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

# Final Audit Report

## AUDIT OF INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT THE SPECIAL AGENTS MUTUAL BENEFIT ASSOCIATION

Report Number 1B-44-00-14-065
October 28, 2015

**-- 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 Information Systems General and Application Controls at the Special Agents Mutual Benefit Association*

**Report 1B-44-00-14-065** **October 28, 2015**

**Background**

The Special Agents Mutual Benefit Association (SAMBA) 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 SAMBA's information technology (IT) environment.

**What Did We Audit?**

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

**Michael R. Esser**
*Assistant Inspector General for Audits*

**What Did We Find?**

On January 29, 2015, we issued a Flash Audit Alert (FAA) to bring to the Office of Personnel Management's immediate attention serious concerns we had regarding SAMBA's ability to adequately secure sensitive Federal data. The FAA contained three recommendations related to inadequate IT policies and procedures and critical security vulnerabilities on SAMBA's computer servers. We also issued a draft audit report on June 2, 2015 with additional findings and recommendations.

In the time since the FAA and draft reports were issued, SAMBA has made significant progress in improving its IT security posture and has already implemented most of our recommendations. Most important, SAMBA has developed a comprehensive set of IT security policies and procedures that provide the foundation of its IT security management program. While work certainly remains to continue to improve IT security at SAMBA, the organization has many more controls in place protecting sensitive Federal data than it did when we began this audit.

The areas of concern that have not been fully addressed (or adequate supporting documentation has not been provided) include:

- The physical access controls protecting SAMBA's facilities and data center could be improved.
- SAMBA has not provided evidence that it has implemented an intrusion detection/prevention system.
- SAMBA has not provided evidence that it has implemented controls to encrypt user workstation hard drives and removable media devices.
- Our vulnerability scans indicated that several critical vulnerabilities that have known exploits exist in SAMBA's technical environment.
- Our claims testing exercise identified several scenarios where SAMBA's claims system failed to detect medical inconsistencies.

# ABBREVIATIONS

| | |
|---|---|
| **the Act** | **The Federal Employees Health Benefits Act** |
| **CFR** | **Code of Federal Regulations** |
| **FEHBP** | **Federal Employees Health Benefits Program** |
| **FISCAM** | **Federal Information Systems Control Audit Manual** |
| **GAO** | **U.S. Government Accountability Office** |
| **HIO** | **Healthcare and Insurance Office** |
| **IT** | **Information Technology** |
| **SAMBA** | **Special Agents Mutual Benefit Association** |
| **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** |
| **Plan** | **Special Agents Mutual Benefit Association** |

# TABLE OF CONTENTS

# 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) data by the Special Agents Mutual Benefit Association (SAMBA or Plan).

This was our first audit of SAMBA's information technology (IT) general and application controls. On January 29, 2015, we issued a Flash Audit Alert (FAA) to bring to OPM's immediate attention serious concerns we had regarding SAMBA's ability to adequately secure sensitive Federal data. The FAA contained three recommendations related to inadequate IT policies and procedures and critical security vulnerabilities on SAMBA's computer servers. Those FAA recommendations have been rolled into this final audit report. We also issued a draft audit report on June 2, 2015 with additional findings and recommendations. SAMBA's comments on the draft report were considered in preparing the final report and are attached as the Appendix to this report.

In the time since the FAA and draft reports were issued, SAMBA has made significant progress in improving its IT security posture and has already implemented many of our recommendations. While work certainly remains to further improve IT security at SAMBA, the organization has many more controls in place protecting sensitive Federal data than it did when we began this audit.

The audit was conducted pursuant to FEHBP contract CS 1074; 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.

All SAMBA 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 SAMBA's IT environments. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network Security;
- Configuration management;
- Segregation of duties;
- Contingency planning; and
- Application controls specific to SAMBA's member encounters process.

**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 SAMBA'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 SAMBA'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 SAMBA to process medical insurance claims for FEHBP members, with a primary focus on the claims adjudication applications. SAMBA claims are processed through a claims adjudication system called [redacted]. The business processes reviewed are primarily located in Rockville, Maryland.

The on-site portion of this audit was performed from December 2014 through January 2015. 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 SAMBA as of January 2015.

In conducting our audit, we relied to varying degrees on computer-generated data provided by SAMBA. 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 SAMBA's business structure and environment;
- Performed a risk assessment of SAMBA'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 SAMBA'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;
- Information Technology Governance Institute's CobiT: Control Objectives for Information and Related Technology;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Introduction to Computer Security;
- 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 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, Computer Security Incident Handling Guide.

**Compliance with Laws and Regulations**

In conducting the audit, we performed tests to determine whether SAMBA's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, SAMBA 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 SAMBA's overall IT security program. We evaluated SAMBA's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls. We also reviewed SAMBA's human resources policies and procedures related to hiring, training, transferring, and terminating employees.

**SAMBA developed IT security policies in the months immediately preceding this audit, but they were not comprehensive.**

The sections below outline our concerns with SAMBA' security management program.

1. **IT Policies and Procedures**

   SAMBA developed a set IT security policies in the months immediately preceding this audit. However, these policies did not address several critical IT security topics. In addition, the existing policies are not accompanied by detailed procedures describing how the policies should be implemented and enforced. IT security policies are the critical foundation of a strong information security program, as these documents provide guidance on how IT security should be managed at a specific organization.

   FISCAM states that "Entities should have policies, plans, and procedures that clearly describe the entity's security management program. . . . The security management program should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security and those who own, use, or rely on the entity's computer resources." It also states, "Finally, to be effective, the security program documentation should be maintained to reflect current conditions. It should be periodically reviewed and, if appropriate, updated and reissued to reflect changes in risk due to factors such as changes in entity mission or the types and configuration of computer resources in use."

   Without a well-designed security program, security controls may be inadequate, responsibilities may be unclear, misunderstood, and improperly implemented, and controls may be inconsistently applied.

   **<u>Recommendation 1 (Flash Audit Alert Recommendation 1)</u>**

   We recommend that SAMBA develop comprehensive IT security policies and procedures. At a minimum, SAMBA should implement policies and procedures related to the following topics:

   - IT Security Management
   - Auditing of User Access

- IT Security Training Requirements
- Auditing/Monitoring User and Administrator Activity
- Log Monitoring
- Appropriate Use of Software
- Segregation of Duties
- Vulnerability Remediation
- Server Configuration Management, Baseline Configurations, and Auditing Server Configuration
- Firewall Management

***<u>Plan's Response:</u>***

***"SAMBA has developed and adopted comprehensive IT security policies and procedures for the above. These are attached below as A1-R1. Those indicated as "CAP" were previously provided to OPM OIG in our Corrective Action Plan progress monitoring submission."***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates that SAMBA has developed IT security policies and procedures for the topics noted in the recommendation; no further action is required.

**Recommendation 2 (Flash Audit Alert Recommendation 2)**

We recommend that SAMBA develop detailed procedures to complement the following existing policies, and ensure that they include the level of detail necessary to meet the Plan's long term goals and to establish a secure IT environment:

- Access Control;
- Business Continuity Plan/Testing; and
- Disaster Recovery Plan/Testing;
- Security Incident Response.

***Plan's Response:***

***"SAMBA has developed detailed procedures to compliment the above existing policies. These are attached below as A1-R2."***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates that SAMBA has developed procedures to complement the existing policies noted in the recommendation; no further action is required.

**Recommendation 3**

We recommend that SAMBA implement a process to routinely review and update its IT security policies.

***Plan's Response:***

***"SAMBA has a Regulatory Compliance Committee (RCC). The RCC is responsible to routinely review SAMBA's compliance programs and policies and procedures. The committee meets on a[n] "as needed" basis and annually prior to the scheduled risk assessment. The RCC Charter is formally documented in the attached below as A1-R3."***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates SAMBA has developed a process to routinely review and update its IT security policies; no further action is required.

**2. Enterprise Risk Assessment**

SAMBA completed its first enterprise risk assessment in October 2014. However, prior to this assessment a routine process to evaluate risks at an enterprise level had not been implemented.

NIST SP 800-53 Revision 4, control RA-3, "Risk Assessment," states an organization needs to update its risk assessment on a routine basis or whenever there are significant changes to the information system or environment of operation, or other conditions that may impact the security state of the system.

Failure to conduct a routine risk assessment increases the risk of an organization being unaware of potential threats and vulnerabilities that may impact business.

**Recommendation 4**

We recommend SAMBA implement a procedure to perform routine enterprise risk assessments.

***Plan's Response:***

***"SAMBA has developed and implemented a Risk Management Policy. The Policy requires that a Risk Assessment be performed annually or upon significant change to an information system. The next Risk Assessment is scheduled for October, 2015. The Risk Management Policy is attached below as A2-R4."***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates SAMBA has developed an enterprise risk assessment policy and procedure; no further action is required.

### 3. Background Check Process

SAMBA performs background checks on new employees that include education verification and a high level social media review. However, this process does not include the industry best-practice of also performing a criminal background check or a check against OPM's debarment list.

**Recommendation 5**

We recommend that SAMBA reevaluate the elements included in its background check process. At a minimum it should implement a criminal record check and ensure hired individuals are not on the OPM debarment list.

***Plan's Response:***

***"SAMBA has reevaluated and updated its Background Check Policy & Procedures. The policy and procedures now require criminal background checks for all newly hired employees. SAMBA has verified that no current employees are on the OPM debarment list. The Background Check Policy & Procedures is attached below as A3-R5."***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates SAMBA has developed a background check procedure that includes a criminal record and OPM debarment list check; no further action is required.

### 4. Specialized IT Security Training Requirements

SAMBA employees are provided IT security awareness training on an annual basis. In addition to this training, SAMBA employees with elevated IT security responsibilities receive IT security training from outside sources. However, SAMBA has not documented standardized corporate training requirements for employees with specialized IT security responsibilities.

FISCAM requires employees with significant IT security responsibilities to receive specialized IT training.

Failure to document the training requirements for employees with specialized IT security responsibilities increases the potential that these individuals are not receiving the necessary training to adequately fulfill their important job function.

**Recommendation 6**

We recommend that SAMBA document the IT security training requirements for employees with significant security responsibilities.

***Plan's Response:***

***"SAMBA has modified its IT Security Training for All SAMBA Employees Policy and Procedures to include specific requirements for IT security-related job responsibilities. Documentation of completed specialized IT training and certifications will be maintained electronically. The IT Security Training for All SAMBA Employees Policy and Procedures is attached as A4-R6."***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates SAMBA has developed specific training requirements for employees with significant IT responsibilities; no further action is required.

## 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 SAMBA's facilities and data centers. We also examined the logical controls protecting sensitive data on SAMBA's network environment and claims processing-related applications.

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

- Access badges required for physical access across the facility;
- Strong environmental controls protecting the data center;
- Procedures for granting and revoking facilities access;
- Documented policies and procedures for granting and removing user access; and
- Documented password requirements.

The following section documents several opportunities for improvement related to SAMBA's access controls.

### 1. Physical Access Controls

**SAMBA's physical access controls could be improved.**

SAMBA's facility entrances are protected by a locked door requiring an access badge to open. The SAMBA data center also has the additional control of a numeric keypad paired with an electronic card reader. However, SAMBA does not have additional physical access controls that we typically see at similar organizations such as [redacted] or controls to prevent employees from [redacted].

FISCAM states that “Controls should accommodate employees who work at the entity’s facilities on an everyday basis; occasional visitors, such as employees of another entity facility or maintenance people; and infrequent or unexpected visitors. Physical controls vary, but include: manual door [or cipher key] locks, magnetic door locks that require the use of electronic keycards, [biometrics authentication,] entry logs, … security guards, photo IDs, [and] electronic and visual surveillance systems ….”

Also, FISCAM states that “By obtaining physical access to computer facilities and equipment, an individual could (1) obtain access to terminals or telecommunications equipment that provide input into the computer, (2) obtain access to confidential or sensitive information on magnetic or printed media, (3) substitute unauthorized data or programs, or (4) steal or inflict malicious damage on computer equipment and software.”

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to the SAMBA facility and data center and the sensitive IT resources and confidential data they contain. NIST SP 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” provides guidance for adequately controlling physical access to information systems containing sensitive data.

**Recommendation 7**

We recommend that SAMBA reassess its *facilities’* physical access management and implement controls that will ensure proper physical security to include at a minimum [redacted] and [redacted].

***Plan’s Response:***
***“SAMBA has installed*** [redacted] ***at the*** [redacted] ***We have contracted to install*** [redacted] ***at the same locations to be completed by September 1, 2015.”***

**OIG Comment:**
As part of the audit resolution process, we recommend that SAMBA provide OPM’s Healthcare and Insurance Office (HIO) with evidence that it has adequately implemented this recommendation in its entirety. This statement also applies to all subsequent recommendations in this audit report that SAMBA agrees to implement.

**Recommendation 8**

We recommend that SAMBA reassess its *data center’s* physical access management and implement controls that will ensure proper physical security to include at a minimum [redacted] and [redacted].

***Plan's Response:***

***"SAMBA has installed [redacted] to our data center [redacted]. We have contracted to install an [redacted] to be completed by September 1, 2015."***

### 2. Access Request Forms

SAMBA does not currently utilize a standardized access request form to manage the process of granting physical or logical access. Access is granted or adjusted by the security team when they receive an e-mail notification from human resources that an employee has been hired, transferred, or terminated. These notifications do not specify the level of access an employee requires.

FISCAM states that access authorizations should be documented on standard forms and maintained on file.

Failure to utilize a standard access request form increases the risk of an employee's access being mishandled, altered, unsupported, or above the minimal required for their job function.

**Recommendation 9**

We recommend that SAMBA implement and maintain on file a standardized access request form for both physical and logical access as a part of granting, modifying or removing access.

***Plan's Response:***

***"SAMBA has designed and implemented the use of a formal access request form for both physical and logical access.***

***(1) Physical Access Request Form is utilized to grant, modify or remove access to our facility.***
***(2) Logical Access Request Form is utilized to grant, modify or remove access to our claim processing system, email, voice mail, imaging system, personnel database, virtual private network, and accounting management system.***

***The completed forms require management approval, will indicate the minimum required access needed, and be maintained electronically for auditing purposes. We have updated our Access Control Policy and Procedures and Physical Security Policy to indicate use of these forms. The forms are attached below as B2-R9."***

**<u>OIG Comment:</u>**

Evidence was provided in response to the draft audit report that indicates SAMBA has implemented a formal access request form for both physical and logical access; no further action is required.

3. **Separation of Duties Policy**

Separation of duties is the concept of sharing responsibility of critical tasks between more than one individual as an internal control intended to prevent fraud and error. SAMBA has not developed and documented a separation of duties policy that defines what types of roles would be inappropriate for one individual to have.

NIST SP 800-53 Revision 4 Control AC-5 Separation of Duties states that an organization must document separation of duties of individuals and define information system access authorizations to support separation of duties.

Failure to document and implement controls to ensure separation of duties decreases an organizations ability to prevent fraud and error from a single individual.

By implementing Recommendation 1 in the above Security Management section, SAMBA will address the issue by developing a separation of duties policy.

**4. Physical Access Auditing**

SAMBA requires employees to turn in their physical access badges when their employment is terminated, and their accounts are disabled in the badge system. However, SAMBA does not currently have a routine audit process in place to ensure that access has been removed appropriately or to recertify access to existing active accounts to ensure that only approved individuals maintain access to secured areas.

NIST SP 800-53 Revision 4, “Control Physical Access Authorization,” states that an organization should routinely review the access list detailing authorized facility access by individuals. FISCAM also states that management should conduct regular reviews of individuals with physical access to sensitive areas to ensure such access is appropriate.

Failure to audit physical access to facilities and recertify access to secure areas increases the organization’s risk of unauthorized individuals gaining access to the facilities and information systems.

**Recommendation 10**

We recommend that SAMBA implement a process to routinely audit physical access to its facility. This audit should include verification that no active badge accounts exist for terminated employees, and that the level of access to existing employees remains appropriate.

***Plan's Response:***
***"SAMBA has implemented a process to routinely audit physical access to our facility. Our Physical Security Policy requires audits to be conducted at least quarterly. A "Badge Access List" is reviewed by the Security Officer and Human Resources Manager to verify employees are actively employed and access levels are appropriate for each individual. Results of the review process will be documented and maintained electronically. The Physical Security Policy is attached below as B4-R10."***

**OIG Comment:**
Evidence was provided in response to the draft audit report that indicates SAMBA has implemented a process to routinely audit physical access to its facility; no further action is required.

### 5. Access Monitoring

Monitoring user access is a critical component to an organization's security assurance process for information systems. However, SAMBA currently does not monitor access for general employees. SAMBA also does not monitor privileged user access or activity.

NIST SP 800-53 Revision 4, AC-2, "Account Management," states that organizations should monitor the user of information system accounts and monitor privileged role assignments and activities.

Failure to monitor general users and privileged user access increases the risk to an organization of insider attacks.

**Recommendation 11**

We recommend that SAMBA implement a process to log and monitor user access (logon and logoff activity) for both general and privileged users.

***Plan's Response:***
***"SAMBA has implemented a process to log and monitor user access for both general and privileged users. Our Network Vulnerability Scanning and Log Monitoring Policy require the use of a NetOps Check List. The NetOps Check List is used to document the Logs and***

***indicate who reviewed them. The [redacted] application is used to monitor logon and logoff activity of both general and privileged users. The logs are reviewed by Network Operations Staff with oversight by the Security Officer. A copy of our Network Vulnerability Scanning and Log Monitoring Policy is attached below as A5-R11."***

**OIG Comment:**
Evidence was provided in response to the draft audit report that indicates SAMBA has implemented a process to log and monitor user access; no further action is required.

**Recommendation 12**

We recommend that SAMBA implement a process to log and monitor all transaction activity of privileged users including, but not limited to, domain and database administrators.

***Plan's Response:***
***"SAMBA has implemented a process to log and monitor all transaction activity of all users, including privileged users. Our Network Vulnerability Scanning and Log Monitoring Policy and Procedures specify that logs are checked daily for activity and proper system functionality. The [redacted] application is used to monitor internet activity of all users including the activity of privileged users. The [redacted] batch report is utilized to monitor activity on the claim system database. [redacted] is utilized to monitor privileged users on the domain. The Network Operations Staff, with oversight by the Security Officer, is task[ed] with reviewing the daily logs. The Human Resource Manager reviews the Security Officer's access and activity with the assistance of the System Administrator. The claim system database batch reports are monitored by our Claims Department Manager or designee."***

**OIG Comment:**
Evidence was provided in response to the draft audit report that indicates SAMBA has implemented a process to log and monitor all transaction activity of privileged users; no further action is required.

## 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 SAMBA's network security program and also independently performed several automated vulnerability scans and compliance audits on SAMBA's computer servers and network devices. We noted the following opportunities for improvement related to network security controls.

### 1. Firewall Management

SAMBA has implemented firewalls to help secure the network environment supporting the claims processing system.  However, a firewall configuration/hardening policy has not been developed.  Without a firewall configuration standard, it is not possible for SAMBA to audit the current settings of the firewall for appropriateness.

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. . . .  The policy should also include specific guidance on how to address changes to the rule set.”

Failure to implement a thorough firewall configuration policy and continuously manage the devices’ settings increases the organization’s exposure to insecure traffic and vulnerabilities.

#### Recommendation 13

We recommend that SAMBA document a formal firewall management policy and configuration baseline.

***Plan’s Response:***

***“SAMBA has a formal Firewall Management Policy & Procedure and a documented firewall configuration baseline.  The policy includes specific guidelines to manage, update, and define the rule sets of SAMBA firewalls.  Our Firewall Management Policy & Procedure was provided in our response to Recommendation 1.  Our configuration baseline is attached below as C1-R13.”***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates SAMBA has developed and documented a formal firewall management policy and baseline configuration; no further action is required.

#### Recommendation 14

We recommend that SAMBA implement a process to conduct routine configuration reviews on its network firewalls to ensure performance and security optimization, as defined by the firewall management policy.

***<u>Plan's Response:</u>***

***"We have updated our Firewall Management Procedure to indicate that Firewall Rule sets and Configurations require quarterly review. The updated Firewall Management Policy & Procedure as well as documentation of a recent review is attached below as C1-R14."***

**<u>OIG Comment:</u>**

Evidence was provided in response to the draft audit report that indicates SAMBA has implemented a process to routinely review firewall configurations; no further action is required.

### 2. Intrusion Detection/Prevention

SAMBA does not currently have a standardized process in place to log security-related network events, and has not implemented an automated intrusion detection/prevention system within its network environment. At the time of audit we were informed by SAMBA personnel that they were in the process of acquiring an intrusion detection/prevention system and would be implementing it by the end of the second quarter of 2015.

NIST SP 800-53 Revision 4, control SI-4, "Information System Monitoring," requires that an organization monitor information to detect for access, attacks, and indicators of potential attacks. This control also states that an organization needs to deploy monitoring devices within the information system to collect essential information.

Failure to log security-related network events and implement an intrusion detection/prevention system increases the Plan's risk of malicious attacks going undetected and uncontrolled.

**<u>Recommendation 15</u>**

We recommend that SAMBA document the types of network activity that should be logged within its information systems and then modify its information systems to collect these logs.

***<u>Plan's Response:</u>***

***"SAMBA has implemented the [redacted] system. [redacted] provides SAMBA a process to log security related network events and the type of network activity within our information systems."***

**<u>OIG Comment:</u>**

Although SAMBA states that it has implemented a process to log security-related network events, no evidence was provided to support this statement. As part of the audit resolution process, we recommend that SAMBA provide OPM's HIO with evidence that it has fully implemented this recommendation.

**Recommendation 16**

We recommend that SAMBA implement an intrusion detection/prevention system.

***Plan's Response:***
***"SAMBA has implemented an intrusion detect/prevention system imbedded within our Firewall."***

**OIG Comment:**
Although SAMBA states that it has implemented an intrusion detection/prevention system, no evidence was provided to support this statement. As part of the audit resolution process, we recommend that SAMBA provide OPM's HIO with evidence that it has fully implemented this recommendation.

### 3. Media Encryption

SAMBA has not implemented controls to encrypt user workstation hard drives and removable media devices. SAMBA personnel informed the OIG that these functions would be implemented by the end of the second quarter of 2015.

FISCAM states that media controls should be implemented to control unauthorized access to digital media both within information systems and removed from them. FISCAM also states that information system digital media includes diskettes, magnetic tapes, hard drives, flash/thumb drives, compact disks, and digital video disks.

Failure to encrypt information system media increases SAMBA's risk for leaking personally identifiable information.

**Recommendation 17**

We recommend that SAMBA implement encryption controls on both internal and removable information system media.

***Plan's Response:***
***"Media controls have been implemented to control unauthorized access to digital media removed from the information system and within. All optical drives have been disabled from SAMBA workstations. In additions, SAMBA implemented [redacted] application that will encrypt all hard drives and any thumb drive that are utilized. All hard drives have been encrypted. SAMBA also utilizes [redacted] which auto encrypts all outgoing email."***

**OIG Comment:**

Although SAMBA states that it has implemented encryption controls over internal and removable data, no evidence was provided to support this statement. As part of the audit resolution process, we recommend that SAMBA provide OPM's HIO with evidence that it has fully implemented this recommendation.

### 4. Vulnerability Scanning/Remediation

SAMBA does not have a vulnerability scanning and remediation process to ensure all systems within the network do not have known weaknesses and have been updated with the latest patches and fixes.

NIST SP 800-53 Revision 4, Control RA-5, "Vulnerability Scanning," states that an organization should routinely scan for vulnerabilities in the information system and hosted applications. It also states that an organization should analyze vulnerability scan reports and results and then remediate the legitimate vulnerabilities.

Failure to identify and remediate known vulnerabilities greatly increases the organization's risk to easily exploited weaknesses. This may lead to a loss of personal health information and control of information systems and applications.

**Recommendation 18**

We recommend that SAMBA implement a routine automated vulnerability scanning process to ensure all known weaknesses within the information systems are identified in a timely manner.

***Plan's Response:***

***"SAMBA has implemented a routine automated vulnerability scanning and remediation process. We routinely scan for vulnerabilities to ensure all systems within the network do not have any known weaknesses and are updated with the latest patches and fixes. Our Network Vulnerability Scanning and Log Monitoring Policy and Procedure, provided in recommendation 11, contain details of our remediation requirements. The Policy requires, at a minimum, weekly scans. A copy of a recent scan is attached below as C4-R18."***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates SAMBA has implemented a routine vulnerability scanning process; no further action is required.

**<u>Recommendation 19</u>**

We recommend that SAMBA implement a methodology to routinely analyze the vulnerability scan reports, identify legitimate vulnerabilities and remediate them in a timely manner.

***<u>Plan's Response:</u>***
***"Our Network Vulnerability Scanning and Log Monitoring Policy and Procedure was updated to include log monitoring requirements. Logs are checked daily, using our NetOps Check List, for proper system functionality and to insure no malicious activity occurs on SAMBA systems. If activity is found that violates any SAMBA policy, or any malicious activity is found, the results are reported to SAMBA's Security Officer and the RCC to begin a remediation process."***

**<u>OIG Comment:</u>**
Recommendation 19 relates to implementing a process to do something meaningful with vulnerability scan results – it does not directly relate to monitoring security logs. A vulnerability scan is a tool to identify issues such as insecure configurations and missing patches. However, running a vulnerability scan in and of itself does not add any value. An organization must analyze the results of a vulnerability scan and take action to remediate the issues that were identified. SAMBA's response to recommendation 18 provided sufficient evidence that such a process is now in place, and therefore, no further action is required.

### 5. Vulnerabilities Identified in Scans

We worked with SAMBA employees to independently perform automated vulnerability scans on a sample of servers, databases, and user workstations. The results of our vulnerability scans indicated that several critical vulnerabilities that have known exploits exist in SAMBA's technical environment. The details of these scans will not be included in this report, but were provided directly to SAMBA.

**Security vulnerabilities were detected in SAMBA's servers, databases, and user workstations.**

NIST SP 800-53 Revision 4 states that the Plan 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.

**<u>Recommendation 20 (Flash Audit Alert Recommendation 3)</u>**

We recommend that SAMBA make the appropriate changes to its computer servers in order to address the critical weaknesses identified in the vulnerability scans.

***<u>Plan's Response:</u>***
***"All critical weaknesses identified in the vulnerability scans have been remediated. Documentation for Flash Audit Alert Recommendation 3 was provided with our Corrective Action Plan."***

**<u>OIG Comment:</u>**
The Corrective Action Plan indicates that several weaknesses had been scheduled for remediation, but the action was not yet complete. As part of the audit resolution process, we recommend that SAMBA provide OPM's HIO with evidence once all vulnerabilities identified in the scans have been remediated.

## D. <u>Configuration Management</u>

The SAMBA claims processing application, [redacted], is housed in a distributed environment, and includes many supporting applications and system interfaces. We evaluated SAMBA's management of the configuration of these information systems.

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

### 1. Baseline Configurations

SAMBA has not documented baseline configurations for all operating platforms used in its technical environment. A baseline configuration is a formally approved policy or standard outlining how to securely configure an operating platform.

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 meet performance requirements defined by the organization.

**<u>Recommendation 21</u>**

We recommend that SAMBA document approved baseline configurations for all server and database platforms used in its environment.

***Plan's Response:***

***"SAMBA now has documented baseline configurations for all operating platforms. Our Configuration Management Policy & Procedure has been updated to address our baseline configurations. If a change is requested or required, the IT Manager will form and lead a Configuration Management Team (CMT). Should any changes be made to an operating system, the CMT is responsible for assuring that any related baselines are updated. Documentation of our current baseline configurations are maintained electronically. The Configuration Management Policy & Procedure was provided in Recommendation 1 response. The Firewall baseline was provided in Recommendation 13 response. Our server and database configurations are attached below as D1-R21."***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates SAMBA has developed security baseline configurations; no further action is required.

### 2. Configuration Compliance Auditing

As noted above, SAMBA does not maintain approved operating platform configuration baselines for its servers and databases. Therefore, SAMBA cannot effectively audit the 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 that could lead to data breaches.

**Recommendation 22**

We recommend that SAMBA routinely audit all server and database security configuration settings to ensure they are in compliance with approved baselines.

***Plan's Response:***

***"SAMBA's Configuration Management Policy & Procedure was updated to indicate that SAMBA's baseline configurations are audited and reviewed quarterly. We utilize [redacted] to create and maintain our baselines. The Baseline***

***Configuration Audit List, provided above in Response 21, is utilized to document the audit.”***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates SAMBA has implemented a process to routinely audit all server and database security configuration settings to ensure they are in compliance with established baselines; no further action is required.

## E. Contingency Planning

We reviewed the following elements of SAMBA’s contingency planning program to determine whether controls were in place to prevent or minimize interruptions to business operations when disastrous events occur:

- Disaster recovery plan;
- Business continuity plan; and
- Implemented real time data replication recovery on IT systems.

SAMBA has identified and prioritized the systems and resources that are critical to business operations, and has developed high level plans to recover those systems and resources. However, the sections below document areas for improvement related to SAMBA’s configuration management controls.

### 1. Documented Business Continuity Procedures and Testing

SAMBA has established an enterprise level business continuity plan in the event of a disaster or disrupting event. However, SAMBA has not yet documented detailed procedures to supplement the business continuity plan. SAMBA also has not completed a functional test of its business continuity plan.

NIST SP 800-53 Revision 4 states that an organization needs to develop procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. NIST SP 800-53 Revision 4, Control CP-4, “Contingency Plan Testing,” states that an organization must test the contingency plan for the information system to determine the effectiveness of the plan and organization readiness to execute the plan.

Failure to develop procedures to facilitate the implementation of the contingency planning policy and without testing the plan before an actual disaster could result in a loss of information, inability to meet recovery time objectives, and meet contractual obligations.

By implementing Recommendation 2 in the Security Management section, above, SAMBA will address the issue of a lack of contingency plan procedures.

## F. Claims Adjudication

The following section details our review of the applications and business process supporting SAMBA's claims adjudication process.

### 1. Application Configuration Management

We evaluated the policies and procedures governing the application change control of SAMBA's claims processing system.

SAMBA's claims processing system, [redacted], is a commercial product. However, SAMBA is responsible for implementing and testing changes or updates from the vendor. While policies and procedures have been implemented for the change control process, the process could be improved. Currently, all four members of SAMBA's IT staff have access to move files/updates between the test and production environments.

**Recommendation 23**

We recommend that SAMBA review its application change control process and implement appropriate separation of duties for this process.

***Plan's Response:***
***"We have updated our Change Management Procedures and created a Segregation of Duties Policy to assure that no one individual is responsible for application changes. No one individual who updates files in the Test environment can update the Production environment. A "Change Request Form" will be utilized. The Change Management Group will provide oversight and approval of applications changes. The authorizer of the change cannot be the individual to deploy a change to Production. A copy of our Change Management Procedures is attached below as F1-R23."***

**OIG Comment:**
Evidence was provided in response to the draft audit report that indicates SAMBA has implemented a stronger change control process with appropriate separation of duties controls; no further action is required.

### 2. Claims Processing System

We evaluated the input, processing, and output controls associated with SAMBA's claims processing system. We have determined the following controls are in place over SAMBA's claims adjudication system:

- Validation checks are conducted on SAMBA's incoming claims;
- Claims are monitored as they are processed through the system; and
- Claims output files are fully reconciled.

Nothing came to our attention to indicate that SAMBA has not implemented adequate procedural controls over the claims adjudication process.

### 3. Enrollment

We evaluated SAMBA's procedures for managing its database of member enrollment data. Changes to member enrollment information are primarily received via an electronic transmission. Although SAMBA has an audit function to review both electronic submissions and manually entered data, our analysis of the manual review showed high error rates for users entering enrollment data.

**Recommendation 24**

We recommend that SAMBA adjust the audit policy so that all manually entered enrollment data is reviewed for errors.

***Plan's Response:***

***"SAMBA has updated its Enrollment Policy and Procedure to include an audit process for review of manually entered enrollment data. A copy of the updated Policy and Procedure and a copy of the daily log are attached below as F3-R24."***

**OIG Comment:**

Evidence was provided in response to the draft audit report that indicates SAMBA has implemented a process to review all manually entered enrollment data for errors; no further action is required

### 4. Debarment

SAMBA has adequate procedures for updating its claims system with debarred provider information. SAMBA downloads the OPM OIG debarment update list every month and that data is loaded into its claims processing system. On a quarterly basis, SAMBA downloads the entire debarment list and loads that into its claims processing system. Any debarred providers that appear in SAMBA's provider database are flagged to prevent claims submitted by that provider from being processed successfully during the claims adjudication process.

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

### 5. Application Controls Testing

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

Our test results indicated that SAMBA's system has controls and system edits in place to identify the following scenarios:

- Duplicate and near duplicate claims;
- Timely filing;
- Gender / procedure inconsistencies;
- Dependent benefits structure;
- Enrollment inconsistencies;
- Invalid date of service;
- Chiropractic benefit structure;
- Lab bundling inconsistencies; and
- Overlapping Hospital stays.

The section below documents an opportunity for improvement related to SAMBA's claims application controls.

#### a. Medical Editing

Our claims testing exercise identified several scenarios where SAMBA's claims system 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:

- Age / Procedure – a procedure code for [redacted];
- Diagnosis / Procedure – a procedure code for [redacted];
- Place of Service / Procedure – a procedure code for [redacted];
- Provider / Procedure – a procedure code for [redacted]; and
- Facility / Procedure – a procedure code for [redacted].

These system weaknesses increase the risk that benefits are being paid for procedures that were not actually performed.

**<u>Recommendation 25</u>**

We recommend that SAMBA make the appropriate system modifications to prevent medically inconsistent claims from being processed.

***Plan's Response:***

***"SAMBA has modified its claim editing products to prevent medically inconsistent claims from being processed."***

**OIG Comment:**

Although SAMBA indicated it has modified its claim editing products to prevent medically inconsistent claims from being processed, no evidence was provided to support this statement. As part of the audit resolution process, we recommend that SAMBA provide OPM's HIO with evidence that it has implemented these changes.

# IV. MAJOR CONTRIBUTORS TO THIS REPORT

**Information Systems Audit Group**

[redacted], Auditor-In-Charge

[redacted], Lead IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

---

[redacted], Group Chief

# Appendix

11301 Old Georgetown Road
Rockville, Maryland 20852-2800

SAMBA
FEDERAL EMPLOYEE BENEFIT ASSOCIATION

(301) 984-1440 • (800) 638-6589
www.SambaPlans.com

July 31, 2015

**Sent Via Email**:

[redacted]
Lead IT Auditor-In-Charge
Information Systems Audit Group
United States Office of Personnel Management
Office of the Inspector General

Dear [redacted]:

Enclosed please find SAMBA's responses to the recommendations made in the draft report issued by the Office of the Inspector General, Office of Personnel Management, entitled, "Audit of Information Systems General and Application Controls at Special Agents Mutual Benefit Association" (Report Number 1B-44-00-14-065), dated June 2, 2015.

SAMBA has either fully implemented or is in the process of implementing each of the recommendations made in the draft report. Our responses to each recommendation are set forth in the enclosure. Where appropriate, supporting documentation is embedded with the response and labeled to correspond with the recommendation.

If you have any questions about our responses, please contact me at [redacted].

Sincerely,

Walter E. Wilson

Walter E. Wilson
Executive Director

Enclosure: (1)

cc: [redacted], Contract Officer, Health Insurance Group II
[redacted], Contract Specialist, Health Insurance Group II

SAMBA
FEDERAL EMPLOYEE BENEFIT ASSOCIATION

# Responses to the Recommendations in the Draft Audit Report

**Recommendation 1 (Flash Audit Alert Recommendation 1)**

We recommend that SAMBA develop comprehensive IT security policies and procedures.
At a minimum, SAMBA should implement policies and procedure related to the following topics:

- IT Security Management-**(CAP)**
- IT Security Training Requirements-**(CAP)**
- Auditing/Monitoring User and Administrator Activity
- Log Monitoring-**(CAP)**
- Appropriate Use of Software
- Segregation of Duties
- Auditing of User Access-**(CAP)**
- Vulnerability Remediation-**(CAP)**
- Server Configuration Management, Baseline Configurations, and Auditing Server Configuration
- Firewall Management-**(CAP)**

***SAMBA Response:***
**SAMBA has developed and adopted comprehensive IT security policies and procedures for the above. These are attached below as A1-R1. Those indicated as "CAP" were previously provided to OPM OIG in our Corrective Action Plan progress monitoring submission.**

**Recommendation 2 (Flash Audit Alert Recommendation 2)**

We recommend that SAMBA develop detailed procedures to compliment the following existing policies, and ensure that they include the level of detail necessary to meet the Plan's long term goals and to establish a secure IT environment:

- Access Control
- Business Continuity Plan/Testing
- Disaster Recovery Plan/Testing
- Security Incident Response

***SAMBA Response:***
**SAMBA has developed detailed procedures to compliment the above existing policies. These are attached below as A1-R2.**

**Recommendation 3**

We recommend that SAMBA implement a process to routinely review and update its IT security policies.

***SAMBA Response:***
**SAMBA has a Regulatory Compliance Committee (RCC). The RCC is responsible to routinely review SAMBA's compliance programs and policies and procedures. The committee meets on as "as needed" basis and annually prior to the scheduled risk assessment. The RCC Charter is formally documented in the attached below as A1-R3.**

**Recommendation 4**

We recommend SAMBA implement a routine enterprise risk assessment policy and procedure.

***SAMBA Response:***
**SAMBA has developed and implemented a Risk Management Policy. The Policy requires that a Risk Assessment be performed annually or upon significant change to an information system. The next Risk Assessment is scheduled for October, 2015. The Risk Management Policy is attached below as A2-R4.**

## Recommendation 5

We recommend that SAMBA reevaluate the elements included in its background check process. At a minimum it should implement a criminal record check and ensure hired individuals are not on the OPM debarment list.

***SAMBA Response:***

**SAMBA has reevaluated and updated its *Background Check Policy & Procedures.* The policy and procedures now require criminal background checks for all newly hired employees. SAMBA has verified that no current employees are on the OPM debarment list. The *Background Check Policy & Procedures* is attached below as A3-R5.**

## Recommendation 6

We recommend that SAMBA document the IT security training requirements for employees with significant security responsibilities.

***SAMBA Response:***

**SAMBA has modified its *IT Security Training for All SAMBA Employees Policy and Procedures* to include specific requirements for IT security-related job responsibilities. Documentation of completed specialized IT training and certifications will be maintained electronically. The *IT Security Training for All SAMBA Employees Policy and Procedures* is attached as A4-R6.**

## Recommendation 7

We recommend that SAMBA reassess its facilities' physical access management and implement controls that will ensure proper physical security to include at a minimum [redacted] and [redacted] [redacted].

***SAMBA Response:***

**SAMBA has installed [redacted] at the [redacted] We have contracted to install [redacted] at the same locations to be completed by September 1, 2015.**

## Recommendation 8

We recommend that SAMBA reassess its data centers' physical access management and implement controls that will ensure proper physical security to include at a minimum [redacted] and [redacted] [redacted].

***SAMBA Response:***

**SAMBA has installed [redacted] to our data center [redacted]. We have contracted to install an anti-piggy backing detection system to be completed by September 1, 2015.**

## Recommendation 9

We recommend that SAMBA implement a formal access request form for both physical and logical access as a part of granting, modifying or removing access and maintain it on file.

***SAMBA Response:***

**SAMBA has designed and implemented the use of a formal access request form for both physical and logical access.**

**(1) Physical Access Request Form is utilized to grant, modify or remove access to our facility.**

**(2) Logical Access Request Form is utilized to grant, modify or remove access to our claim processing system, email, voice mail, imaging system, personnel database, virtual private network, and accounting management system.**

**The completed forms require management approval, will indicate the minimum required access needed, and be maintained electronically for auditing purposes. We have updated our *Access Control Policy and Procedures* and *Physical Security Policy* to indicate use of these forms. The forms are attached below as B2-R9.**

### Recommendation 10

We recommend that SAMBA implement a process to routinely audit physical access to its facility. This audit should include verification that no active badge accounts exist for terminated employees, and that the level of access to existing employees remains appropriate.

***SAMBA Response:***

**SAMBA has implemented a process to routinely audit physical access to our facility. Our *Physical Security Policy* requires audits to be conducted at least quarterly. A "Badge Access List" is reviewed by the Security Officer and Human Resources Manager to verify employees are actively employed and access levels are appropriate for each individual. Results of the review process will be documented and maintained electronically. The *Physical Security Polic*y is attached below as B4-R10**

### Recommendation 11

We recommend that SAMBA implement a process to log and monitor user access (logon and logoff activity) for both general and privileged users.

***SAMBA Response:***

**SAMBA has implemented a process to log and monitor user access for both general and privileged users. Our *Network Vulnerability Scanning and Log Monitoring Policy* require the use of a NetOps Check List. The NetOps Check List is used to document the Logs and indicate who reviewed them. The [redacted] application is used to monitor logon and logoff activity of both general and privileged users. The logs are reviewed by Network Operations Staff with oversight by the Security Officer. A copy of our *Network Vulnerability Scanning and Log Monitoring Policy* is attached below as A5-R11.**

### Recommendation 12

We recommend that SAMBA implement a process to log and monitor all transaction activity of privileged users including, but not limited to, domain and database administrators.

***SAMBA Response:***

**SAMBA has implemented a process to log and monitor all transaction activity of all users, including privileged users. Our *Network Vulnerability Scanning and Log Monitoring Policy and Procedures* specify that logs are checked daily for activity and proper system functionality. The [redacted] application is used to monitor internet activity of all users including the activity of privileged users. The [redacted] batch report is utilized to monitor activity on the claim system database. [redacted] is utilized to monitor privileged users on the domain. The Network Operations Staff, with oversight by the Security Officer, is task with reviewing the daily logs. The Human Resource Manager reviews the Security Officer's access and activity with the assistance of the System Administrator. The claim system database batch reports are monitored by our Claims Department Manager or designee.**

### Recommendation 13

We recommend that SAMBA document a formal firewall management policy and configuration baseline.

***SAMBA Response:***

**SAMBA has a formal *Firewall Management Policy & Procedure* and a documented firewall configuration baseline. The policy includes specific guidelines to manage, update, and define the rule sets of SAMBA firewalls. Our *Firewall Management Policy & Procedure* was provided in our response to Recommendation 1. Our configuration baseline is attached below as C1-R13**

**Recommendation 14**

We recommend that SAMBA implement a process to conduct routine configuration reviews on its network firewalls to ensure performance and security optimization, as defined by the firewall management policy.

***SAMBA Response:***
**We have updated our Firewall Management Procedure to indicate that Firewall Rule sets and Configurations require quarterly review. The updated *Firewall Management Policy & Procedure* as well as documentation of a recent review is attached below as C1-R14.**

**Recommendation 15**

We recommend SAMBA document the types of network activity that should be logged within its information systems and then implement modify its information systems to collect these logs.

***SAMBA Response:***
**SAMBA has implemented the [redacted] system. [redacted] provides SAMBA a process to log security related network events and the type of network activity within our information systems.**

**Recommendation 16**

We recommend SAMBA implement an intrusion detect/prevention system.

***SAMBA Response:***
**SAMBA has implemented an intrusion detect/prevention system imbedded within our Firewall.**

**Recommendation 17**

We recommend that SAMBA implement encryption controls on both internal and removable information system media.

***SAMBA Response:***
**Media controls have been implemented to control unauthorized access to digital media removed from the information system and within. All optical drives have been disabled from SAMBA workstations. In additions, SAMBA implemented [redacted] application that will encrypt all hard drives and any thumb drive that are utilized. All hard drives have been encrypted. SAMBA also utilizes [redacted] which auto encrypts all outgoing email.**

**Recommendation 18**

We recommend that SAMBA implement a routine automated vulnerability scanning process to ensure all known weaknesses within the information systems are identified in a timely manner.

***SAMBA Response:***
**SAMBA has implemented a routine automated vulnerability scanning and remediation process. We routinely scan for vulnerabilities to ensure all systems within the network do not have any known weaknesses and are updated with the latest patches and fixes. Our *Network Vulnerability Scanning and Log Monitoring Policy and Procedure,* provided in recommendation 11, contain details of our remediation requirements. The Policy requires, at a minimum, weekly scans. A copy of a recent scan is attached below as C4-R18.**

**Recommendation 19**

We recommend that SAMBA implement a methodology to routinely analyze the vulnerability scan reports, identify legitimate vulnerabilities and remediate them in a timely manner.

***SAMBA Response:***
**Our *Network Vulnerability Scanning and Log Monitoring Policy and Procedure* was updated to include log monitoring requirements. Logs are checked daily, using our NetOps Check List, for proper system functionality**

**and to insure no malicious activity occurs on SAMBA systems. If activity is found that violates any SAMBA policy, or any malicious activity is found, the results are reported to SAMBA's Security Officer and the RCC to begin a remediation process.**

**Recommendation 20 (Flash Audit Alert Recommendation 3)**

We recommend that SAMBA make the appropriate changes to its computer servers in order to address the critical weaknesses identified in the vulnerability scans.

***SAMBA Response:***

**All critical weaknesses identified in the vulnerability scans have been remediated. Documentation for Flash Audit Alert Recommendation 3 was provided with our Corrective Action Plan.**

**Recommendation 21**

We recommend that SAMBA document approved baseline configurations for all server and database platforms used in its environment.

***SAMBA Response:***

**SAMBA now has documented baseline configurations for all operating platforms. Our *Configuration Management Policy & Procedure* has been updated to address our baseline configurations. If a change is requested or required, the IT Manager will form and lead a Configuration Management Team (CMT). Should any changes be made to an operating system, the CMT is responsible for assuring that any related baselines are updated. Documentation of our current baseline configurations are maintained electronically. The *Configuration Management Policy & Procedure* was provided in Recommendation 1 response. The Firewall baseline was provided in Recommendation 13 response. Our server and database configurations are attached below as D1-R21.**

**Recommendation 22**

We recommend that SAMBA routinely audit all server and database security configuration settings to ensure they are in compliance with approved baselines.

***SAMBA Response:***

**SAMBA's *Configuration Management Policy & Procedure* was updated to indicate that SAMBA's baseline configurations are audited and reviewed quarterly. We utilize [redacted] to create and maintain our baselines. The Baseline Configuration Audit List, provided above in Response 21, is utilized to document the audit.**

**Recommendation 23**

We recommend that SAMBA review its application change control process and implement appropriate separation of duties for this process.

***SAMBA Response:***

**We have updated our C*hange Management Procedures* and created a *Segregation of Duties Policy* to assure that no one individual is responsible for application changes. No one individual who updates files in the Test environment can update the Production environment. A "Change Request Form" will be utilized. The Change Management Group will provide oversight and approval of applications changes. The authorizer of the change cannot be the individual to deploy a change to Production. A copy of our *Change Management Procedures* is attached below as F1-R23.**

**Recommendation 24**

We recommend that SAMBA adjust the audit policy so that all manually entered enrollment data is reviewed for errors.

***SAMBA Response:***

**SAMBA has updated its *Enrollment Policy and Procedure* to include an audit process for review of manually entered enrollment data. A copy of the updated Policy and Procedure and a copy of the daily log are attached below as F3-R24.**

**Recommendation 25**

We recommend that SAMBA make the appropriate system modifications to prevent medically inconsistent claims from being processed.

***SAMBA Response:***

**SAMBA has modified its claim editing products to prevent medically inconsistent claims from being processed.**

# 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