TEXAS HEALTH AND HUMAN SERVICES COMMISSION

INSPECTOR GENERAL

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

MAXIMUS Enrollment Broker

February 23, 2018
OIG Report No. AUD-18-011

HHSC IG

TEXAS HEALTH AND HUMAN SERVICES COMMISSION

INSPECTOR GENERAL

February 23, 2018

SECURITY CONTROLS OVER CONFIDENTIAL HHS SYSTEM INFORMATION

MAXIMUS Enrollment Broker

WHY THE IG CONDUCTED THIS AUDIT

The State of Texas contracts with MAXIMUS for Medicaid and CHIP enrollment broker services. In performing those services, MAXIMUS (a) uses personally identifiable information to enroll qualified individuals into Medicaid and CHIP MCOs, (b) stores confidential information for Medicaid and CHIP applicants and enrollees, and (c) transmits confidential information to MCOs and other entities across multiple networks.

MAXIMUS is required to protect and secure confidential HHS System information in accordance with the contract and HHS Information Security Standards and Guidelines (ISSG).

WHAT THE IG RECOMMENDS

HHSC Medicaid and CHIP Services should coordinate with HHS IT to ensure MAXIMUS system security plans are timely reviewed, and should require MAXIMUS to:

- Improve access controls for systems containing confidential HHS System information.
- Strengthen account management practices and password configurations.
- Timely prioritize and remediate identified security weaknesses.
- Develop system maintenance processes that include updating system security documents.
- Obtain information and documentation from its subcontractors to enable evaluation of subcontractor performance.

For more information, contact:
IG.AuditDivision@hhsc.state.tx.us

WHAT THE IG FOUND

MAXIMUS had an adequate physical security environment in its primary data center to protect confidential information, and processes to monitor information systems activities were sufficient to identify and prevent harmful activities such as viruses on the network.

MAXIMUS did not (a) adequately manage access to systems that store and transmit confidential HHS System information, (b) configure password parameters to meet applicable standards, (c) timely remediate identified vulnerabilities, or (d) maintain and execute system maintenance processes.

Areas in which MAXIMUS' existing IT controls did not fully comply with ISSG, as required by the contract, are indicated with an X in the table below.

Control Areas Tested	Operating System	Application	Database
Information Security Oversight	X	X	X
User Account Management *	X	X	X
Configuration Settings *		X	X
Information Systems Monitoring			
Vulnerability Assessment and Remediation	X	X	X
Physical Security			

**Oracle did not provide information needed to test the control area.*

MAXIMUS submitted annual system security plans for its EBSSP and MAXeb applications, as required by ISSG, detailing the design of IT security control structures for these systems that process or store confidential HHS System information. The 2016 MAXIMUS system security plans were not reviewed by the HHS ISO because the HHS ISO was not notified or provided the security plans for review.

Oracle, the MAXIMUS infrastructure and hardware services subcontractor, did not provide information needed for the IG to fully evaluate and conclude on the effectiveness of security controls over confidential HHS System information hosted at Oracle's data center. By not providing the information, Oracle created an audit scope limitation that prevented the IG from fully achieving the audit objective, which was to assess the design and effectiveness of selected security controls over HHS System confidential information stored and processed by MAXIMUS.

MCS generally agreed with the audit recommendations, and indicated some action plans have already been implemented and others were in progress. MAXIMUS, in a comment letter included in Appendix D of the report, generally agreed with the IG Audit Division recommendations, but did not agree that requested information not provided to the IG Audit Division by Oracle created a scope limitation. An Auditor Comment follows the MAXIMUS comment letter.

TABLE OF CONTENTS

INTRODUCTION

The Texas Health and Human Services Commission (HHSC) Inspector General (IG) Audit Division has completed an audit of security controls over confidential Health and Human Services (HHS) System information at MAXIMUS, Inc. (MAXIMUS), the Medicaid and Children's Health Insurance Program (CHIP) enrollment broker.

The IG Audit Division conducted the audit to determine whether confidential HHS System information in the custody of MAXIMUS and its data center services subcontractor, Oracle, Inc. (Oracle), was protected from unauthorized access, loss, or disclosure.

Unless otherwise described, any year referenced is the state fiscal year, which covers the period from September 1 through August 31.

Objective and Scope

The audit objective was to assess the design and effectiveness of selected security controls over confidential HHS System information stored and processed by MAXIMUS.

The scope included:

- MAXIMUS logical and physical security controls, including network access and authentication, designed to safeguard the MAXeb and EBSSP applications, and their associated databases, which process and store confidential HHS System information.
- MAXIMUS security plans and associated HHSC security plan review processes for fiscal years 2016 and 2017.
- MAXIMUS IT controls for physical security of data and equipment, user account management, information system monitoring, and vulnerability remediation efforts, from September 2015 through February 2017.

The scope included the MAXIMUS production environment, but did not include the system backup environment.

Background

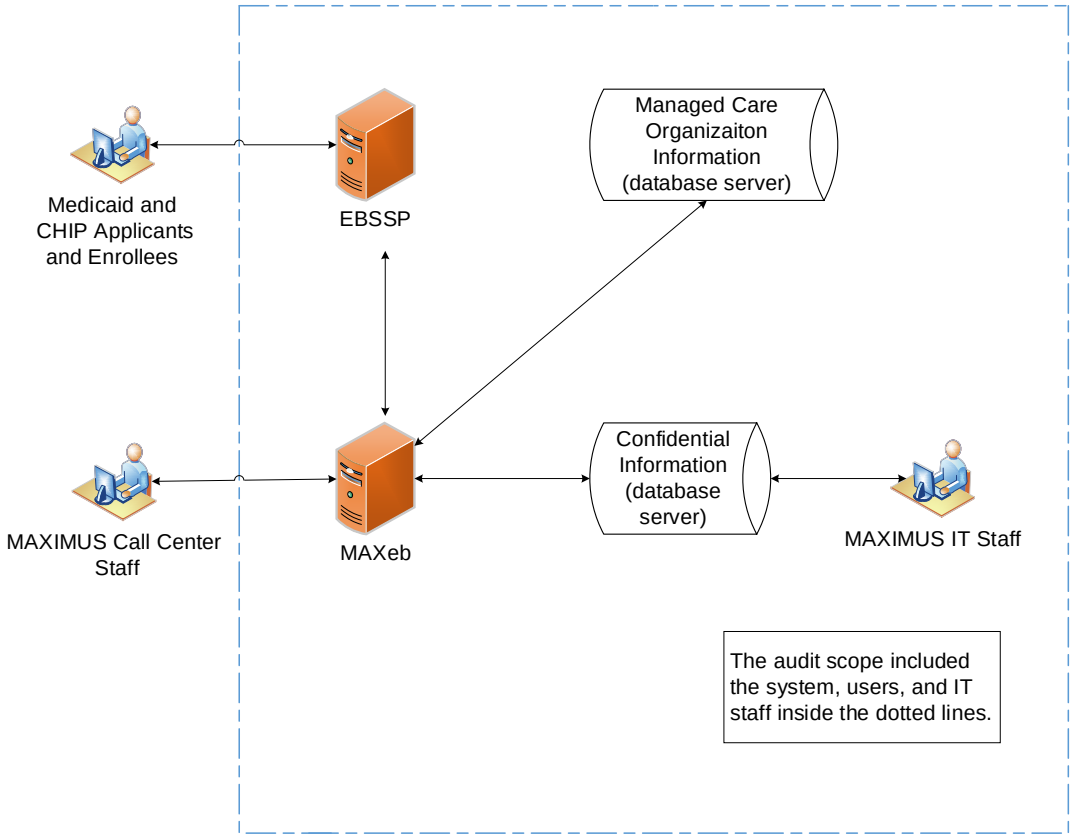
The MAXIMUS enrollment broker contractual responsibilities include providing outreach, education, and enrollment services for Medicaid and CHIP programs.

Under the enrollment broker contract,[1] MAXIMUS functions as the sole Medicaid and CHIP enrollment broker for the State of Texas, and uses personally identifiable information to enroll qualified individuals into managed care organizations (MCOs). MAXIMUS stores confidential information for Medicaid and CHIP applicants and enrollees, and transmits the information to MCOs and other entities across multiple networks.

Figure 1 diagrams the information flow from the Enrollment Broker Self Service Portal (EBSSP) to the MAXIMUS enrollment broker application, MAXeb. Medicaid and CHIP applicants submit applications online in the EBSSP application, which transmits the enrollment information to the MAXeb application. The MAXeb application processes the enrollment information by utilizing system logic to assign applicants to appropriate Medicaid and CHIP programs and MCOs. Both applications transmit and utilize personally identifiable information, which is stored in an associated database. Additionally, MAXIMUS call center staff enter applicant information directly into the MAXeb application when contacted by the applicant for enrollment or to update information. Other MAXIMUS staff utilize the MAXeb application to query and report on enrollment for clients and programs.

[1] Enrollment Broker Operations and Texas Health Steps Outreach and Informing Agreement Between the Health and Human Services Commission and MAXIMUS, INC, HHSC Contract No. 529-10-0005-00001 (Oct. 2013).

Figure 1: MAXeb and EBSSP System Diagram as of April 2017



Source: Prepared by the IG Audit Division

The enrollment broker contract incorporates a Data Use Agreement (DUA)[2] and requires compliance with applicable laws, rules, and regulations regarding information security, including but not limited to:

- Health and Human Services Circular C-021, Health and Human Services Information Security/Cybersecurity Policy.
- Health and Human Services Information Security Standards and Guidelines (ISSG),[3] which includes the Security Controls Catalog.
- Title 1, Sections 202.1 and 202.3 through 202.26, Texas Administrative Code (TAC).
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

[2] HHS Data Use Agreement V.7.4., HHSC Contract No. 529-10-0005-00001, Attachment 7 Security Guidelines and Procedures (Oct. 21, 2014).

[3] This document was previously entitled Enterprise Information Security Standards and Guidelines. The title of the document has since been changed to Information Security Standards and Guidelines.

HHSC Medicaid and CHIP Services (MCS), HHS IT, and MAXIMUS share accountability for safeguarding state information systems and protecting confidential HHS System information from accidental or unauthorized access, loss, or disclosure. The enrollment broker contract requires MAXIMUS, each year, to submit a Security Management Plan for HHSC's review and approval.[4] The security plan should include a detailed approach for establishing and maintaining security, and contains detailed management, operational, and technical information about a system, its security requirements, and the controls implemented to provide protection against risks and vulnerabilities.

The security plan is designed to document current system security controls that protect the confidentiality, integrity, and availability of HHS System data processed, stored, and transmitted by MAXIMUS. Security controls must follow guidance provided in the ISSG catalog of security controls, which is based on the National Institute of Standards and Technology (NIST) security standards. The IG Audit Division applied the ISSG criteria, along with MAXIMUS' security policy and procedures, to design audit tests to assess the design and effectiveness of selected security controls over confidential HHS System information stored and processed by MAXIMUS.

The security management plan submitted by MAXIMUS is comprised of system security plans for each critical application under the purview of MAXIMUS, including enrollment broker systems. MAXIMUS subcontracts with Oracle to provide the facilities and IT infrastructure for MAXIMUS' applications, including EBSSP and MAXeb. Oracle's data center is responsible for the maintenance of MAXIMUS' IT infrastructure.

The IG Audit Division conducted this audit in accordance with:

- Generally accepted government auditing standards issued by the Comptroller General of the United States
- Standards for Information Systems Audit and Assurance issued by ISACA

The IG Audit Division presented audit results, issues, and recommendation to responsible management in MCS, HHS IT, and at MAXIMUS in a draft report dated November 10, 2017. Each was provided with the opportunity to study and comment on the report. The MCS management response to audit recommendations contained in the report is included in the report following the recommendations.

[4] Enrollment Broker Operations and Texas Health Steps Outreach And Informing Agreement Between The Health And Human Services Commission and MAXIMUS, INC, HHSC Contract No. 529-10-0005-00001, Exhibit B, Deliverables, Deliverable ID # EB 653(A), Security Management, Security Management Plan (Oct. 2013).

MCS concurred with the IG Audit Division recommendations outlined in this report, and indicated some corrective actions have already been implemented. MCS indicated it plans to complete the remaining corrective actions by June 2018.

MAXIMUS' comments are included in Appendix D. MAXIMUS generally agreed with the IG Audit Division recommendations, but did not agree that requested information not provided to the IG Audit Division by Oracle created a scope limitation. An Auditor Comment follows the MAXIMUS comment letter.

AUDIT RESULTS

The IG Audit Division assessed relevant security controls protecting confidential HHS System information in the custody of MAXIMUS, including information processed through the EBSSP and MAXeb applications. Key control areas and the associated control groups tested during the audit are identified in Table 1. Key control areas for information security contain controls that are required in order to provide reasonable assurance that material errors will be prevented or timely detected. Control groups are ISSG-defined groupings of security controls. Each control group contains multiple controls which must be applied as required, based on data risk, to provide customized controls for information security.

Table 1: Key Control Areas and Control Groups

Key Control Areas Selected for Audit	ISSG Control Groups
Information Security Oversight	Planning Controls Risk Assessment Controls
User Account Management	Access Controls Identification and Authentication
Configuration Settings	Configuration Management
Information Systems Monitoring	Incident Response
Vulnerability Assessment and Remediation	Security Assessment and Authorization Controls
Physical Security	Physical and Environmental Protection Controls

Source: Created by the IG Audit Division based on ISSG Information

An overview of all control areas tested in this audit is presented in Appendix C.

The IG Audit Division tested IT security controls and relevant activities supporting data security at MAXIMUS. In addition, the IG Audit Division attempted to test baseline server configurations and third party vendor access to confidential HHS System information stored on MAXIMUS resources at the third party vendor, Oracle. Oracle provided a minimal amount of information in response to requests for evidence of activities and controls in place to protect confidential HHS System information, but did not provide information on administrative user access to servers and data, or on baseline security configurations, limiting the IG Audit Division's ability to fully achieve the audit objective. Issues relevant to this scope limitation are noted in the narratives describing audit results for each applicable control area.

Audit results indicated that MAXIMUS had an adequate physical security environment in its primary data center to protect confidential information. Additionally, processes to monitor information systems activities were sufficient to identify and prevent harmful activities such as viruses on the network.

Improvements are needed in several control areas to further protect confidential HHS System information from unauthorized access, loss, or disclosure, including:

- Information security oversight
- User account management
- Configuration settings
- Vulnerability assessment and remediation

Issue 1: Information Security Oversight

The enrollment broker contract's DUA requires MAXIMUS to submit a security plan annually. The ISSG requires MCS, as the contract manager and information owner, to collaborate with the HHS Information Security Officer (ISO) to ensure the security plans submitted by MAXIMUS are complete in accordance with the HHS information system security plan template.[5] Texas Administrative Code requires state agency chief information officers to coordinate the review of data security requirements, specifications, and, if applicable, third-party risk assessments of any new computer applications or services that receive, maintain, and share confidential data.[6] The HHS information system security plan template[7] is used by contractors to document their applicable system security controls, and by HHS to monitor contractors' system security.[8]

MAXIMUS is required to assign a security categorization to each critical system, such as high, moderate, or low, depending on the nature of the confidential HHS System information it stores, processes, or transmits using each applicable critical system. Based on the assigned security categorization, security controls are to be designed and implemented per the ISSG control catalog,[9] and documented in the system security plan. To comply with these requirements, MAXIMUS must document critical systems and facility security in accordance with ISSG. MAXIMUS submitted security plans in the required format and with the completed controls catalog for each of the critical applications.

[5] HHS Information Security Standards and Guidelines Controls Catalog, § 2.3.2 Compliance Monitoring, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[6] 1 Tex. Admin. Code, § 202.21 (Mar. 17, 2015) and (Mar. 16, 2016).

[7] HHS Information Security Plan Template, v. 1.3 (July 2015) through v. 1.6 (May 2016).

[8] HHS Information Security Standards and Guidelines Controls Catalog, § 2.3.2 Compliance Monitoring, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[9] HHS Information Security Standards and Guidelines Controls Catalog, § 2.1 Information System Security Categorization, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Responsibilities for Review of System Security Plans by HHS ISO Was Not Defined

MCS did not collaborate with the HHS ISO for review of MAXIMUS security plans. MAXIMUS submitted annual system security plans utilizing required templates for MAXeb and EBSSP, systems that process, store, and transmit confidential HHS System information, to the Contract Compliance and Performance Management (CCPM) section at MCS. In accordance with established procedures, CCPM then forwarded the MAXIMUS security plans to another MCS section, Medicaid Management Information Systems (MMIS), rather than forwarding them to the HHS ISO. MMIS was to review the plans and communicate feedback on the security plans to CCPM, which in turn would have communicated the MMIS feedback to MAXIMUS. However, MMIS indicated that it did not possess the skill sets necessary to adequately evaluate the content and appropriateness of the MAXIMUS security plans.

The 2016 MAXIMUS system security plans were not reviewed by the HHS ISO because the HHS ISO was not notified or provided the security plans for review. However, the HHS ISO reviewed the 2017 security plans in December 2016, after this audit began, and requested that MAXIMUS make clarifications and changes to the MAXeb security plan. The security plan was subsequently updated and resubmitted to the HHS ISO in February 2017, and was approved in June 2017. The delayed review, revision, and acceptance of MAXIMUS system security plans (a) created a false assurance to HHSC that confidential HHS System information in the custody of MAXIMUS and its subcontractors was protected from unauthorized access, loss, or disclosure, and (b) hindered HHSC's ability to hold MAXIMUS accountable for incomplete or inadequate system security plans.

Recommendation 1

MCS, through its contract oversight responsibility and in coordination with the HHS ISO, should establish formal roles, responsibilities, and processes for the review and approval of system security plans submitted by contractors. A process to ensure timely notification and review should be developed to ensure MCS and the HHS ISO coordinate and collaborate on the review and approval of contractor system security plans.

Management Response

Action Plan

The Contract Administration and Provider Monitoring (CAPM), formally known as Contract Compliance and Vendor Management agrees with the finding and will coordinate with Medicaid Management Information Systems and HHS Information Security Office and revise its existing procedures to enhance processes associated with the review and approval process of the system security plans submitted by the Enrollment Broker (EB)

Responsible Manager

CAPM Director

Target Implementation Date

June 2018

Issue 2: Oracle Limited Access to Information

The enrollment broker contract states that MAXIMUS, as the contractor, "will provide, and will cause its subcontractors to provide auditors and inspectors, as HHSC may from time to time designate, with access to: (1) contractor service locations, facilities, or installations; and (2) contractor software and equipment. Also, the contractor must provide as part of the services any assistance that such auditors and inspectors reasonably may require to complete such audits or inspections."[10]

Through a subcontracted service arrangement with MAXIMUS, Oracle provides infrastructure and hardware services for MAXIMUS enrollment broker applications. The IG Audit Division, through MAXIMUS, requested information from Oracle needed to evaluate the design and effectiveness of security controls over the confidential HHS System information processed and stored in the Oracle data center. Oracle provided limited access to the requested information, asserting that the IG Audit Division should place reliance on Oracle's Service Organization Controls (SOC) reports.

[10] Enrollment Broker Operations and Texas Health Steps Outreach and Informing Agreement Between the Health and Human Services Commission and MAXIMUS, INC, HHSC Contract No. 529-10-0005-00001, Article VIII, Audit and Financial Compliance, § 8.02 Access to records, books, and documents; and § 8.03 Audits of Services, Deliverables and Inspections (Oct. 2013).

A SOC report is intended to meet the needs of users who require detailed information and assurance about the controls at a service organization[11] relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data, and the confidentiality and privacy of the information processed by these systems. The use of the reports is generally restricted to customers and stakeholders.

The professional standards utilized by the IG Audit Division require that the extent of use and reliance on other auditors' or experts' work is dependent on (a) the significance and scope of the other auditor's work, (b) planning, supervision, assumptions, and testing being adequately documented, and (c) findings being supported by evidence. Audit standards also recommend that some retesting of the work of the other experts should occur in order to conclude on the current IT audit objectives and document a conclusion. The IG Audit Division was not able to review the work performed by the SOC auditor and was unable to retest work. Therefore, the IG Audit Division was not able to rely on the SOC report.

MAXIMUS did not, as required by the enrollment broker contract, require Oracle to provide the IG Audit Division with requested information needed to evaluate the security of confidential HHS System information. To accommodate Oracle protocols and gain access to the information needed to conduct the audit, the IG Audit Division worked with MAXIMUS and Oracle to execute a nondisclosure agreement. After the auditors arrived at Oracle to conduct the test procedures, Oracle displayed policy and procedure documents from a projector for the auditors to review. Oracle did not provide user account information the IG Audit Division needed to evaluate privileged user account management. Additionally, Oracle provided no evidence of configuration settings for servers that process and store confidential HHS System information.

Because it did not receive the requested information, the IG Audit Division is unable to evaluate and conclude on the effectiveness of security controls over confidential HHS System information hosted at the Oracle data center. Until the requested information is made available, HHSC does not have assurance that confidential information processed by and stored in the enrollment broker system is adequately protected from unauthorized access, loss, and disclosure.

Recommendation 2

MCS, through its contract oversight responsibility, should require MAXIMUS to cause its subcontractors to comply with contractual requirements related to audits and inspections, and to consider tailored contractual remedies to require compliance.

[11] A service organization is defined as an organization providing services to "user entities." User entities are simply organizations using the services of a service organization.

Management Response

Action Plan

MCS CAPM requires MAXIMUS to comply with all contractual requirement related to audits and inspections, including any provisions which flow down to subcontractors such as access to facilities and access to records, books, and documentation. Up until this audit, MCS has not identified any issues with the EB subcontractors adhering to State requirements. CAPM will coordinate with HHS internal departments such as HHS Information Technology, HHS Audit, Procurement and Contract Services; the Contract Provider, and the Department of Information Resources to determine if risk mitigation opportunities are available and document the outcome of these findings to include any implementation strategies that may need to occur.

Responsible Manager

CAPM Director

Target Implementation Date

June 2018

Issue 3: User Account Management

User account management consists of procedures to request, establish, issue, suspend, modify, and deactivate access to systems and confidential information. The procedures apply to all account types, including application end users, system administrators, and privileged accounts assigned to both internal and external users. Privileged accounts have escalated access within a computer system. Escalated access allows permission to edit or create user accounts, data, or settings within the operating system, application, or database. User account management procedures should accommodate the special needs of privileged accounts to include provisioning, authentication, authorization, password management, auditing, and access controls over shared or generic (non-unique) privileged accounts.

Many shared or generic privileged accounts are built-in system accounts automatically created when an operating system, application, or database is first installed. These types of privileged accounts may not be subject to normal account management processes and require additional control considerations, such as renaming or disabling the accounts, changing the default account passwords, and monitoring account access and use.

Key control principles include least privilege access and separation of duties. Least privilege access is the practice of allowing only the access for users that is necessary to accomplish assigned tasks in accordance with business functions.[12]

To accomplish least privilege access control practices, roles are created for various job functions, and permissions to perform certain operations are assigned to specific roles. System users are assigned roles, and through those role assignments acquire permissions to perform only job-related functions in the system.

Separation of duties segregates the duties of individuals to prevent malevolent activity from occurring,[13] including preventing developers from changing or updating production environments, applications, and data without appropriate authorization, testing, and approval.

MAXIMUS Granted Excessive Privileged Access Within MAXeb

MAXIMUS did not limit user access within the MAXeb application to only the permissions needed to perform job duties. MAXIMUS granted privileged access to 18 end users who did not require privileged access to perform their job duties. Although there was no evidence that inappropriate activities occurred, this access could have allowed the MAXeb users to schedule or release jobs in the scheduler application, which controls the timing and execution of batch jobs.

Another seven IT personnel (three developers and four database administrators) had privileged access assigned in the MAXeb application. End user access within the application was not appropriate for these types of IT operations staff. Operational staff such as developers and database administrators' job duties should not require access to the application. Without adequate separation of duties, abuse of privileges could occur and risk of inappropriate activities exists.

Additionally, the IG Audit Division requested that Oracle provide privileged account information needed to evaluate user account management for access to confidential HHS System information stored on MAXIMUS servers hosted at the Oracle data center. Oracle did not provide the information. As a result, the IG Audit Division was unable to evaluate and conclude on the effectiveness of Oracle's privileged user account management practices relevant to the protection of confidential HHS System information. See Issue 2, which discusses audit limitations resulting from Oracle not providing requested information.

[12] HHS Information Security Standards and Guidelines Controls Catalog, § 7.1 Access Controls, AC-6 Least Privilege, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[13] HHS Information Security Standards and Guidelines Controls Catalog, § 7.1 Access Controls, AC-5 Separation of Duties, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Access to Production Was Not Segregated From Developers

MAXIMUS allowed 16 developers access to the production environment for the MAXeb application, which included workflows and data that were outside of their job functions. MAXIMUS indicated that the developers' roles should have been limited to creating and testing computer programs and logic functions in the MAXeb application. The creation, development, and testing of computer programs should occur only in a protected development environment, and developers with access to the development environment should not also have access to production systems and data.[14]

Recommendation 3.1

MCS, through its contract oversight responsibility, should:

- Require MAXIMUS to (a) limit user account permissions to only those activities needed to perform job responsibilities, (b) remove privileged permissions for the 18 end users who do not require the permissions, and (c) remove 7 operational staff from the MAXeb application.

- Require MAXIMUS to obtain privileged account information from its subcontractor and provide it to MCS.

- Require MAXIMUS to remove the 16 developer accounts in the production environment. If access is deemed necessary, then account use should be limited to the time needed, and activities performed under the accounts should be monitored.

MCS should consider tailored contractual remedies to compel MAXIMUS to effectively perform account management activities.

[14] HHS Information Security Standards and Guidelines Controls Catalog, § 7.5 Configuration Management, CM-5 Access Restrictions for Change, and § 7.1 Access Controls, AC-5 Separation of Duties, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Management Response

Action Plan

MCS agrees with the recommendation and has since corrected the issue and implemented the appropriate measures to ensure that permissions within MAXeb are issued according to State guidelines.

Responsible Manager

Enrollment Broker Operations Director

Target Implementation Date

Completed

Generic System Administrator Account Was Active In MAXeb

A generic system administrator account existed and was utilized in the MAXeb application. No one individual was assigned as the user of the account, and the account had no logging enabled to track the actions performed by the account. User accounts should uniquely identify and authenticate organizational users.[15] Generic accounts, especially privileged accounts, can be targets for abuse and have no accountability for their use. MAXIMUS disabled the system administrator account before the completion of the audit and provided sufficient information to verify that the account was disabled.

Recommendation 3.2

MCS, through its contract oversight responsibility, should require MAXIMUS to demonstrate it has processes in place for renaming or disabling generic and default accounts, and for changing default account passwords. Additionally, periodic monitoring of account access and use should occur.

[15] HHS Information Security Standards and Guidelines Controls Catalog, § 7.7 Identification and Authentication, IA-2 Identification and Authentication Organization Users, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Management Response

Action Plan

MCS agrees with the recommendation and has since corrected the issue and implemented the appropriate measures to ensure that permissions within MAXeb are issued according to State guidelines.

Responsible Manager

Enrollment Broker Operations Director

Target Implementation Date

Completed

Issue 4: Configuration Settings

ISSG specifies that documentation and maintenance of current and secure baseline configuration settings for network components are key controls in securing IT systems.[16] Baseline security configurations include documented standards about information system components' settings and parameters to protect data. Configuration standards include password settings, software installation parameters, and server settings for functions, ports, protocols, services, and remote connections intended to protect information resources from unauthorized access, modification, and loss.

The IG Audit Division evaluated encryption protocols and password settings and determined encryption was enabled for data at rest and in transit throughout the enrollment broker network as required. However, password settings were not in compliance with established requirements for the MAXeb and EBSSP applications.

Password Configurations Did Not Comply With ISSG Standards or the MAXIMUS Security Plan

The MAXeb and EBSSP applications password settings were weaker than required by ISSG standards for password configurations. In addition, password configurations implemented for the MAXeb and EBSPP applications were not in compliance with the MAXIMUS system security plans.

[16] HHS Information Security Standards and Guidelines Controls Catalog, § 7.5 Configuration Management, CM-2 Baseline Configurations, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

Detailed results are confidential under Texas Government Code Sections 552.139(b) and 2054.077(c), and are therefore not included in this report. The confidential, detailed results have been provided separately to responsible HHS System personnel and contractors, and applicable state officials authorized to receive computer vulnerability information.

Recommendation 4.1

MCS, through its contract oversight responsibility, should require MAXIMUS to address identified password control weaknesses and ensure password requirements are enforced.

See separate document, "Confidential Issues: Audit of Security Controls over Confidential HHS System Information at MAXIMUS."

MCS should consider tailored contractual remedies to compel MAXIMUS to comply with password requirements.

Management Response

Action Plan

MCS agrees with the recommendation and has since corrected the issue and implemented the appropriate measures to ensure that password requirements within MAXeb are configured according to State guidelines.

Responsible Manager

Enrollment Broker Operations Director

Target Implementation Date

Completed

Baseline Server Configurations Could Not Be Verified

The IG Audit Division was unable to perform sufficient testing to provide reasonable assurance of the effectiveness of server configuration controls because MAXIMUS did not require Oracle to provide evidence of configuration settings for servers that process and store confidential HHS System information.

Documented server configurations are an essential component to (a) harden system security by locking ports and services, (b) develop repeatable server builds, (c) implement efficient change management, and (d) assist in troubleshooting security events or incidents. Baseline configuration settings for new server

installations and server rebuilds help ensure that services, ports, and default accounts are appropriately implemented and maintained. See Issue 2, which discusses audit limitations resulting from Oracle not providing requested information.

Recommendation 4.2

MCS, through its contract oversight responsibility, should:

- Require MAXIMUS to document baseline configurations for servers, as well as any other network devices that store and process confidential HHS System information.

- Require MAXIMUS to obtain evidence of server configuration settings from its subcontractor and provide it to MCS.

MCS should consider tailored contractual remedies to compel MAXIMUS to effectively document and maintain baseline configurations for servers.

Management Response

Action Plan

MCS is actively taking a number of steps to enhance its contract monitoring and oversight control activities. Enrollment Broker Operations will coordinate with other MCS areas along with MAXIMUS to develop and execute a system to document baseline configurations for servers and obtain evidence of server configuration settings from their subcontractors. MCS CAPM will work on developing and implementing a Key Performance Requirement (KPR) entailing potential liquidated damages.

Responsible Manager

Enrollment Broker Operations Director

Target Implementation Date

June 2018

Issue 5: Vulnerability Assessment and Remediation

ISSG requires MAXIMUS to conduct network vulnerability scans at least annually.[17] Oracle scanned the hardware and devices at MAXIMUS that protected networks from outside internet traffic on a quarterly basis to identify security weaknesses. These scans identify vulnerabilities within the network and equipment. Oracle communicates the vulnerabilities and remediation plans to MAXIMUS for its concurrence if downtime is required. The IG Audit Division reviewed MAXIMUS processes for the tracking and prioritization of remediation of identified vulnerabilities.

Oracle scanned selected IP addresses associated with devices and servers throughout the enrollment broker system during different quarters, to provide coverage of each IP address at least once each year. The scanning tools produced reports, grouped by IP address, of network vulnerabilities by severity. The IG Audit Division reviewed these reports and noted that there were no high risk vulnerabilities. However, opportunities exist for improving processes for managing moves and changes to servers, to ensure that Oracle scans all hardware and remediates security issues timely.

Remediation of Identified Vulnerabilities Was Not Performed Timely

Oracle identified a security vulnerability when it performed a scan in July 2016, but did not inform MAXIMUS of the weakness until September 2016. MAXIMUS began remediation efforts in October 2016, 13 weeks after the identification of the vulnerability. ISSG requires that legitimate vulnerabilities be (a) shared with designated security personnel and system administrators to help eliminate similar vulnerabilities in other information systems, (b) remediated, and (c) prioritized in accordance with the risk.[18]

Unnecessary delays impact the risk determination and timely remediation of security weaknesses, placing confidential HHS System information at continued risk of unauthorized access, loss, or modification.

Recommendation 5.1

MCS, through its contract oversight responsibility, should require MAXIMUS to improve the timeliness of addressing identified security weaknesses that require remediation.

[17] HHS Information Security Standards and Guidelines Controls Catalog, § 7.15 Risk Assessment, RA-5 Vulnerability Scanning, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

[18] HHS Information Security Standards and Guidelines Controls Catalog, § 7.15 Risk Assessment, RA-5 Vulnerability Scanning, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

MCS should consider tailored contractual remedies to compel MAXIMUS to effectively respond to identified security weaknesses.

Management Response

Action Plan

MCS is actively taking a number of steps to enhance its contract monitoring and oversight control activities. MCS CAPM will work with MAXIMUS to develop a process to improve timeliness of addressing identified security weaknesses requiring remediation. MCS CAPM will monitor MAXIMUS' responses and will pursue any contractual remedies available to compel performance.

Responsible Manager

CAPM Director

Target Implementation Date

June 2018

System Maintenance Processes Were Not Adequate

The MAXIMUS system security plan listed a database server and associated IP address that were no longer in use at MAXIMUS. Additionally, MAXIMUS' system security plan did not list a server used to support the MAXeb and EBSSP processes, resulting in the server not being included in the annual scanning process performed by Oracle. MAXIMUS indicated the server was only utilized for file transfer and would not be scanned anyway. Failure to maintain system maintenance processes[19] hinders the accuracy of system and security documentation and limits MAXIMUS' ability to appropriately monitor and protect confidential data. Undocumented changes to the operating environment may disrupt backup and recovery processes as well as contingency planning efforts.

Recommendation 5.2

MCS, through its contract oversight responsibility, should require MAXIMUS to develop and execute system maintenance processes to ensure changes to architecture are updated in the system security documents.

[19] HHS Information Security Standards and Guidelines Controls Catalog, § 7.9 Maintenance, MA-2 Controlled Maintenance, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015).

MCS should consider tailored contractual remedies to compel MAXIMUS to develop procedures and processes that require system and security documentation to be updated after system maintenance is performed.

Management Response

Action Plan

MCS is actively taking a number of steps to enhance its contract monitoring and oversight control activities. MCS will work with MAXIMUS to develop and execute system maintenance processes for updates on the security documents. MCS CAPM will monitor MAXIMUS' responses and will pursue any contractual remedies available to compel performance.

Responsible Managers

CAPM Director and Enrollment Broker Operations Director

Target Implementation Date

June 2018

CONCLUSION

The IG Audit Division completed an audit of selected security controls over confidential HHS System information in the custody of MAXIMUS. The audit included an evaluation of IT security controls over the EBSSP and MAXeb applications. The IG Audit Division conducted site visits at MAXIMUS during January and February 2017.

MCS, HHS IT, and MAXIMUS share accountability for ensuring that state information systems are sufficiently safeguarded to protect confidential information from accidental or unauthorized viewing, access, or modifications.

The IG Audit Division concluded:

- MAXIMUS implemented adequate physical security in its primary data center to protect confidential information.
- Processes to monitor information systems activities were sufficient to identify and prevent harmful activities such as viruses on the network.
- HHSC had not developed a workflow process to ensure that all appropriate parties received and reviewed MAXIMUS' annual security plans, or that any comments, risks, and recommendations resulting from security plan reviews were captured, tracked, and communicated to information owners or the HHS ISO.
- MAXIMUS did not require Oracle to provide the IG Audit Division information requested and needed to evaluate the security of confidential HHS System information in the custody of Oracle, as required by the enrollment broker contract.
- MAXIMUS did not effectively manage access to information systems that contained confidential HHS System information.
- MAXIMUS password settings for the EBSSP and MAXeb applications did not comply with ISSG standards.
- MAXIMUS did not require Oracle to provide baseline configurations requested and needed to validate security of servers administered by Oracle that store or process confidential HHS System information.

- Oracle did not timely notify MAXIMUS of identified scan vulnerabilities, resulting in delayed actions to prioritize and remediate the vulnerabilities.

- MAXIMUS did not have adequate system maintenance processes to ensure documentation was updated to reflect changes, including changes impacting system security.

The IG Audit Division offered recommendations to HHSC which, when implemented, will result in MAXIMUS having:

- Properly reviewed and approved system security plans.

- Subcontractors who comply with audit requests for information and documentation.

- Segregation between production and development environments.

- Stronger account management practices and password configurations.

- Documented baseline server configurations.

- Timely prioritization and remediation of identified vulnerabilities.

- Well maintained system documentation that represents the operating environment.

The IG Audit Division thanks the management and staff of MCS, HHS IT, and MAXIMUS for their cooperation and assistance during the audit.

Appendix A: Objective, Scope, and Methodology

Objective

The objective of this audit was to assess the design and effectiveness of selected security controls over confidential HHS System information stored and processed by the Medicaid and CHIP enrollment broker, MAXIMUS.

Scope

The scope of the IT security audit of MAXIMUS included:

- MAXIMUS logical and physical security controls, including network access and authentication, designed to safeguard the MAXeb and EBSSP applications, and their associated databases, which process and store confidential HHS System information.

- MAXIMUS security plans and associated HHSC security plan review processes for fiscal years 2016 and 2017.

- MAXIMUS IT controls for physical security of data and equipment, user account management, information system monitoring, and vulnerability remediation efforts, from September 2015 through February 2017.

The scope included MAXIMUS' production environment, but did not include the system backup environment.

Methodology

To accomplish its objectives, the IG Audit Division collected information through discussions and interviews with responsible staff at HHSC and MAXIMUS, and reviewed the following documentation:

- Network penetration reports
- Service organization controls reports
- MAXIMUS security plans and associated IT contract deliverables
- MAXIMUS IT security policies and procedures

The IG Audit Division issued an engagement letter to MAXIMUS, providing information about the upcoming audit, and conducted fieldwork at MAXIMUS' facility in Austin, Texas, on January 17, 2017 and February 16, 2017. While on site, the IG Audit Division interviewed responsible personnel, observed, and tested password configurations and information security monitoring processes, and reviewed documentation relevant to describe the design of the control environment.

Criteria

The IG Audit Division used the following criteria to evaluate the information provided:

- 45 C.F.R. § 160 and § 164 (Feb. 20, 2013)
- 1 Tex. Admin. Code, § 202.1 and § 202.3 and Subchapter B (Mar. 17, 2015) and (Mar. 16, 2016)
- Enrollment Broker Operations and Texas Health Steps Outreach and Informing Agreement Between the Health and Human Services Commission and MAXIMUS, INC, HHSC Contract No. 529-10-0005-00001 (Oct. 2013)
- HHS Data Use Agreement V.7.4., HHSC Contract No. 529-10-0005-00001, Attachment 7 Security Guidelines and Procedures (Oct. 21, 2014)
- HHS Information Security Standards and Guidelines Controls Catalog, v. 5.1 (Mar. 11, 2013) through v. 6 (Sept. 21, 2015)
- HHS Information Security Plan Template v. 1.3 (July 2015) through v. 1.6 (May 2016)

Auditing Standards

GAGAS

The IG Audit Division conducted this audit in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the issues and conclusions based on our audit objectives. The IG Audit Division believes the evidence obtained provides a reasonable basis for our issues and conclusions based on our audit objectives.

ISACA

The IG Audit Division performs work in accordance with the IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals published by ISACA.

Appendix B: Testing Methodology

The IG Audit Division examined enrollment broker system logical and physical IT security controls for the period of September 2015 through February 2017. After a risk and controls assessment of IT security controls, the IG Audit Division performed testing of selected security controls over the MAXeb and EBSSP production environment and supporting infrastructure.

Information Security Oversight

The IG Audit Division examined processes over HHSC's review and acceptance of annual MAXIMUS system security plans for MAXeb and EBSSP to determine whether the plans were complete, accurate, and approved.

Privileged User Account Management

The IG Audit Division reviewed controls over privileged user access to determine whether controls were in place, adequately designed, and operating effectively, and whether privileged access to information systems was appropriate. The IG Audit Division tested privileged accounts for MAXeb and EBSSP.

Configuration Settings

The IG Audit Division interviewed MAXIMUS personnel and examined applicable IT policies and asserted controls for configuration settings. Additionally, Oracle provided no evidence of configuration settings for servers that process and store confidential HHS System information.

Information Systems Monitoring

The IG Audit Division interviewed MAXIMUS personnel and reviewed the controls asserted by MAXIMUS and Oracle to (a) determine whether virus management and network analytic tools were implemented and monitored to review the movement of data and use of the network by its workforce and (b) identify processes for monitoring and responding to security events on the MAXIMUS network.

Vulnerability Assessment and Remediation

The IG Audit Division reviewed the results of the recent vulnerability assessments conducted for MAXIMUS by Oracle, and examined the remediation plans to determine whether the activities detailed in the plans appeared designed to address identified risks.

Physical Security

The IG Audit Division performed an inspection of the Oracle data center to review the physical security controls in place to safeguard the MAXIMUS infrastructure.

Appendix C: Controls Tested

Control Group	Control Description	Control Issue Control Design (CD) or Control Effectiveness (CE)	Report Issue
Access Control (AC)			
AC-1	Policy and Procedures		N/A
AC-2	Account Management	CE	3.1
AC-2(1)	Automated System Account Management	CD	3.1
AC-5	Separation of Duties	CD	3.2
AC-6	Least Privilege	CD	3.2
AC-6(1)	(1) Authorize Access to Security Functions	CD	3.1 & 3.2
AC-7	Unsuccessful Logon Attempts	CD	3.1
AC-17	Remote Access	CE	N/A
Security Assessment and Authorization Control (CA)			
CA-1	Security Assessment and Authorization Policy and Procedures		N/A
CA-2	Security Assessments		N/A
CA-5	Plan of Action and Milestones		N/A
CA-6	Security Authorization		N/A
CA-7	Continuous Monitoring		N/A
Configuration Management (CM)			
CM-2	Baseline Configuration	Scope Limited	4.2
CM-3	Configuration Change Control	Scope Limited	4.2
CM-6	Configuration Settings	Scope Limited	4.2
CM-7	Least Functionality Priority/Baseline	Scope Limited	4.2
CM-8	Information System Component Inventory		N/A
CM-9	Configuration Management Plan	Scope Limited	4.2
Identification and Authentication (IA)			
IA-1	Identification and Authentication Policy and Procedures		N/A
IA-2	Identification and Authentication [Organization Users]	Scope Limited	3.1
IA-3	Device Identification and Authentication	Scope Limited	3.1
IA-8	Identification and Authentication [Non-organizational Users]	Scope Limited	3.1
Incident Response (IR)			
IR-1	Incident Response Policy and Procedures		N/A
IR-3	Incident Response Testing		N/A
IR-4	Incident Handling		N/A
IR-5	Incident Monitoring		N/A
IR-6	Incident Reporting	CE	5.1
IR-8	Incident Response Plan		N/A

Control Group	Control Description	Control Issue Control Design (CD) or Control Effectiveness (CE)	Report Issue
Physical and Environmental Protection Controls (PE)			
PE-3	Physical Access Control		N/A
PE-6	Monitoring Physical Access		N/A
Maintenance			
MA-2	Controlled Maintenance	CE	5.2
Planning Controls (PL)			
PL-1	Security Planning Policy and Procedures		N/A
PL-2	System Security Plan	CD	1
PL-8	Information Security Architecture		N/A
Risk Assessment Control			
RA-1	Risk Assessment Policy and Procedures		N/A
RA-2	Security Categorization		N/A
RA-3	Risk Assessment		N/A
RA-5	Vulnerability Scanning		N/A

Appendix D: Maximus Management Comment

January 31, 2018

Steve Sizemore, CIA, CISA, CGAP
Performance Audit Director
Inspector General
Texas Health and Human Services Commission
PO Box 85200, MC1310
Austin, TX 78708-5200

Dear Mr. Sizemore:

Inspector General
Texas Health and Human Services Commission
PO Box 85200, MC1310
Austin, TX 78708-5200

MAXIMUS, INC. (MAXIMUS) and its subcontractors provide services to the State of Texas Health and Human Services Commission (HHSC) pursuant to the Enrollment Broker Operations and Texas Health Steps Outreach and Informing Agreement between the HHSC and MAXIMUS (Agreement) executed in October, 2013. The Agreement allows HHSC to audit MAXIMUS subcontractors.

We are providing this comment letter in connection with audit of security controls over confidential HHSC System information at MAXIMUS conducted from November 2015 through February 2016. The parties also worked together to put in place a non-disclosure agreement with Oracle to enable the onsite audit of the Oracle data center. This portion of the audit took place on April 26-27, 2017.

The objective of the audit was to assess the design and effectiveness of selected security controls over confidential HHSC System information stored and process by the Medicaid enrollment broker, MAXIMUS.

The scope of the audit of the enrollment broker system included the period of September 2015 through the end of fieldwork in April 2017. The scope of the audit included testing the design and operating effectiveness of selected security controls over the Enrollment Broker (MAXeb) and Enrollment Broker Self Service Portal (EBSSP) applications, and supporting infrastructure. Fieldwork encompassed the production and development environments and did not include the system backup environment.

1891 METRO CENTER DRIVE | RESTON, VIRGINIA 20190 | 703.251.8500 | 703.251.8240 FAX | WWW.MAXIMUS.COM

We note that OIG recommendations 3.1, 3.2, 4.1 have been completed and recommendations 4.2, 5.1 and 5.2 are targeted to be completed by end of June 2018.

The purpose of this letter is to provide certain responses to the following findings in the audit.

Issue 2: Oracle Limited Access to Information

The draft audit report states that "Oracle, the MAXIMUS infrastructure and hardware services subcontractor, did not provide information needed for the IG to fully evaluate and conclude on the effectiveness of security controls over confidential HHS System information hosted at Oracle's data center. By not providing the information, Oracle created an audit scope limitation that prevented the IG from fully achieving the audit objective, which was to assess the design and effectiveness of selected security controls over HHS System confidential information stored and processed by MAXIMUS."

MAXIMUS Response:

MAXIMUS provides the following response to this assessment.

Before the audit was conducted in April 2017, Oracle stated that it would not provide access to any Oracle assets and that it does not permit third parties to conduct its own security scans. Oracle does not allow any third-party access to Oracle Managed Cloud Services due to security and privacy considerations as Oracle is charged to maintain the security and integrity of its services environment to secure all customer content.

The audit took place over two days in Austin, TX from April 26 -27, 2017. The audit was conducted by Norm Blevins (Oracle) with assistance from two other Oracle personnel, Frances Carlson (Dir, Managed Security Services) and Pat Fitzsimmons (Security Services Manager). For purposes of the audit, Oracle set up live interviews, document reviews, and process demonstrations in lieu of releasing hardcopy documentation. Oracle does not share certain security or customer management process information in either hardcopy or softcopy outside of Oracle to protect the integrity and security of such information.

During the audit Oracle presented information regarding:

- system access and authentication / user access controls;
- vulnerability assessment and remediation
- system settings and configurations; and
- security posture/intrusion detection.

Oracle also provided the Service Organization Controls (SOC) 2 audit report of the Oracle facility, which was prepared by the auditor Ernst & Young LLP, at the onset of the audit. Section IV of the SOC 2 audit report ("Description of Criteria, Controls, Tests and Results of Testing") contains a description of the tests that were carried out by the auditor as well as the test results and auditor observations.

Oracle answered questions about and demonstrated system settings and configurations. Oracle demonstrated using an online system to show how user access is managed and answered questions about and demonstrated system settings and configurations. After the audit there was no follow-up request to Oracle for additional information regarding configuration settings.

During the audit, Oracle discussed the Oracle Production Acceptance process which is used to harden the customer environments prior to Go Live. Visual evidence of the process was provided. The use of Audit Vault in the customer's environment also was demonstrated.

Change Management was addressed via the My Oracle Support – Request for Change training, which was demonstrated and can be made available by MAXIMUS. All other processes are described in the Security Practices Guide and Tested as part of the SOC 2.

Oracle also performs external scans in accordance with the HIPAA Security Services Schedule. These scans are performed quarterly on MAXIMUS-specified environments. Reports of such scans were made available.

In summary Oracle provided the following:

a. System access and authentication materials[1];
b. Vulnerability assessment and remediation / user access controls
c. System settings;
d. Security posture/intrusion detection;
e. SOC 2 audit report, prepared by auditor Ernst & Young LLP, at the onset of the audit;
f. A demonstration on how user access is managed;
g. Documentation outlining User Password Management;
h. Implementation vs policy evidence;

i. Oracle Production Acceptance process which is used to harden the customer environments prior to Go Live.
j. A demonstration regarding the use of Audit Vault in the MAXIMUS' environment.

MAXIMUS believes the IG Audit Division was provided sufficient information to evaluate and determine the effectiveness of security controls over confidential HHS System information hosted at the Oracle data center. Additionally, the confidential information processed by and stored in the enrollment broker system is adequately protected from unauthorized access, loss, and disclosure.

[1] Although requested, Oracle did not provide a list of Oracle users who have access to the system.

- 4 -

OIG Recommendation 2:

"MCSD, through its contract oversight responsibility, should require MAXIMUS to cause its subcontractors to comply with contractual requirements related to audits and inspections, and to consider tailored contractual remedies to require compliance."

MAXIMUS believes that it has fully complied with its contract oversight responsibilities related to audits of its subcontractors. However, MAXIMUS will work with HHSC to determine if improvements can be made.

Bruce Perkins
Sr. Vice President
Deputy General Counsel
MAXIMUS, INC.

(Date)

Auditor Comments

The IG Audit Division respects the MAXIMUS position that sufficient information was provided to determine the security of confidential HHS System information hosted at the Oracle data center. However, the MAXIMUS comment letter does not include relevant information we believe warrants comment.

The IG Audit Division worked with MAXIMUS, and then Oracle, from November 2016 through April 2017, a period of six months, in an effort to satisfy conditions Oracle stated were necessary for the auditors to gain access to the Oracle facility and conduct audit testing. This included negotiating and signing a non-disclosure agreement not required under the IG's authority to audit. Fieldwork for the audit was initially expected to conclude in January 2017, so efforts to gain access to Oracle delayed the audit by at least four months.

While on site at Oracle on April 26 and 27, 2017, the IG Audit Division was limited to viewing documents on an overhead projector and observing (a) demonstrations of processes for authenticating access, (b) management of passwords and selected settings or parameters for passwords, (c) processes for identifying outside threats, and (d) procedures for promoting changes from development to production environments.

In addition, Oracle did not provide information the IG Audit Division requested, including (a) a list of all users with access to systems storing confidential HHS System information, (b) password parameters and settings associated with access to confidential HHS System information, and (c) configuration settings for servers that store and process large volumes of confidential HHS System information.

The demonstrations provided by Oracle enabled the IG Audit Division to observe the existence of some of Oracle's control processes, but were not sufficient to allow the IG Audit Division to conclude on the effectiveness of the control environment, resulting in a scope limitation and Issue 2.

Appendix E: Report Team and Distribution

Report Team

The IG staff members who contributed to this audit report include:

- Steve Sizemore, CIA, CISA, CGAP, Audit Director
- Melissa Larson, CIA, CISA, CFE, Audit Manager
- James A. Hicks, CISA, IT Audit Project Manager
- Fred Ramirez, CISA, IT Staff Auditor
- Joseph Mader, CPA, Staff Auditor
- Lawrence Gambone, Quality Assurance Reviewer
- Scott Miller, Senior Audit Operations Analyst

Report Distribution

Health and Human Services

- Charles Smith, Executive Commissioner
- Cecile Erwin Young, Chief Deputy Executive Commissioner
- Kara Crawford, Chief of Staff
- Heather Griffith Peterson, Chief Operating Officer and Acting Chief Information Officer
- Victoria Ford, Chief Policy Officer
- Karen Ray, Chief Counsel
- Karin Hill, Director of Internal Audit
- Enrique Marquez, Deputy Executive Commissioner of Medical and Social Services
- Stephanie Muth, State Medicaid Director, Medicaid and CHIP Services
- Tony Owens, Deputy Associate Commissioner, Health Plan Monitoring and Contract Services
- Ivan Libson, Deputy Associate Commissioner, Program Enrollment and Support
- Grace Windbigler, Director, Managed Care Compliance and Operations

- Dana Collins, Director, Contract Administration and Provider Monitoring
- Shirley Erp, HHS Chief Information Security Officer
- PJ Fritsche, Director, Health Services Systems
- Sandra Knight, Director, Enrollment Broker Operations

MAXIMUS

- Melinda Metteauer, Senior Vice President and Enrollment Broker Director

Appendix F: IG Mission and Contact Information

The mission of the IG is to prevent, detect, and deter fraud, waste, and abuse through the audit, investigation, and inspection of federal and state taxpayer dollars used in the provision and delivery of health and human services in Texas. The senior leadership guiding the fulfillment of IG's mission and statutory responsibility includes:

- Sylvia Hernandez Kauffman, Inspector General
- Christine Maldonado, Chief of Staff and Deputy IG for Operations
- Olga Rodriguez, Senior Advisor and Director of Policy and Publications
- Roland Luna, Deputy IG for Investigations
- Brian Klozik, Deputy IG for Medicaid Program Integrity
- David Griffith, Deputy IG for Audit
- Quinton Arnold, Deputy IG for Inspections
- Alan Scantlen, Deputy IG for Data and Technology
- Judy Hoffman-Knobloch, Interim Deputy IG for Medical Services
- Anita D'Souza, Chief Counsel

To Obtain Copies of IG Reports

- IG website: https://oig.hhsc.texas.gov

To Report Fraud, Waste, and Abuse in Texas HHS Programs

- Online: https://oig.hhsc.texas.gov/report-fraud
- Phone: 1-800-436-6184

To Contact the Inspector General

- Email: OIGCommunications@hhsc.state.tx.us
- Mail: Texas Health and Human Services Commission
  Inspector General
  P.O. Box 85200
  Austin, Texas 78708-5200
- Phone: 512-491-2000