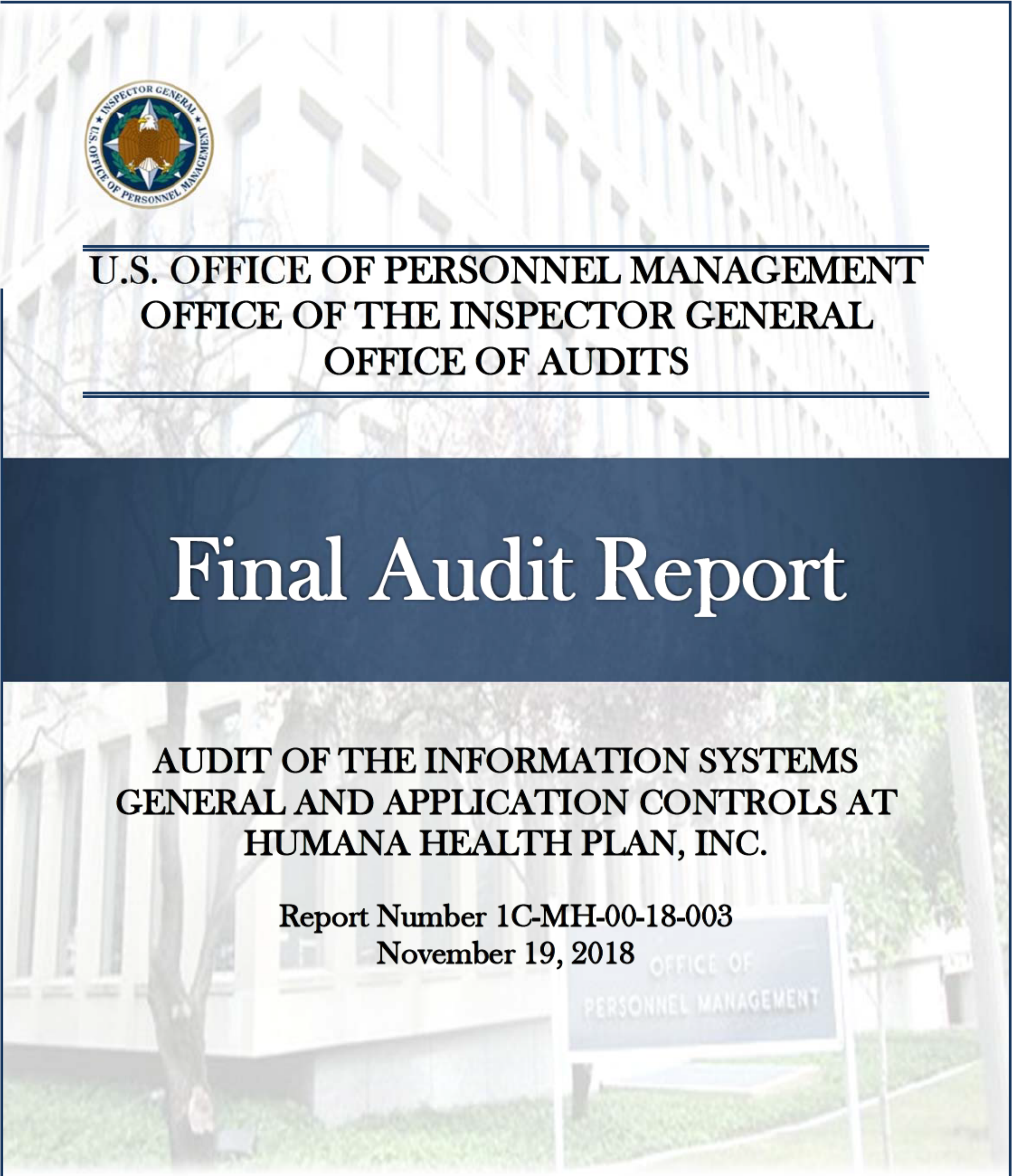
U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT HUMANA HEALTH PLAN, INC.

Report Number 1C-MH-00-18-003
November 19, 2018



EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Humana Health Plan, Inc.

Report No. 1C-MH-00-18-003 **November 19, 2018**

Why Did We Conduct the Audit?

Humana Health Plan, Inc. (Humana) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in Humana's information technology (IT) environment.

What Did We Audit?

The scope of this audit centered on the information systems used by Humana to process and store data related to insurance claims for FEHBP members.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of Humana's IT security controls determined that:

- Humana has established an adequate security management program.
- Humana's physical and logical access controls could be improved to prevent unauthorized access to the data centers by implementing multi-factor authentication for all privileged users.
- Humana could improve its network security posture by implementing data loss prevention on its servers and a formal process to ensure that weaknesses identified from vulnerability scanning are remediated in a timely manner.
- Humana has documented and approved a formal configuration management policy. However, Humana does not routinely audit security configuration settings for its mainframe and [redacted] systems.
- Humana has documented contingency plans that are tested on a routine basis.
- Humana has implemented many controls over its claims adjudication process to ensure that FEHBP claims are processed accurately.

ABBREVIATIONS

FEHBP	**Federal Employees Health Benefits Program**
FISCAM	**Federal Information System Controls Audit Manual**
Humana	**Humana Health Plan, Inc.**
IT	**Information Technology**
NIST SP	**National Institute of Standards and Technology Special Publication**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**

TABLE OF CONTENTS

I. BACKGROUND

This final audit report details the findings, conclusions, and recommendations resulting from the audit of general and application controls over the information systems responsible for processing Federal Employees Health Benefits Program (FEHBP) data by Humana Health Plan, Inc. (Humana).

The audit was conducted pursuant to FEHBP contracts CS 1570, 1773, 1895, 2110, 2931, 2940, and 2887; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations Chapter 1, Part 890. The audit was performed by the U.S. Office of Personnel Management's (OPM) Office of the Inspector General (OIG), as established by the Inspector General Act of 1978, as amended.

The Federal Employees Health Benefits Act, enacted on September 28, 1959, established the FEHBP to provide health insurance benefits for Federal employees, annuitants, and qualified dependents. The provisions of the Federal Employees Health Benefits Act are implemented by OPM through regulations codified in Title 5, Chapter 1, Part 890 of the Code of Federal Regulations. Health insurance coverage is made available through contracts with various carriers that provide service benefits, indemnity benefits, or comprehensive medical services.

This was our first audit of the information technology (IT) general and application controls at Humana. All Humana personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The objectives of this audit were to evaluate controls over the confidentiality, integrity, and availability of FEHBP data processed and maintained in Humana's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to Humana's claims processing system.

SCOPE AND METHODOLOGY

This performance audit was conducted in accordance with the Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of Humana's internal controls through interviews and observations, as well as inspection of various documents, including IT and other related organizational policies and procedures. This understanding of Humana's internal controls was used in planning the audit by determining the extent of compliance testing and other auditing procedures necessary to verify that the internal controls were properly designed, placed in operation, and effective.

The scope of this audit centered on the information systems used by Humana to process medical insurance claims and/or store the data of Humana members. The business processes reviewed are primarily located in Louisville, Kentucky.

The onsite portion of this audit was performed in January and February of 2018. We completed additional audit work before and after the on-site visits at our office in Washington, D.C. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general and application controls in place at Humana as of March 2018.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Humana. Due to time constraints, we did not verify the reliability of the data used to complete some of our audit steps, but we determined that it was adequate to achieve our audit objectives. However, when our objective was to assess computer-generated data, we completed audit steps necessary to obtain evidence that the data was valid and reliable.

In conducting this audit we:

- Gathered documentation and conducted interviews;

- Reviewed Humana's business structure and environment;

- Performed a risk assessment of Humana's information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office's Federal Information System Controls Audit Manual (FISCAM); and

- Conducted various compliance tests to determine the extent to which established controls and procedures are functioning as intended. As appropriate, we used judgmental sampling in completing our compliance testing.

Various laws, regulations, and industry standards were used as a guide to evaluating Humana's control structure. These criteria include, but are not limited to, the following publications:

- Title 48 of the Code of Federal Regulations;

- U.S. Office of Management and Budget Circular A-130;

- U.S. Office of Management and Budget Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;

- COBIT 5: A Business Framework for the Governance and Management of Enterprise IT;

- U.S. Government Accountability Office's FISCAM;

- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Revision 1, An Introduction to Computer Security: The NIST Handbook;

- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and
- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether Humana's practices were consistent with applicable standards. While generally compliant with respect to the items tested, Humana was not in complete compliance with all standards, as described in Section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY MANAGEMENT

The security management component of this audit involved examining the policies and procedures that are the foundation of Humana's overall IT security program. We evaluated Humana's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

Humana has developed a risk management methodology and remediation plans to address weaknesses identified.

Humana has developed both a risk management methodology and remediation plans to address weaknesses identified during risk assessments. Humana also maintains adequate human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that Humana has not implemented adequate controls over its security management process.

B. ACCESS CONTROLS

Access controls are the policies, procedures, and techniques used to prevent or detect unauthorized physical or logical access to sensitive resources.

We examined the physical access controls at Humana's facilities and datacenters. We also examined the logical access controls protecting sensitive data on Humana's network environment and applications.

The access controls observed during this audit include, but were not limited to:

- Procedures for appropriately granting and removing physical access to facilities and datacenters; and

- Procedures for appropriately granting and adjusting logical access to applications and software resources.

The following sections document opportunities for improvement related to Humana's access controls.

1) Data Center – Multi-factor Authentication

Humana operates its own primary and secondary data centers. Access to each data center is controlled with employee badges and proximity access readers. Humana has established several different physical access zones within the data centers and only grants access based on an individual's role or job function. However, access to the secured areas within the data center does not require multi-factor authentication (e.g., an access card and a unique pin). As Humana has made the business decision to implement zone-based access throughout its data center, this weakness could allow an unauthorized individual access to the secured area.

NIST SP 800-53, Revision 4, provides guidance for adequately controlling physical access to information systems containing sensitive data.

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to confidential data.

Recommendation 1

We recommend that Humana implement multi-factor authentication requirements for the secured areas within the data center.

Humana Response:

"We agree with the recommendation. [redacted]**."**

OIG Comment:

As a part of the audit resolution process, we recommend that Humana provide OPM's Healthcare and Insurance Office, Audit Resolution Group with evidence when it has fully implemented this recommendation. This statement also applies to subsequent recommendations in this audit report that Humana agrees to implement.

2) Privileged User – Multi-factor Authentication

[redacted]

[redacted]

NIST SP 800-53, Revision 4, requires that "The information system implements multifactor authentication for local access to privileged accounts."

[redacted]

Recommendation 2

We recommend that Humana implement multi-factor authentication for privileged user accounts on its information systems.

Humana Response:

"We agree with the recommendation. We have an ongoing strong authentication program in place and will continue to expand the program [redacted]***."***

C. NETWORK SECURITY

Network security includes the policies and controls used to prevent or monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. We evaluated Humana's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit. We observed the following controls in place:

- Preventive controls at the network perimeter;
- Security event monitoring throughout the network; and
- A documented incident response program.

The following section documents an opportunity for improvement related to Humana's network security controls.

1) Data Loss Prevention

[redacted]

[redacted]

NIST SP 800-53, Revision 4, requires that "The organization prevents the unauthorized exfiltration of information across managed interfaces." NIST SP 800-122 also provides guidance and recommendations on protecting confidential and personal information on information systems.

Failure to implement a data loss prevention solution on servers increases the risk of unauthorized data exfiltration and extensive damage to the organization's reputation.

Recommendation 3

We recommend that Humana configure and implement [redacted]

Humana Response:

"We agree with the finding and are evaluating options to mitigate the identified risk. We have an ongoing data loss prevention program in place [redacted]***. We will work with the OPM Audit Resolution Group on a final plan."***

D. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. We evaluated Humana's management of the configuration of its servers and databases. Our review found the following controls in place:

Humana maintains documented security configuration standards for all operating platforms in use.

- System configuration changes are documented;
- A formal change approval process; and

- Vulnerability scanning procedures are implemented.

The sections below document areas for improvement related to Humana's configuration management controls.

1) Security Configuration Auditing

Humana has documented standard security configurations for all of the organization's servers and workstations. Humana also performs routine audits on its [redacted] server and workstation configurations using an automated tool. However, a routine audit of security configurations has not been implemented for the mainframe and [redacted] operating platforms.

NIST SP 800-53, Revision 4, states that an organization must monitor and control "changes to the configuration settings in accordance with organizational policies and procedures" and also requires that configurations be routinely checked for all of the organization's systems. Additionally, FISCAM requires "Current configuration information [to] be routinely monitored for accuracy. Monitoring should address the . . . baseline and operational configuration of the hardware, software, and firmware that comprise the information system."

Failure to implement configuration compliance auditing using approved security configuration standards increases the risk that servers are not configured appropriately, which if left undetected can create a potential gateway for unauthorized access or malicious activity.

Recommendation 4

We recommend that Humana improve its configuration auditing process to routinely audit [redacted] server configuration settings against an approved configuration standard.

Humana Response:

"We agree with the recommendation. We will implement by 1Q/19."

Recommendation 5

We recommend that Humana improve its configuration auditing process to routinely audit mainframe configuration settings against an approved configuration standard.

Humana Response:

"We agree with the recommendation. We will implement by 1Q/19."

2) Vulnerability Management

[redacted]

FISCAM states, "When weaknesses are identified, the related risks should be reassessed, appropriate corrective or remediation actions taken, and follow-up monitoring performed to make certain that corrective actions are effective." Additionally, NIST SP 800-53, Revision 4, requires organizations to remediate legitimate vulnerabilities identified in information systems and hosted applications.

Failure to remediate vulnerabilities in a timely manner increases the risk that bad actors could exploit system weaknesses for malicious purposes.

Recommendation 6

We recommend that Humana implement a process to ensure that vulnerabilities identified from vulnerability scanning are remediated in a timely manner.

Humana Response:

"We agree with the recommendation. [redacted] ***"***

E. CONTINGENCY PLANNING

Humana has adequate controls related to contingency planning.

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. We reviewed the following elements of Humana's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disruptive events occur:

- Disaster recovery plan (e.g., recovery of hardware and software infrastructure);
- Business continuity plan (e.g., people and business processes);
- Contingency plan tests; and
- Emergency response procedures.

We determined that the contingency planning documentation contained the critical elements suggested by NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems." Humana has identified and prioritized the systems and resources that are critical to business operations, and has developed detailed procedures to recover those systems and resources.

Nothing came to our attention to indicate that Humana has not implemented adequate controls related to contingency planning.

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting Humana's claims adjudication process. This included a review of the processes related to claims adjudication: application configuration management, claims processing, enrollment and provider debarment.

1) Application Configuration Management

We evaluated the policies and procedures governing application development and change control for Humana's claims processing systems.

Humana has implemented policies and procedures related to application configuration management, and adopted a system development life cycle methodology that IT personnel follow during routine software modifications. We observed the following controls related to testing and approval of software modifications:

- Policies and procedures that allow modifications to be tracked throughout the change process;

- Unit, integration, and user acceptance testing are conducted in accordance with industry standards; and
- A group independent from the software developers moves code between development and production environments to ensure separation of duties.

Nothing came to our attention to indicate that Humana has not implemented adequate controls related to the application configuration management process.

2) Claims Processing System

We evaluated the business process controls associated with Humana's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data.

We determined that Humana has implemented policies and procedures to help ensure that:

- Claims are properly input and tracked to ensure timely processing;
- Claims are monitored as they are processed through the system with real time tracking of the system's performance; and
- Claims scheduled for payment are actually paid.

Nothing came to our attention to indicate that Humana has not implemented adequate controls over its claims processing systems.

3) Enrollment

We evaluated Humana's procedures for managing its database of member enrollment data. Enrollment information is received either electronically or in paper format, and either automatically or manually loaded into the claims processing system. All enrollment transactions are fully audited to ensure information is entered accurately and completely.

Nothing came to our attention to indicate that Humana has not implemented adequate controls over the enrollment process.

4) Debarment

Humana has documented procedures for updating its claims system with debarred provider information. Humana is notified by OPM that an update to the debarment list is available to download. Humana reviews the updated list to determine if any debarred providers have active contracts with Humana. To update the system, Humana uses the monthly debarment list, which only shows that month's changes in provider debarment status, rather than the full debarment list. If an active provider is identified on this list, the provider is manually flagged in the claims processing system. However, Humana does not have a quality assurance process to ensure that this manual process is completed accurately.

Failure to review the manual debarment process increases the risk that Humana never detects a debarred provider status. This could result in improperly paying debarred provider claims.

Recommendation 7

We recommend that Humana implement a quality assurance review process to ensure that all debarred providers from the OPM OIG debarment list are accurately inputted into the claims processing system in a timely manner.

Humana Response:

"Humana implemented a quality review 2Q/18 to ensure debarred providers are captured and accurately flagged in the claims processing system."

OIG Comment:

In response to the draft audit report, Humana provided evidence that a process has been implemented to ensure that all debarred providers from the OPM OIG debarment list are accurately inputted into the claims process system. No further action is required.

APPENDIX

July 10, 2018

[redacted], Auditor-In-Charge
Information Systems Audits Group
United States Office of Inspector General

Dear [redacted],

The table below shows our comments/responses to the draft audit report (Report No. 1C-MH-00-18-003) provided to Humana on May 15, 2018.

OIG Finding	Humana Responses
Debarment	Humana implemented a quality review 2Q/18 to ensure debarred providers are captured and accurately flagged in the claims processing system.
Privileged User Multi-factor Authentication	We agree with the recommendation. We have an ongoing strong authentication program in place and will continue to expand the program [redacted].
Data Loss Prevention	We agree with the finding and are evaluating options to mitigate the identified risk. We have an ongoing data loss prevention program in place [redacted] We will work with the OPM Audit Resolution Group on a final plan.
Security Configuration Management – Mainframe	We agree with the recommendation. We will implement by 1Q/19.
Security Configuration Management – [redacted]	We agree with the recommendation. We will implement by 1Q/19.
Vulnerability Management	We agree with the recommendation. [redacted].
Data Center - Multi-factor Authentication	We agree with the recommendation. [redacted].

Respectfully,

[redacted], SVP, Chief Information Security Officer

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100