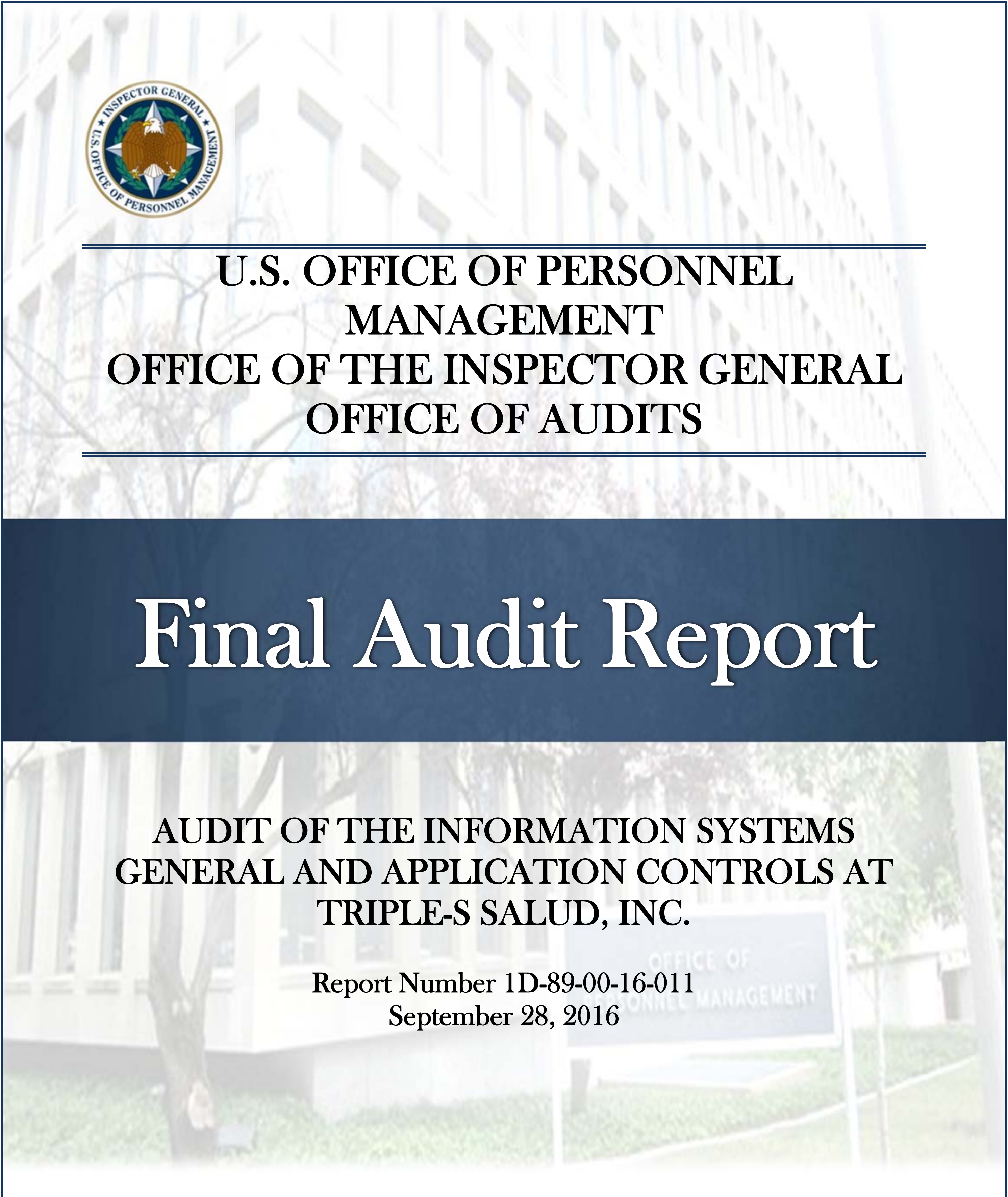

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT TRIPLE-S SALUD, INC.

Report Number 1D-89-00-16-011
September 28, 2016

-- CAUTION --

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage (*http://www.opm.gov/our-inspector-general*), caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Triple-S Salud, Inc.

Report No. 1D-89-00-16-011 **September 28, 2016**

Background

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

Why Did We Conduct the Audit?

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

What Did We Audit?

The scope of this audit centered on the information systems used by Triple-S Salud 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 the IT security controls of Triple-S Salud determined that:

- Triple-S Salud has established a security management program.
- Triple-S Salud has implemented a variety of physical and logical access controls. However, we noted that:
  - [redacted];
  - [redacted] and
  - Physical access controls at the data center could be improved.
- Triple-S Salud has implemented a thorough incident response plan.
- Triple-S Salud has implemented a variety of network security controls, but we noted the following opportunities for improvement:
  - Triple-S Salud has not formally documented approved configuration settings for firewalls within the network;
  - Triple-S Salud does not conduct routine reviews of its firewall settings against the approved configuration settings;
  - Credentialed vulnerability scans of the entire network are not routinely conducted;
  - There is no process in place to track and remediate known security vulnerabilities; and
  - There are numerous servers running unsupported versions of operating systems.
- Triple-S Salud has developed formal configuration management policies. However, we noted several opportunities for improvement related to configuration management:
  - Security configuration settings are not approved or documented;
  - Security configuration audits are not routinely performed;
  - Multiple critical software patches are missing; and
  - Several servers contain insecure configuration settings.
- Triple-S Salud's business continuity and disaster recovery plans contain the elements suggested by relevant guidance and publications.
- Triple-S Salud has implemented many controls in its claims adjudication processes to ensure that FEHBP claims are processed accurately and completely. However, our claims testing identified issues related to medical editing and patient history.

ABBREVIATIONS

CIS	Center for Internet Security
CFR	Code of Federal Regulations
EoL	Information System End-of-Life
FEHBP	Federal Employees Health Benefits Program
FISCAM	Federal Information Security Controls Audit Manual
GAO	U.S. Government Accountability Office
HIO	OPM Healthcare and Insurance Office
IT	Information Technology
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology’s Special Publication
OIG	Office of the Inspector General
OMB	U.S. Office of Management and Budget
OPM	U.S. Office of Personnel Management
Triple-S Salud	Triple-S Salud, Inc.
VPN	Virtual Private Network

TABLE OF CONTENTS

Page

I. BACKGROUND

This final 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) claims by Triple-S Salud, Inc. (Triple-S Salud or Plan).

The audit was conducted pursuant to FEHBP contract CS 1090; 5 U.S.C. Chapter 89; and 5 Code of Federal Regulations (CFR) 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 FEHBP was established by the Federal Employees Health Benefits Act (the Act), enacted on September 28, 1959. The FEHBP was created to provide health insurance benefits for federal employees, annuitants, and qualified dependents. The provisions of the Act are implemented by OPM through regulations codified in Title 5, Chapter 1, Part 890 of the CFR. 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 Triple-S Salud's information technology (IT) general and application controls. All Triple-S Salud 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 Triple-S Salud's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Segregation management;
- Contingency planning; and
- Application controls specific to Triple-S Salud's claims processing system.

Scope and Methodology

This performance audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States. Accordingly, we obtained an understanding of Triple-S Salud's internal controls through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of Triple-S Salud'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 Triple-S Salud to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in San Juan, Puerto Rico.

Triple-S Salud is a subsidiary of Triple-S Management Corporation, which offers a wide range of insurance products and services in Puerto Rico. Another subsidiary of Triple-S Management Corporation, TriServe Tech, manages data center operations and information security for all Triple-S Management Corporation subsidiaries. The operations of TriServe Tech were considered within the scope of this audit.

The on-site portion of this audit was performed in December of 2015 and January of 2016. We completed additional audit work before and after the on-site visit 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 Triple-S Salud as of January 2016.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Triple-S Salud. 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 review we:

- Gathered documentation and conducted interviews;
- Reviewed Triple-S Salud’s business structure and environment;
- Performed a risk assessment of Triple-S Salud’s information systems environment and applications, and prepared an audit program based on the assessment and the U.S. Government Accountability Office’s (GAO) 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 Triple-S Salud’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 (OMB) Circular A-130, Appendix III;
- OMB 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;
- GAO’s FISCAM;
- National Institute of Standards and Technology’s Special Publication (NIST SP) 800-12, An Introduction to Computer Security: The NIST Handbook;
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems;
- 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, 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 Triple-S Salud's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, Triple-S Salud 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 the examination of the policies and procedures that are the foundation of Triple-S Salud's overall IT security program. We evaluated Triple-S Salud's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

Triple-S Salud maintains a series of thorough IT security policies and procedures.

Triple-S Salud has implemented a series of formal policies and procedures that comprise its security management program. Triple-S Salud has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. We also reviewed Triple-S Salud's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that Triple-S Salud does not have an adequate security management program.

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 of Triple-S Salud's facilities and data center. We also examined the logical controls protecting sensitive data on Triple-S Salud's network environment and claims processing related applications.

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

- Procedures for appropriately granting and removing physical access to facilities and the data center;
- Procedures for appropriately granting, adjusting, and removing logical access;
- Procedures for routinely reviewing user access; and
- Adequate environmental controls over the data center.

The following sections document opportunities for improvement related to Triple-S Salud's access controls.

1. Privileged User Authentication

Access to Triple-S Salud's privileged user (i.e., system administrator) accounts requires the use of a password management tool for temporary privilege elevation – administrators must first authenticate to the tool before being granted privileged credentials. Although this control adds security value, we expect all FEHBP contractors to also have [redacted] for administrator-level access to information systems.

The Federal government requires [redacted]. Although Triple-S Salud is not a government entity, it is a custodian of sensitive healthcare data of Federal employees, and we therefore recommend that Triple-S Salud implement this control for privileged users at a minimum. NIST SP 800-53, Revision 4, states that information systems should implement [redacted]. Failure to implement [redacted] increases the risk that privileged user credentials could be compromised and that unauthorized users could access sensitive and proprietary data.

Recommendation 1

We recommend that Triple-S Salud implement [redacted] for privileged user access to all information systems.

Plan Response:

"We agree with the recommendation. We will expand the use of the [redacted]***;*** [redacted] ***to include domain administrator accounts by acquiring a password vault under a vendor agreement license."***

OIG Comment:

As part of the audit resolution process, Triple-S Salud should provide OPM's Healthcare and Insurance Office (HIO) with evidence that this recommendation has been addressed. This statement also applies to all subsequent recommendations in this report that Triple-S Salud agrees to implement.

2. Remote Access

Remote access to Triple-S Salud's information systems is granted via a virtual private network (VPN). Employees with approved VPN remote access can authenticate to the

Triple-S Salud network by using [redacted].

NIST SP 800-53, Revision 4, states that privileged and non-privileged users should use [redacted] for remote access. Implementing [redacted] for remote access to information systems reduces the risk of unauthorized access to sensitive data.

<u>Recommendation 2</u>

We recommend that Triple-S Salud require [redacted] for privileged and non-privileged users to access systems remotely.

<u>Plan Response:</u>

"We agree with the recommendation. We have implemented the integration of the [redacted] system for [redacted] for all authorized remote access users. View Attachment 1."

<u>OIG Comment:</u>

The evidence provided by Triple-S Salud in response to the draft audit report indicates that the Plan has implemented [redacted] for privileged and non-privileged users to access systems remotely; no further action is required.

3. Data Center Physical Access

Physical access to Triple-S Salud's data center is controlled by proximity card readers. The data center has additional physical access controls such as real-time video monitoring, security guards, and a man-trap[1] in the lobby. However, the data center does not have the following controls that we typically observe at similar facilities:

Triple-S Salud's data center physical controls could be improved.

- [redacted]
- [redacted]

[1] **Man-trap:** A man-trap is a small room with two sets of doors, and one set of doors cannot be opened until the other is closed and locked. Man-traps are used to better control entry to secure areas and to prevent piggybacking.

In the near future, Triple-S Salud plans to commercially rent a portion of its data center space and IT resources to outside organizations. Representatives from these commercial clients will be granted physical access to Triple-S Salud's data center, further increasing the importance of strong physical access controls like the two mentioned above. Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to Triple-S Salud's data center that contains sensitive IT resources and confidential data.

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

Recommendation 3

We recommend that Triple-S Salud improve the physical access controls of its data center. At a minimum, the computer room should have [redacted].

Plan Response:

"We agree with the recommendation. Our data center location is highly secure, and we only grant limited access to authorized personnel. It maintains a 24/7 security guards monitoring service. Nonetheless, we will acquire a security system under a vendor agreement where [redacted] ***and*** [redacted] ***for the access door will be installed in our data center."***

C. Network Security

Network security includes the policies and controls used to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

We evaluated Triple-S Salud's network security program and reviewed the results of several automated vulnerability scans that we performed during this audit. We observed the following controls in place:

- Documented incident response plan;
- Encryption of sensitive data; and
- Network controls to prevent rogue devices.

However, we noted the following opportunities for improvement related to Triple-S Salud's network security controls.

1. **Documented Firewall Policy**

Triple-S Salud's network has firewall devices installed at key locations on the network perimeter and demilitarized zone. However, Triple-S Salud has not formally documented the approved settings (i.e., a firewall security configuration standard) for these firewalls.

NIST SP 800-41, Revision 1, states that "A firewall policy dictates how firewalls should handle network traffic for specific IP addresses and address ranges, protocols, applications, and content types (e.g., active content) based on the organization's information security policies."

Without a firewall security configuration standard, the organization cannot routinely audit the current/actual settings of the firewalls to compare them to the approved settings, which potentially increases the organization's exposure to insecure traffic and vulnerabilities.

Recommendation 4

We recommend that Triple-S Salud document formal firewall security configuration standards.

Plan Response:

"We partially agree with the recommendation. We currently maintain a firewall configuration baseline process for the activation, modification and deactivation of firewall rules. In addition, we have a quarterly review process of the firewall rules to identify which rules are no longer required or that require adjustment. Nonetheless, we will modify our current firewall rule baseline policy, as to include a group of updated settings for the organizations' firewalls. We include a copy of the policy and procedure document to be considered as evidence for our baseline process. View Attachment 2."

OIG Comment:

The evidence provided by Triple-S Salud in response to the draft audit report indicates that Triple-S Salud has created adequate guidance for implementing and documenting approved firewall security configuration standards; no further action is required.

2. Firewall Configuration Review

Triple-S Salud stated that its IT personnel periodically review firewall settings on an ad-hoc basis. However, as stated above, it is not possible to thoroughly audit the current/actual settings of the firewall without a firewall security configuration standard to compare them to.

NIST SP 800-53, Revision 4, states that an organization should monitor and control changes to configuration settings. NIST SP 800-41 states that "Policy rules … should also be reviewed periodically to ensure they remain in compliance with security policy."

Failure to routinely audit firewall settings could allow an insecure configuration to remain undetected, potentially exposing the network to unmanaged risk.

Recommendation 5

We recommend that Triple-S Salud perform routine reviews that compare the current settings of its firewalls against an approved firewall security configuration standard.

Plan Response:

"We partially agree with the recommendation. We have policies and procedures for our baseline configuration as stated and evidenced in Attachment 2. Nonetheless, we will expand our quarterly review process to include a routine comparison of current firewall rules against our defined firewall rule baseline. We are requesting a revision of the written recommendation in order to state that we maintain policies and procedures for firewall rule baseline review."

OIG Comment:

The evidence provided by Triple-S Salud in response to the draft audit report establishes a quarterly review procedure to ensure that the current firewall rules in place are in compliance with the approved firewall security configuration standard. We recommend that Triple-S Salud provide OPM's HIO with evidence that these firewall configuration reviews are routinely conducted as stated in the Plan's Standard Operating Procedure.

3. Vulnerability Management Program

Triple-S Salud contracts with a third-party vendor to conduct quarterly security assessments of its information systems. These assessments are conducted from outside the Triple-S Salud network boundary without the benefit of system visibility provided by an internal credentialed vulnerability assessment. Triple-S Salud also contracts with another third-party vendor to conduct penetration testing on an annual basis.

While these assessments certainly add value by potentially identifying penetration access points to get into the network, they do not provide a comprehensive assessment of the security of IT resources within the network.

As part of this audit we performed an internal credentialed vulnerability assessment on a sample of servers in the Triple-S Salud network. Our test work identified many internal servers with vulnerabilities that Triple-S Salud's other vulnerability assessments had not detected.

NIST SP 800-53, Revision 4, states that the organization should scan for "vulnerabilities in the information system and hosted applications [on a routine basis] and when new vulnerabilities potentially affecting the system/applications are identified and reported …."

Failure to perform comprehensive internal vulnerability scanning increases the risk that Triple-S Salud's systems could become compromised and sensitive data lost or stolen.

Recommendation 6

We recommend that Triple-S Salud implement a process to routinely conduct credentialed vulnerability scanning on its entire network environment. Triple-S Salud should also implement a process to track and remediate the vulnerabilities detected during these assessments.

Plan Response:

"We partially agree with the recommendation. We conduct a quarterly vulnerability scan for our external network IT assets and bi-annual for our internal network IT assets. These results are tracked and reported to management during internal status meetings. We include a copy of the Internal comprehensive assessment of IT security scans report within the network. View Attachment 3. Nonetheless, we have included additional Information Security team members who will be dedicated to the analysis and the coordination of the vulnerabilities identified in these reports. View Attachment 4."

OIG Comment:

The evidence provided in response to the draft audit report demonstrates that a third-party conducted a vulnerability scan against Triple-S Salud's firewall ruleset. However, the intent of our recommendation is for Triple-S Salud to conduct routine credentialed vulnerability scans on its entire network environment and to implement a process to track and remediate the vulnerabilities detected during these assessments. The assessments should include all technical assets such as internal servers, databases, and network devices. Triple-S Salud should provide OPM's HIO with evidence such as comprehensive vulnerability scan reports and documentation demonstrating that there is a process in place to track and remediate identified vulnerabilities.

4. System Lifecycle Management

Our vulnerability assessment identified numerous servers running unsupported versions of operating systems. Software vendors typically announce projected dates (known as end-of-life dates) for when they will no longer provide support or distribute security patches for their products. In order to avoid the risk associated with operating unsupported software, organizations must have a methodology in place to phase out software before it reaches its end-of-life date.

NIST SP 800-53, Revision 4, recommends that organizations replace "information system components when support for the components is no longer available from the developer, vendor, or manufacturer …." NIST SP 800-53, Revision 4, also states that "Unsupported components … provide a substantial opportunity for adversaries to exploit new weaknesses discovered in the currently installed components."

Failure to upgrade system software could leave information systems vulnerable to known vulnerabilities without any remediation available.

<u>Recommendation 7</u>

We recommend that Triple-S Salud develop policies and procedures to ensure that information systems are upgraded to current versions prior to the end of vendor support.

<u>Plan Response:</u>

"We agree with the recommendation. As part of our periodic review to ensure compliance with Information Systems End-of-Life (EoL) cycles, we identified collision processes under key business vendors, examining schematic difficulties within their system abilities, thus conflicting with our systems' migration procedures. We will develop an Information Technology Infrastructure Library based IT Asset Management process with a set of business practices that join financial, contractual, and inventory functions to support EoL

cycle management and strategic decision making. An Information Technology upgrade/EoL Management Policy and Procedure document will be drafted."

D. Configuration Management

A configuration management program is the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. We evaluated Triple-S Salud's management of the configuration of its computer servers and databases.

The sections below document areas for improvement related to Triple-S Salud's configuration management controls.

1. Security Configuration Standards

Triple-S Salud has not documented formal security configuration standards for its computer servers or databases. A security configuration standard is a formally approved document that contains details on how security settings should be configured for a specific operating platform.

NIST SP 800-53, Revision 4, states that an organization should establish and document "configuration settings for information technology products employed within the information system … that reflect the most restrictive mode consistent with operational requirements …."

Triple-S Salud does not maintain approved security configuration standards for its operating platforms and databases.

In addition, NIST SP 800-53, Revision 4, states that an organization must develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved system configuration settings increases the risk the system may not be configured in a secure manner.

Recommendation 8

We recommend that Triple-S Salud document approved security configurations for all operating platforms and databases deployed in its technical environment.

Plan Response:

"We agree with the recommendation. We maintain security guidelines, nonetheless we will update our policies to include further strengthened security processes for our

computer servers and databases, and integrate different technology components used recommended by the Center of Internet Security (CIS).”

2. Security Configuration Auditing

As noted above, Triple-S Salud does not maintain approved security configuration standards for its operating platforms and databases, and therefore cannot effectively audit its system’s security settings (i.e., there are no approved settings to which to compare the actual settings).

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.

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 a thorough configuration compliance auditing program increases the risk that insecurely configured servers exist undetected, creating a potential gateway for malicious virus and hacking activity.

Recommendation 9

We recommend that Triple-S Salud implement a process to routinely audit the configuration settings of servers and databases to ensure they are in compliance with the approved security configuration standards.

Plan Response:

“We agree with the recommendation. We currently have an Information Security Team in charge of monitoring compliance, and maintaining audit trail events for all security controls, including sensitive accounts within our organization. Nonetheless, we will implement an automated tool to facilitate and improve the current monitoring process, as well as integrate the IT Infrastructure team to respond to identified issues. View Attachment 4.”

OIG Comment:

The evidence provided by Triple-S Salud in response to the draft audit report indicates that the Information and Cyber Security Department is responsible for monitoring compliance and maintaining security control audit trails. Triple-S Salud should provide OPM’s HIO with evidence that the Information Security Team is routinely auditing the approved security configuration settings that the Plan has agreed to implement.

3. Patch Management

Triple-S Salud uses an automated tool to install operating system and third-party patches on all systems. According to Triple-S Salud's policy, critical security patches should be installed quarterly after being tested in a development environment. However, the results of our vulnerability scans identified multiple critical operating system and third-party patches that were missing from numerous hosts in Triple-S Salud's environment. Each of these patches were released more than 90 days before the date our vulnerability scans were conducted and should have been implemented as part of Triple-S Salud's patch management process.

NIST SP 800-53, Revision 4, states that security-relevant software and firmware updates should be installed within timeframes defined by the organization. Failure to install software patches could leave systems exposed to known vulnerabilities that could allow an attacker unauthorized access to sensitive data.

At the conclusion of our field work, Triple-S Salud informed us that it redesigned its patch management process and that it plans to deploy critical patches on a monthly basis.

Recommendation 10

We recommend that Triple-S Salud provide OPM's contracting office with evidence that it is routinely installing critical patches in accordance with its patch management policy.

Plan Response:

"We agree with the recommendation. We have updated our Patch Vulnerability Management (PVM) process in order to be NIST 800-30 compliant. The PVM process is supported by the acquired and implemented [redacted]. This process includes reports of the current patches installed, which will be provided to OPM in a quarterly timeframe. View Attachment 5."

OIG Comment:

The evidence provided by Triple-S Salud in response to the draft audit report indicates that an adequate standard operating procedure has been developed related to patch and vulnerability management. Triple-S Salud should provide OPM's HIO with evidence that critical patches are routinely installed in accordance with the patch management policy.

4. Server Configuration Settings

The results of our vulnerability scans indicate that several servers contain insecure configurations that could allow hackers or unauthorized users to gain access to sensitive and proprietary information. The detailed results of these scans will not be included in our audit report, but were provided directly to Triple-S Salud.

NIST SP 800-53, Revision 4, states that Triple-S Salud must scan for vulnerabilities in the information system and hosted applications, analyze the reports, and remediate legitimate vulnerabilities. Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

Recommendation 11

We recommend that Triple-S Salud remediate the specific technical weaknesses outlined in the vulnerability scanning audit inquiry issued during the audit.

Plan Response:

"We agree with the recommendation. We are currently modifying our vulnerability remediation process as to amend the technical weaknesses outlined during the audit."

E. Contingency Planning

We reviewed the following elements of Triple-S Salud's contingency planning program to determine whether controls are in place to prevent or minimize interruptions to business operations when disastrous events occur:

- Disaster recovery plan;
- Business continuity plan;
- Disaster recovery 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." Triple-S Salud has identified and prioritized the systems and resources that are critical to business operations, and have developed detailed procedures to recover those systems and resources.

Nothing came to our attention to indicate that Triple-S Salud 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 Triple-S Salud's processing of Federal data.

1. Application Configuration Management

We evaluated the policies and procedures governing application development and change control of Triple-S Salud's claims processing systems.

Triple-S Salud utilizes a commercial off-the-shelf claims processing application and does not have the ability to develop or directly make changes to the source code. All change requests are submitted to the software vendor for design and development. Triple-S Salud tests all changes provided by the vendor in a separate environment prior to implementation into the production environment.

Triple-S Salud has adequate controls over its application configuration management.

We do not have any concerns regarding Triple-S Salud's application configuration management process.

2. Claims Adjudication Process

We evaluated the input, processing, and output controls associated with Triple-S Salud's claims adjudication process. We determined that Triple-S Salud has implemented policies and procedures to help ensure that:

- Paper claims that are received in the mail room or dropped-off at Triple-S Salud facilities are 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.

We did not detect any opportunities for improvement related to Triple-S Salud's claims adjudication process.

3. Enrollment

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

We do not have any concerns regarding Triple-S Salud's enrollment process.

4. Debarment

Triple-S Salud has documented procedures for reviewing provider files for debarments and suspensions. Triple-S Salud downloads the OPM OIG debarment list monthly and manually compares the list to its provider information system; any potential matches are reviewed and confirmed. Debarred providers are then suspended in the system. Any claim submitted by a debarred provider is flagged by Triple-S Salud to adjudicate through the OPM OIG debarment process to include initial member notification, a 15-day grace period, and then denial.

Nothing came to our attention to indicate that Triple-S Salud has not implemented adequate controls over the debarment process.

5. Application Controls Testing

We conducted a test on Triple-S Salud's claims adjudication application to validate the system's processing controls. The exercise involved processing test claims designed with inherent flaws and evaluating the manner in which Triple-S Salud's system adjudicated the claims.

Our test results indicate that Triple-S Salud's claims processing application has controls and system edits in place to identify many of our test scenarios. In addition to the edits in the claims processing system, Triple-S Salud also performs what they refer to as a "verification ready to pay process." This process involves a manual analysis before claims are paid to ensure accuracy. The analysis looks at duplicate payments, certain diagnosis codes, providers, modifiers, and all claims over [redacted]. Triple-S Salud has an Audit and Investigation office that is responsible for recovering funds and investigating fraud after payments have been made.

The sections below document opportunities for improvement related to Triple-S Salud's claims application controls.

i. Medical Editing

Our claims testing exercise identified several scenarios where Triple-S Salud's claims processing application failed to detect medical inconsistencies. For each of the following scenarios, a test claim was processed and paid without encountering any edits detecting the inconsistency:

- *Invalid Place of Service (Professional)* – (1) a procedure code for a [redacted] with place of service codes for a [redacted] and another at a [redacted]; and (2) a procedure code for a [redacted] with a place of service code for a [redacted]; and
- *Age/Procedure Inconsistencies (Professional)* – (1) an [redacted] procedure on a [redacted] female; and (2) a [redacted] female [redacted].

During our audit we were informed that the claims processing system's place of service medical edits are created based on coding relationships established by third-party industry sources such as the American Medical Association and Centers for Medicare and Medicaid Services. If a coding relationship has not been established for a specific place of service code by an industry source, claims will process without pending for review. The place of service codes used in our test scenarios did not have an established coding relationship in Triple-S Salud's claims processing system, and therefore a risk exists that benefits are not being paid appropriately.

Failure to detect age to procedure inconsistencies increases the risk that benefits are being paid for procedures that were not actually performed.

Recommendation 12

We recommend that Triple-S Salud assess the feasibility of implementing technical system edits that address the scenarios of our testing exercise.

Plan Response:

"We agree with the recommendation. We will be implementing, as part of our claims processing system, specified medical edits and codification identifiers established for procedures given in the noted place of service; as well as detection for age to procedure inconsistencies."

ii. Patient History

Our claims testing exercise identified several scenarios where Triple-S Salud's claims processing system failed to detect patient history inconsistencies. For each of the following scenarios, a test claim was processed and paid without encountering any edits detecting the inconsistency:

- *Near Duplicate Claims (Professional) (Hospital)* – (1) a test claim with a [redacted] procedure code was submitted that processed and paid appropriately. Another claim was submitted with the same [redacted] procedure code, same patient, same date of service, with a different provider that also processed and paid; (2) a test claim with a [redacted] procedure code was submitted that processed and paid appropriately. Another claim was submitted with the same [redacted] procedure code, same patient, same date of service, with a different provider that also processed and paid; and
- *Procedure History (Hospital)* – (1) a test claim was submitted for a woman that [redacted] and was processed and paid appropriately. Another test claim was submitted with a date of service a month later for the same woman [redacted] and the claim processed and paid; (2) a test claim was submitted for a woman that [redacted] and was processed and paid appropriately. A subsequent test claim was submitted for the same woman having another [redacted] less than a month later that processed and paid.

Triple-Salud informed us that these scenarios would be detected with the manual "verification ready to pay process" described above. However, this process could be improved by implementing technical edits that would automatically detect claims with potential patient history issues.

Failure to implement a technical control to detect these patient history issues increases the risk of human error and that benefits are being paid for procedures that were not actually performed.

<u>Recommendation 13</u>

We recommend that Triple-S Salud assess the feasibility to implement system edits that compare claims against historical claims data to identify potential patient history issues.

<u>Plan Response:</u>

"We partially agree with the recommendation. The test based scenarios included a technical edit (519) with a WARN identifier for duplicates received in our system.

We are soliciting a review and change for this recommendation, as we have the edits in place. View Attachment 6. Nonetheless, we will enhance our system that maintains edits for patient history issues, in order to update our current technical edits with a simplified comparison process against current historical claims data. View Attachment 7.”

OIG Comment:

The evidence provided by Triple-S Salud in response to the draft audit report indicates that edits to detect duplicate claims based on our test scenarios are now in place. The ruleset now identifies revenue codes that are inclusive of other revenue codes billed on the same day. We recommend that Triple-S Salud continue to enhance the system with technical edits to detect the patient history issues we identified. After the enhancements are in place, please provide OPM’s HIO with evidence of the updated technical edits.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], IT Auditor-In-Charge

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], Group Chief

[redacted], Senior Team Leader

APPENDIX

July 11, 2016

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

[redacted]:

Pursuant to FEHBP contract CS 1090, our information technology controls provide appropriate methods that ensure the confidentiality, integrity, and availability for medical insurance claims data of Federal Employee Health Benefits Program members.

In response to OIG's Draft Report number 1D-89-00-16-01, we include our comments, as well as supplementary documents to consider as completed actions taken for our implemented procedures.

I. Access Controls

A. Privileged User Authentication

Triple S Salud Response: We agree with the recommendation. We will expand the use of the [redacted]; two-factor authentication system to include domain administrator accounts by acquiring a password vault under a vendor agreement license.

B. Remote Access

Triple S Salud Response: We agree with the recommendation. We have implemented the integration of the [redacted] two-factor authentication system for [redacted] for all authorized remote access users. View Attachment 1.

C. Data Center Physical Access

Triple S Salud Response: We agree with the recommendation. Our data center location is highly secure, and we only grant limited access to authorized personnel. It maintains a 24/7 security guards monitoring service. Nonetheless, we will acquire a security system under a vendor agreement where [redacted] and [redacted] for the access door will be installed in our data center.

II. Network Security

A. Documented Firewall Baseline

Triple S Salud Response: We partially agree with the recommendation. We currently maintain a firewall configuration baseline process for the activation, modification and deactivation of firewall rules. In addition, we have a quarterly review process of the firewall rules to identify which rules are no longer required or that require adjustment. Nonetheless, we will modify our current firewall rule baseline policy, as to include a group of updated settings for the organizations' firewalls. We include a copy of the policy and procedure document to be considered as evidence for our baseline process. View Attachment 2.

B. Firewall Configuration Review

Triple S Salud Response: We partially agree with the recommendation. We have policies and procedures for our baseline configuration as stated and evidenced in Attachment 2. Nonetheless, we will expand our quarterly review process to include a routine comparison of current firewall rules against our defined firewall rule baseline. We are requesting a revision of the written recommendation in order to state that we maintain policies and procedures for firewall rule baseline review.

C. Vulnerability Management Program

Triple S Salud Response: We partially agree with the recommendation. We conduct a quarterly vulnerability scan for our external network IT assets and bi-annual for our internal network IT assets. These results are tracked and reported to management during internal status meetings. We include a copy of the Internal comprehensive assessment of IT security scans report within the network. View Attachment 3. Nonetheless, we have included additional Information Security team members who will be dedicated to the analysis and the coordination of the vulnerabilities identified in these reports. View Attachment 4.

D. System Lifecycle Management

Triple S Salud Response: We agree with the recommendation. As part of our periodic review to ensure compliance with Information Systems End-of-Life (EoL) cycles, we identified collision processes under key business vendors, examining schematic difficulties within their system abilities, thus conflicting with our systems' migration procedures. We will develop an Information Technology Infrastructure Library based IT Asset Management process with a set of business practices that join financial, contractual, and inventory functions to support EoL cycle management and strategic decision making. An Information Technology upgrade/EoL Management Policy and Procedure document will be drafted.

III. Configuration Management

A. Security Configuration Baselines

Triple S Salud Response: We agree with the recommendation. We maintain security guidelines, nonetheless we will update our policies to include further strengthened security processes for our computer servers and databases, and integrate different technology components used recommended by the Center of Internet Security (CIS).

B. Configuration Baseline Auditing

Triple S Salud Response: We agree with the recommendation. We currently have an Information Security Team in charge of monitoring compliance, and maintaining audit trail events for all security controls, including sensitive accounts within our organization. Nonetheless, we will implement an automated tool to facilitate and improve the current monitoring process, as well as integrate the IT Infrastructure team to respond to identified issues. View Attachment 4.

C. Patch Management

Triple S Salud Response: We agree with the recommendation. We have updated our Patch Vulnerability Management (PVM) process in order to be NIST 800-30 compliant. The PVM process is supported by the acquired and implemented [redacted]. This process includes reports of the current patches installed, which will be provided to OPM in a quarterly timeframe. View Attachment 5.

D. Server Configuration Settings

Triple S Salud Response: We agree with the recommendation. We are currently modifying our vulnerability remediation process as to amend the technical weaknesses outlined during the audit.

IV. Claims Adjudication

A. Application Controls Testing

i. Medical Editing

Triple S Salud Response: We agree with the recommendation. We will be implementing, as part of our claims processing system, specified medical edits and codification identifiers established for procedures given in the noted place of service; as well as detection for age to procedure inconsistencies.

ii. Patient History

Triple S Salud Response: We partially agree with the recommendation. The test based scenarios included a technical edit (519) with a WARN identifier for duplicates received in our system. We are soliciting a review and change for this recommendation, as we have the edits in place. View Attachment 6. Nonetheless, we will enhance our system that maintains edits for patient history issues, in order to update our current technical edits with a simplified comparison process against current historical claims data. View Attachment 7.

Sincerely,

[redacted]
Federal Programs Administration Manager
Triple-S Salud Inc.

cc: Madeline Hernandez Urquiza, President
[redacted], Corporate Accounts Administration Vice President
[redacted], Healthcare Finance Vice President

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