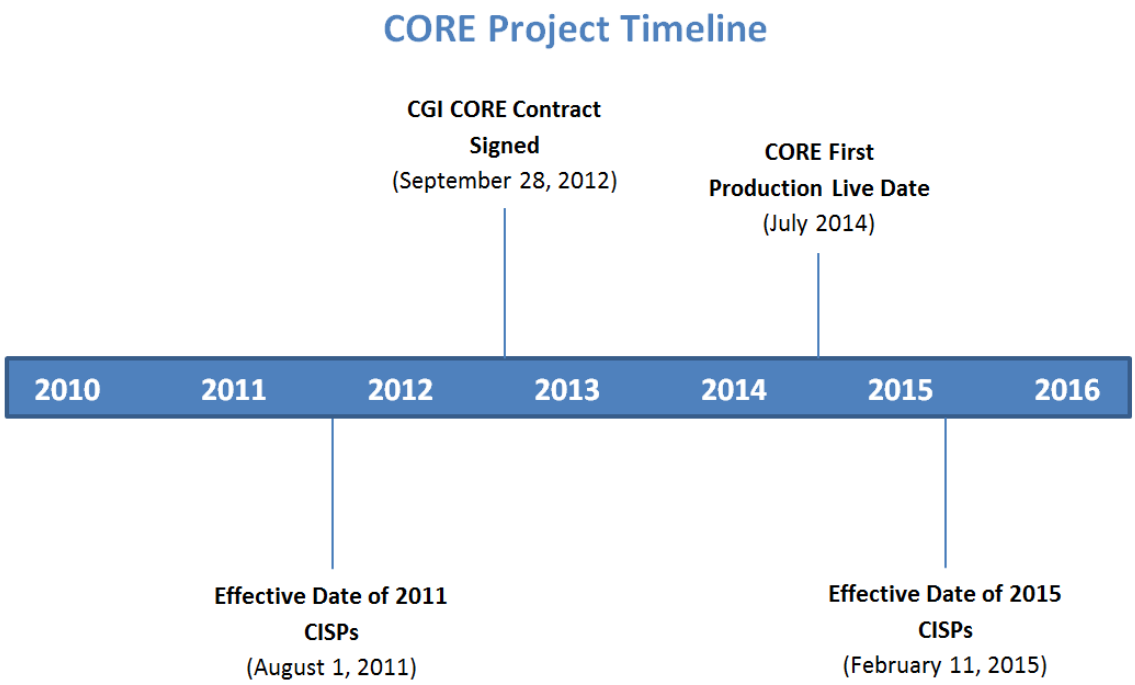

Figure 2 – Project Timeline.

The responsibilities of OIT, DPA/OSC, and CGI for the CORE application are as follows:

OIT	DPA/OSC	CGI
• Manages data interface files exchanged between state systems and CORE. • Manages the network connection between CORE users at state agencies and CGI's communication hardware (router) located at OIT's main data center. • Issues and monitors statewide security policies that must be adhered to by all state agencies and contractors. • Holds CGI accountable for contract deliverables.	• Develops, implements, and updates policies and procedures related to use of CORE, application-level logical access to CORE, and reporting from the CORE system.	• Develops and implements changes to the application software • Hosts the CORE data and manages the primary data center where the CORE data is stored (in Phoenix, AZ). This includes key system infrastructure pieces consisting of the hardware, operating system, and database components. • Maintains physical security of the data center. • Manages the network connection from the router at OIT's main data center (Lakewood) to CGI's data center in Phoenix as well as the OIT backup router located at the Disaster Recovery site (E-fort).

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY (OIT)

The Chief Information Officer (CIO) & Secretary of Technology is responsible for the overall administration of OIT as well as supervising the Chief Information Security Officer (CISO). Colorado statute requires the CIO to coordinate and direct the development, communication, and enforcement of policies, standards, specifications, and guidelines for information technology in public agencies, including those related to backup and recovery.

The state's Chief Information Security Officer (CISO) reports to the CIO and is responsible for overseeing the Office of Information Security and the Colorado Information Security Program which includes governance, risk, compliance, and risk management. Statute requires the CISO to develop, update, communicate, and ensure the incorporation of and compliance with information security policies, standards, and guidelines.

DEPARTMENT OF PERSONNEL & ADMINISTRATION/OFFICE OF THE STATE CONTROLLER (DPA/OSC)

The State of Colorado's Department of Personnel & Administration (DPA) provides centralized human resources, information, tools, resources and materials needed for the State of Colorado government to

function. The programs and services provided by DPA are vitally important to the efficient and effective operation of State government.

The Office of the State Controller is a division within DPA. Within this division the CORE Operations group provides daily system and business support of CORE. CORE help desk specialists, functional experts, and system analysts assist customers with resolution of business and system issues related to CORE. The CORE Operations team also works with the system's software vendor to maintain the system and implement new features and upgrades. The team provides communications and training for CORE users and helps foster continuous improvement of the CORE system and overall operations.

CGI GROUP INC. (CGI)

Founded in 1976, CGI is one of the largest IT and business process services providers in the world with 65,000 professionals operating across 40 countries. The CGI Advantage Enterprise Resource Planning (ERP) set of applications is specifically built for government use and complies with Government Accounting Standards Board (GASB) and Generally Accepted Accounting Principles (GAAP). The CGI Advantage ERP suite contains solutions for Financial Management, Performance Budgeting, Human Resource Management, Procurement, and other business functions.

AUDIT PURPOSE, SCOPE, AND METHODOLOGY

We conducted this audit pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. Audit work was performed from September 2015 through March 2016. We acknowledge the cooperation and assistance by staff and management at the Governor's Office of Information Technology, and the Department of Personnel & Administration/Office of the State Controller.

We conducted this IT performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of the audit were to:

1. Assess the State's information security policies, specifically as they apply or relate to CORE, and determine whether the policies and requirements are adequate in fulfilling the State's statutory information security program requirement of ensuring minimum security controls are in place to safeguard communication and information resources supporting the operations of state agencies.
2. Conduct a gap assessment of the CGI information security control environment covered in the SOC 1, Type 2, SSAE 16 report against the State's information security policies to determine risk areas and policy requirements that are not covered in the SOC 1 report.
3. Assess the risk areas and control gaps noted from the gap assessment to determine whether the State's information security policy requirements have been designed, implemented, and are operating effectively within the CORE system environment managed by CGI.
4. Determine whether the State's information security policy requirements have been designed, implemented, and are operating effectively within the CORE system environment managed by the State.
5. Specific to the deficiencies found in the previous bullet, perform a gap analysis against the information security policies in place at the effective date of the CORE contract and the policies in effect as of the date of fieldwork and determine if these deficiencies are related to changes in the State's information security policies.
6. Develop recommendations to address the changes identified with the security policies gap analysis and any other root cause analysis.
7. Determine if the State is holding CGI accountable for complying with the State's information security policies.

We performed the following procedures to accomplish our audit objectives:

- Reviewed relevant state statutes, rules, CGI and agency policies and procedures, and other guidance relevant to the security and operation of the CORE system.
- Interviewed agency management and staff.
- Interviewed contractor management and staff.
- Gathered and analyzed documentation and data.
- Evaluated system processes and documentation against policy requirements.
- Performed tests and observations of system and process controls, including security configurations and procedures for monitoring security such as logging, log reviews, and system alerts.

We planned our audit work to assess the design and effectiveness of security over, and operation of, the CORE application. The primary criteria for the audit was the Security Policies that were effective in 2015. Additionally, for selected findings we assessed the findings against the requirements in the version of the Colorado Information Security Policies that were effective beginning in 2011 to determine if the issue would have been a finding under the previous Security Policies that were in effect when the contract with CGI was signed.

During our audit work, we identified certain matters that are not included in this audit report that were reported to management in a separate confidential report dated April 25, 2016. These matters were considered sensitive to protecting state information technology assets.

SCOPE LIMITATION

We were not able to assess CGI's compliance with certain requirements of the Colorado Information Security Policies due to restrictions on our testing of the CGI managed infrastructure that is used to support the CORE application for the State of Colorado, but is also used to support applications for other CGI clients. For example, we were unable to test CGI's centralized, Windows-based network authentication controls because these controls are used to support other CGI managed client applications in addition to CORE. Therefore, we were not able to fully address one of our audit objectives, which was to "assess the risk areas and control gaps noted from the gap assessment to determine whether the State's information security policy requirements have been designed, implemented, and are operating effectively within the CORE system environment managed by CGI". According to CGI, allowing us to review and assess this shared infrastructure would create a security and privacy risk for other CGI state clients. Due to this limitation, we were not able to test 84 of the 268 (31 percent) Security Policy requirements in scope. The table below (Figure 3) illustrates, by specific Security Policy reference, the number of relevant Security Policy requirements we could test and the number which we could not test to assess CGI compliance.

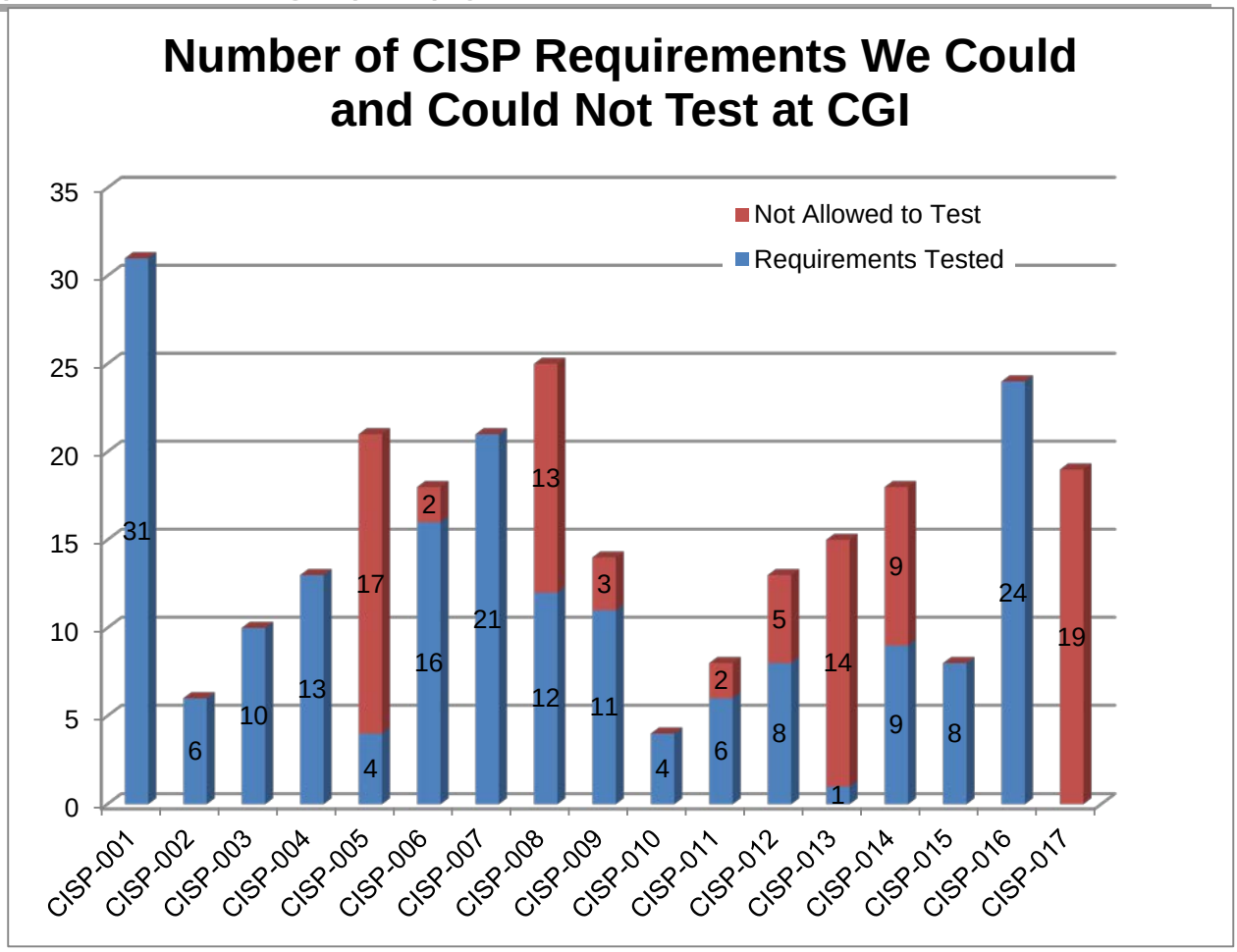

Figure 3 – CISP Requirements Tested at CGI

Note: The absence of a number in the figure indicates that the value is zero (0).

Policy Number	Title	Policy Number	Title
CISP-001	Access Control	CISP-010	Media Protection
CISP-002	Security Awareness and Training	CISP-011	Physical and Environmental Protection
CISP-003	Audit and Accountability	CISP-012	Personnel Security
CISP-004	Security Assessment and Authorization	CISP-013	Risk Assessment
CISP-005	Configuration Management	CISP-014	System and Services Acquisition
CISP-006	Contingency and Planning	CISP-015	System and Communications Protection
CISP-007	Identification and Authentication	CISP-016	System and Information Integrity
CISP-008	Incident Response	CISP-017	Security Planning
CISP-009	System Maintenance		

We were able to test 184 of the 268 (69 percent) specific Security Policy requirements. For the 184 specific requirements that we were able to test, we found that CGI was not fully compliant with 6 of the requirements (3 percent) as written in the Security Policies which were in effect in 2011; and CGI was not fully compliant with 37 of the requirements (20 percent) which were in effect in 2015.

CHAPTER 2

Prior to implementation of CORE (Colorado Operations Resource Engine), the State housed and managed the operation of the previous Statewide financial application, COFRS (Colorado Financial Reporting System), at the State's data center. The change from COFRS to CORE created a fundamental shift in the responsibility for operation of the primary infrastructure including the servers and databases used for CORE. Under a contract between the Governor's Office of Information Technology (OIT) and CGI, CGI - as the CORE contractor - is responsible for maintaining the CORE application at its multi-tenanted data center located in Phoenix, Arizona. As such, this partnership requires contract oversight of CGI to ensure compliance with applicable State laws, rules, and regulations. Although the contract with CGI is with OIT, both the Department of Personnel & Administration's Office of the State Controller (DPA/OSC) and OIT share the responsibility for contract monitoring and vendor management because DPA/OSC is the owner of the State's financial data which is processed by the CORE application.

The remainder of Chapter 2 describes our finding and recommendation related to the CORE infrastructure managed by CGI.

CORE Contractor is not Being Held Accountable for Colorado Information Security Policy Compliance

As part of the process to oversee CGI's compliance under the contract, OIT and DPA/OSC participate in meetings and review the SOC 1 (SSAE 16) report for the CGI Phoenix Data Center which CGI is required to have performed by the contract. The purpose of a SOC 1 (SSAE 16) audit and its resulting report is to evaluate the effect of controls at a service organization that are relevant to a user entity's (in this case the State of Colorado's) internal control over financial reporting. CGI is a service organization because it provides CORE system hosting and other services to the State.

During the initial implementation phase of CORE, the State utilized the Independent Verification and Validation (IV&V) services from the Public Consulting Group and received 3 reports between January and June 2014. However, these IV&V reports were not specifically related to ensuring that CGI was adhering to CISPs for the CORE environment managed by CGI.

In addition, periodic vendor assessments and evaluations are required by State policy to ensure continued satisfactory vendor performance and adherence to contract requirements, including requirements for compliance with State policies such as the Colorado Information Security Policies (Security Policy or Policies). Periodic vendor assessments and evaluations help identify any problems in vendor performance and allow the agency to address them.

State Policies and procedures provide the structure for how the contractor will adhere to State information security requirements. Contractor policies and procedures provide a link between the State's security needs and requirements and the processes that the contractor will perform to meet those requirements.

WHAT AUDIT WORK WAS PERFORMED AND WHAT WAS THE PURPOSE?

In order to perform our audit work, we interviewed OIT and DPA/OSC management and staff to determine what processes were in place for ensuring CGI is complying with Security Policies, including processes for monitoring contract compliance. We also interviewed CGI management to determine whether the State had communicated the requirement for complying with Security Policies to CGI. We also assessed the SOC 1 (SSAE 16) report against the Security Policy requirements to note gaps where the SOC 1 (SSAE 16) report did not address Security Policy requirements and reviewed the contract between OIT and CGI to determine the contact evaluation requirements. We also interviewed CGI personnel and reviewed CGI documentation to determine the documented policies, procedures, and standards in effect for the CORE infrastructure managed by CGI. The purpose of our audit work was to evaluate the effectiveness of OIT and DPA/OSC contract monitoring activities of CGI for compliance with the CISPs and to evaluate whether the contractor has documented policies, procedures, and operating standards as applied to the CORE infrastructure to meet the Colorado Information Security Policy requirements.

WHAT PROBLEM DID THE AUDIT WORK IDENTIFY AND HOW WERE THE RESULTS MEASURED?

A. **OIT is not holding CGI accountable for compliance with the CISPs as required by Security Policy (P-CISP-014-7.6.4) and as directed by the State Chief Information Security Officer.** Detailed results of our audit contain information concerning potential information security control weaknesses and/or vulnerabilities of the CORE system. This information is confidential and the

detailed compliance findings have been presented separately in a confidential non-public report that has been provided to the management of OIT and DPA/OSC.

1. We applied the following criteria when evaluating the adequacy of holding CGI accountable for Security Policy compliance:
    a. **Service Acquisition.** OIT's Security Policy, *CISP—14: System and Services Acquisition* [P-CISP-014-7.6.4]), requires an agency to monitor security control compliance by external service providers on an ongoing basis. In addition, in section 7.3.2 – Security Requirements – it states that security functional and assurance requirements should be included in the acquisition contract.
    b. **State Evaluation Schedule.** According to Statutes, §24-103.5-101(5) and 24-102-205(6), C.R.S., an annual certification and a separate interim evaluation must be completed annually over the lifetime of the contract, either on or before the anniversary date of the contract effective date in each subsequent fiscal year, and should be used as documentation in support of annual certification of the contractor, including the determination whether or not to re-certify the contractor.
    c. **Information Security Act.** According to rules in support of the Colorado Information Security Act each public agency will maintain a Cyber Security Plan**.** We applied the following contractual language:
        1. **Compliance with Law.** The contract states that the "Contractor shall strictly comply with all applicable federal and State laws, rules, and regulations in effect or hereafter established, including, without limitation, laws applicable to discrimination and unfair employment practices.
        2. **Choice of Law.** The contract states "Colorado laws, and rules and regulations issued pursuant thereto, shall be applied in the interpretation, execution, and enforcement of this Contract. Any provision included or incorporated herein by reference which conflicts with said laws, rules, and regulations shall be null and void."
    d. **Vendor Compliance.** On April 27, 2015, the State Chief Information Security Officer issued a memo to all State Employees advising that all vendors wishing to provide IT goods and services to the State must adhere to Security Policies. The purpose of the Systems and Services Acquisition policy (P-CISP-014) effective February 11, 2015 is to ensure all vendors follow the same security requirements to which the State is subject and security documentation for information systems is completed and periodically reviewed and updated. The policy which it superseded, Vendor Management Policy (P-CISP-005), was effective August 1, 2011 and stated in section 7.3.5.1 that vendors are required to comply with all applicable Colorado Information Security Policies.
    e. **Contract Mandated Evaluations.** According to the CORE Contract between OIT and CGI, section # 49660 §23.C Evaluation and Review, "Contractor's performance shall be subject to Evaluation and Review in accordance with the terms and conditions of this Contract, State law, including CRS §24-103.5-101, and State Controller Fiscal Rules, Policies, and Guidance. The State shall also complete an annual assessment of Contractor's performance, but such assessment shall not be entered into the statewide Contract Management System." The contract specifies three milestones, two of which were already due, at which evaluations will be completed. Specifically,
        1. The first milestone is at the completion of COFRS maintenance and support services. COFRS was the State's accounting system prior to being replaced by CORE in July 2014.

2. The second milestone is Ninety (90) days following CORE's go live date of July 7, 2014, for services provided by CGI, such as, provisioning, installation, and maintenance of hardware, operating system (OS), and database software as well as installation and management of software licensed by the State (Advantage Software and Bundled Software Products) to support the hosted System at the usage levels.
3. The third milestone is Five (5) years following CORE's go live date of July 7, 2014 for services provided by CGI, such as, provisioning, installation, and maintenance of hardware, operating system (OS), and database software as well as installation and management of software licensed by the State (Advantage Software and Bundled Software Products) to support the hosted System at the usage levels.

WHY DID THE PROBLEM OCCUR?

We identified the following causes for the problem identified:

1. **CONTRACTUAL LANGUAGE REGARDING SECURITY POLICY COMPLIANCE IS UNCLEAR AND AMBIGUOUS.** The contract language related to compliance with the Security Policies is not clear and is open to varying interpretations. While a section of the contract states CGI must comply with applicable federal and State laws, rules, and regulations, the contract does not specifically reference compliance with Security Policies. The contract also requires CGI to provide OIT with an annual SOC 1 (SSAE 16) report to allow OIT to assess whether any exceptions in the report caused the State to be in violation with Security Policies. OIT asserted that the contract language requires CGI to comply with the 2011 Security Policies OIT released in 2011 and in effect when the contract was signed, but that the contract does not require CGI to comply with any future Security Policy releases, such as the 2015 release. CGI asserted that OIT did not communicate the Security Policy compliance requirement and that its internal controls are aligned with its corporate internal control standards, as documented in the SOC 1 (SSAE 16) report. OIT believed that the contract language was sufficient to require CGI to comply with the CISPs that were current when the contract was signed, and that the contract requirement for the SOC 1 (SSAE 16) would allow them to assess compliance with the CISPs. OIT updated the CISPs effective February 11, 2015, but did not take additional steps, such as amending the contract, to ensure that CGI was aware of the security policy updates and the requirement that vendors must comply with current State CISPs.
2. **THE SOC 1 (SSAE 16) REPORT IS NOT AN EFFECTIVE MECHANISM FOR HOLDING CGI ACCOUNTABLE FOR COMPLYING WITH SECURITY POLICIES**. Although the review is not documented, OIT asserted that it does review the SOC 1 (SSAE 16) report, but not to assess compliance with Security Policies. The report is reviewed for reasonableness of the control objectives and associated control activities, as well as the overall final opinion.
3. **RESPONSIBILITY FOR CONTRACT OVERSIGHT IS MUDDLED**. The contract for CORE is currently assigned to OIT because the initial funding for the CORE implementation and operation was held by the agency. In practice, DPA/OSC, as the system owner, takes the lead for contract oversight while OIT maintains certain contractual monitoring obligations. Effective May 1, 2015, funding for CORE was transferred from OIT to DPA/OSC, but the contract with CGI has not been transferred to DPA/OSC.
4. **DIFFERENT STANDARDS.** CGI asserted that it is an International Organization for Standardization certified company and therefore its policies align with ISO standards. The International Organization for Standardization, is an independent, non-governmental organization,

and is the world's largest developer of voluntary international standards including security standards. Since Colorado Security Policies are aligned with National Institute of Standards and Technology (NIST), the two standards may have different rules for implementing information security standards and thus CGI would not have implemented all of the NIST related requirements. NIST is a non-regulatory federal agency that promotes standards including security standards.

WHY DOES THIS FINDING MATTER?

A. The Security Policies were created to support achievement of the Colorado Information Security Act and ultimately to ensure that the information the citizens have entrusted to agencies is safe, secure, and protected from unauthorized access, unauthorized use, or destruction. The State and citizens of Colorado cannot be certain that information is being adequately secured if Security Policies are not enforced. Without ongoing, timely, and consistent oversight, OIT cannot ensure that CGI is achieving program goals and objectives, meeting contract requirements and performance measures, and complying with the Security Policies.

B. The Security Policies were established to reduce the risk to the State of loss of data or unauthorized access to applications and are mandatory for all vendors providing services to the State. The transition of the Colorado statewide financial application from the State managed data center to a cloud-based solution hosted by CGI as a third-party service provider significantly increases the need for monitoring to ensure data privacy, compliance, service integrity, and information protection controls are in place that meet State requirements.

RECOMMENDATION 1

The Governor's Office of Information Technology should improve oversight of CGI, as the CORE application's third-party service provider, to ensure compliance with the Colorado Information Security Policies (Security Policy or Policies) by:

a. Amending the CGI contract as necessary to clearly and unambiguously state that the contractor is required to comply with all current and future updated State of Colorado Information Security Policies.

b. Ensuring it has a process and effective mechanism in place to assess CGI for compliance with the CISPs including ensuring that CGI's policies and procedures for CORE comply with the Security Policies.

c. Amending the CGI contract as necessary to assign DPA/OSC primary responsibility for contract oversight, while stipulating that OIT should continue to ensure compliance with the Security Policies.

RESPONSE

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

A Agree. Implementation Date: July 2017

OIT will develop a contract amendment that requires CGI to comply with all Information Security policies and will evaluate with DPA the costs associated with executing such amendment. Should additional funding be necessary, OIT will work with the General Assembly on a budget request for this item.

B **Agree. Implementation Date: July 2018**

OIT agrees that evaluating its vendors for compliance with CISPs is necessary; however, the security unit is currently not staffed to perform this work effectively. Therefore, OIT will work with the General Assembly on a request for funding to establish a vendor security assessment team and acquire tools for Fiscal Year 2018. Should funding not be approved, OIT will implement a manual process which includes requiring completion of a questionnaire by CGI on its security processes and a risk based evaluation of responses by the OIT security unit.

C **Agree. Implementation Date: July 2017**

OIT will work with DPA to establish contractual ownership, and if the costs of a new contract are acceptable, OIT will amend the contract with CGI to reflect the agreement between OIT and DPA. If approved, OIT will begin this effort by December 2016; new contract will be implemented July 2017.

GLOSSARY

TERMS

Critical System

Systems that provide critical data to the public, and serve a vital function to government, but do not affect life-safety and must be recovered within 72 hours to a week of a system failure.

Essential System

Systems where loss or unavailability is unacceptable, due to life-safety issues, and must be recovered within 2 to 24 hours of a system failure.

Executive Branch Agency

All of the departments, divisions, commissions, boards, bureaus, and institutions in the Executive Branch of the state government. This does not include the legislative or judicial department, the department of law, the department of state, the department of the treasury, or state-supported institutions of higher education.

Public Agency

Every state office, whether executive or judicial, and all its respective offices, departments, divisions, commissions, boards, bureaus, and institutions. “Public agency” does not include institutions of higher education or the general assembly.

System

For the purpose of this audit, the OSA defines a “system” as an application, the application’s operating system(s), and the application’s database(s).

Access Control

Access controls are typically logical controls designed into the hardware and software of a computing system. Identification is accomplished both under program control and physical controls.

Audit Log

A chronological record of information system activities, including records of system accesses and operations performed in a given period.

Authorization

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the State based on the implementation of an agreed-upon set of security controls.

Compensating Security Controls

The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization.

Configuration Control

Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

Configuration Management

A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

External Information System Service Provider

A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.

Information Owner

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Risk

The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the State due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Malicious Code Malware

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Network

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Privileged User

A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Risk Assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the State, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

System Security Plan

Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Vulnerability Assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.