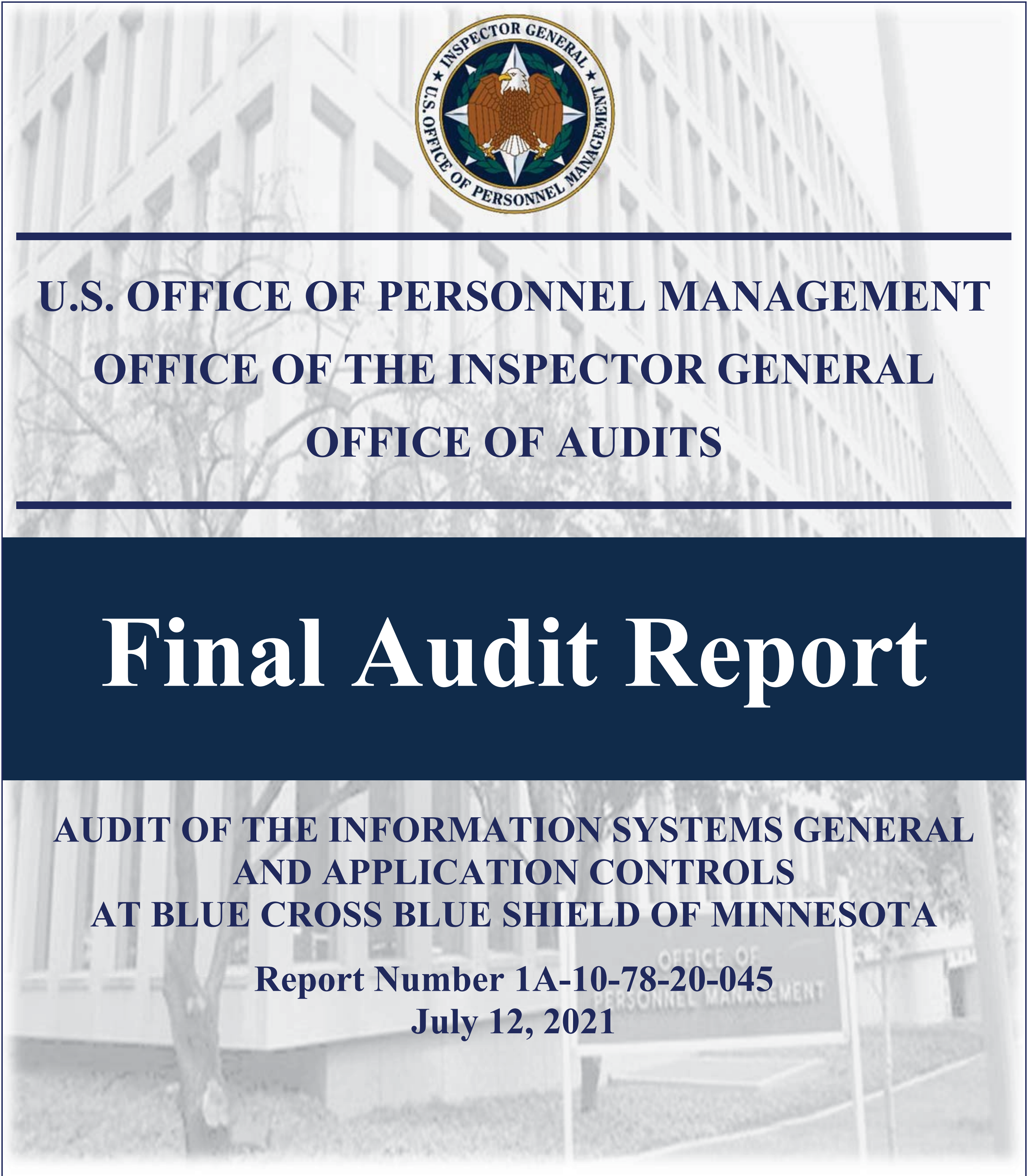

U.S. OFFICE OF PERSONNEL MANAGEMENT

OFFICE OF THE INSPECTOR GENERAL

OFFICE OF AUDITS

Final Audit Report

AUDIT OF THE INFORMATION SYSTEMS GENERAL AND APPLICATION CONTROLS AT BLUE CROSS BLUE SHIELD OF MINNESOTA

Report Number 1A-10-78-20-045
July 12, 2021

EXECUTIVE SUMMARY

Audit of the Information Systems General and Application Controls at Blue Cross Blue Shield of Minnesota

Report No. 1A-10-78-20-045 **July 12, 2021**

Why Did We Conduct the Audit?

Blue Cross Blue Shield of Minnesota (BCBSMN) contracts with the U.S. Office of Personnel Management as part of the Federal Employees Health Benefits Program (FEHBP).

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

What Did We Audit?

The scope of this audit centered on the information systems used by BCBSMN 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?

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

- BCBSMN has adequate controls over security management.
- BCBSMN has implemented controls for granting and removing physical access to facilities. However, [redacted]
- BCBSMN has controls in place related to network security, such as encryption to protect sensitive data and data loss prevention.
- BCBSMN has a documented change management process. However, [redacted]
- BCBSMN has a documented business continuity plan. However, [redacted]
- BCBSMN conducted a disaster recovery plan test [redacted]
- BCBSMN has adequate controls over its claims adjudication process.

ABBREVIATIONS

BCBSMN	Blue Cross Blue Shield of Minnesota
CFR	Code of Federal Regulations
FEHBP	Federal Employees Health Benefits Program
FISCAM	Federal Information System Controls Audit Manual
GAO	U.S. Government Accountability Office
IT	Information Technology
NIST SP	National Institute of Standards and Technology Special Publication
OIG	Office of the Inspector General
OPM	U.S. Office of Personnel Management

TABLE OF CONTENTS

I. BACKGROUND

This final 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 Blue Cross Blue Shield of Minnesota (BCBSMN).

The audit was conducted pursuant to FEHBP contract CS 1039; 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 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 or comprehensive medical services.

This was our first audit of the information technology (IT) general and application controls at BCBSMN. All BCBSMN 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 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 BCBSMN's IT environment. We accomplished these objectives by reviewing the following areas:

- Security management;
- Access controls;
- Network security;
- Configuration management;
- Contingency planning; and
- Application controls specific to BCBSMN'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 BCBSMN'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 BCBSMN'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 BCBSMN to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in St. Paul, Minnesota.

Due to social distancing guidance related to COVID-19, all audit work was completed at our office in Washington, D.C. The remote work performed included teleconference interviews of staff, documentation reviews, and remote testing of the general and application controls in place over BCBSMN's information systems. The findings, recommendations, and conclusions outlined in this report are based on the status of information system general controls in place at BCBSMN as of October 2020.

In conducting our audit, we relied to varying degrees on computer-generated data provided by BCBSMN. 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:

- Performed a risk assessment of BCBSMN'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);

- Gathered documentation and conducted interviews;

- Reviewed BCBSMN's business structure and environment; 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 BCBSMN's control structure. These criteria included, but were not limited to, the following publications:

- GAO's FISCAM;

- National Institute of Standards and Technology Special Publication (NIST SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; and

- NIST SP 800-41, Revision 1, Guidelines on Firewalls and Firewall Policy.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether BCBSMN's practices were consistent with applicable standards. While generally compliant with respect to the items tested, BCBSMN 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 an examination of the policies and procedures that are the foundation of BCBSMN's overall IT security program. We evaluated BCBSMN's ability to develop security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls.

BCBSMN has adequate controls over security management.

BCBSMN has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. BCBSMN has also implemented human resources policies and procedures related to hiring, training, transferring, and terminating employees.

Nothing came to our attention to indicate that BCBSMN has not implemented adequate controls related to security management.

B. ACCESS CONTROLS

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

We examined the physical access controls at BCBSMN's facilities and data center. We also examined the logical access controls protecting sensitive data in BCBSMN's network environment and claims processing 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 and removing logical access to applications and software resources; and

- Routine access reviews for logical and physical access.

However, we noted the following opportunities for improvement related to physical access to BCBSMN's data center.

1. Data Center Physical Access Controls

The primary data center is located [redacted] Access to the entrance of the office building requires a valid access card and is monitored by a security guard. [redacted]

- [redacted]
- [redacted]

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

[redacted]

Recommendation 1

We recommend that BCBSMN [redacted]

BCBSMN's Response:

"BCBSMN disagrees with the recommendation and feels that it has adequate controls in place [redacted]

OIG Comments:

In response to the draft audit report, BCBSMN provided evidence that it has implemented [redacted]; no further action is required.

Recommendation 2

We recommend that BCBSMN [redacted]

BCBSMN's Response:

"BCBSMN agrees with the recommendation. [redacted]

OIG Comments:

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

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.

BCBSMN has adequate data loss prevention controls

We evaluated BCBSMN's controls related to network design, data protection, and systems monitoring. We also reviewed the results of several automated vulnerability scans performed during this audit.

We observed the following controls in place:

- Perimeter controls to secure connections to external networks;
- Encryption to protect sensitive data at rest; and
- Data loss prevention controls.

BCBSMN conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in its network environment on our behalf. The specific vulnerabilities that we identified were provided to BCBSMN in the form of an audit inquiry, but will not be detailed in this report.

BCBSMN responded to our audit inquiry and provided evidence that [redacted]. Therefore, we did not identify any opportunities for improvement related to BCBSMN's network security controls.

D. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. BCBSMN employs a team of technical personnel who manage system software configuration for the organization. We evaluated BCBSMN's management of the configuration of its computer servers and databases.

Our review found the following controls in place:

- Documented system change control process; and
- An established system build and hardening process.

However, we noted the following opportunity for improvement related to BCBSMN's configuration management program.

1. Configuration Management Policies and Procedures

We requested all of BCBSMN's policies and procedures related to configuration management. We received a high level lifecycle flow diagram and change management procedures. However, [redacted]

NIST SP 800-53, Revision 4, states that the organization develops, documents and disseminates to organization-defined personnel: "A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance; and … [p]rocedures to facilitate the implementation of the configuration management policy and associated configuration management controls … ."

[redacted]

Recommendation 3

We recommend that BCBSMN [redacted]

BCBSMN's Response:

"BCBSMN agrees with the recommendation. BCBSMN will [redacted]

E. CONTINGENCY PLANNING

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

- Data center environmental controls to minimize disruptions;
- Business continuity plan (e.g., people and business processes); and
- Disaster recovery plan (e.g., recovery of hardware and software infrastructure).

However, we noted the following opportunity for improvement related to BCBSMN's contingency planning.

1. Disaster Recovery Plan

BCBSMN provided us with its disaster recovery plan. However, [redacted]

[redacted]

NIST SP 800-53, Revision 4, states that "The organization … [u]pdates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing … ."

[redacted]

Recommendation 4

We recommend that BCBSMN [redacted]

BCBSMN's Response:

"BCBSMN agrees with the recommendation. BCBSMN [redacted]

OIG Comments:

In response to the draft audit report, BCBSMN provided evidence that [redacted] further action is required.

2. Disaster Recovery Plan Testing

BCBSMN's Business Resilience Policy states, "The Business Resilience Office shall ensure that recovery plans are exercised. The type of exercise, scope and frequency shall be determined by the Business Resilience Office." We were told that disaster recovery plans are tested annually at a minimum. We were provided with a disaster recovery plan test that was conducted from October 29 to November 1, [redacted]

NIST SP 800-53, Revision 4, states that the organization should test the contingency plan "to determine the effectiveness of the plan and the organizational readiness to execute the plan." Furthermore, NIST SP 800-53, Revision 4, states that "The organization tests the contingency plan at the alternate processing site:

(a) To familiarize contingency personnel with the facility and available resources; and

(b) To evaluate the capabilities of the alternate processing site to support contingency operations."

[redacted]

Recommendation 5

We recommend that BCBSMN [redacted]

BCBSMN's Response:

"BCBSMN agrees with the recommendation. BCBSMN [redacted]

F. CLAIMS ADJUDICATION

The following sections detail our review of the applications and business processes supporting BCBSMN's claims adjudication process. BCBSMN adjudicates claims using a third-party vendor's claims processing application called OSCAR. The third-party vendor is also part of the FEHBP. OSCAR was developed and is maintained in-house by the third-party vendor. Additionally, claims are processed by the Blue Cross Blue Shield Association's nationwide Federal Employee Program Direct system. We reviewed the following processes related to claims adjudication: application change control, claims processing, and provider debarment and suspension.

1. Application Change Control

We evaluated the policies and procedures governing application development and change control over BCBSMN's claims processing system.

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

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

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

2. Claims Processing System

We evaluated the business process controls associated with BCBSMN's claims processing system that ensure the completeness, accuracy, and confidentiality of transactions and data. We determined that BCBSMN has implemented policies and procedures to help ensure that:

BCBSMN has sufficient input, processing, and output controls over claims processing.

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

Nothing came to our attention to indicate that BCBSMN has not implemented adequate controls over the claims processing system.

3. Debarment and Suspension

BCBSMN has documented procedures for reviewing provider files for debarments and suspensions. The OPM OIG debarment list is downloaded monthly and compared against claims records. Positive matches are identified and flagged within the claims processing systems. In accordance with OPM OIG debarment guidelines, affected members are notified of the debarment and extended a 15-day grace period to select a new provider. All subsequent claims from the debarred provider are denied.

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

APPENDIX

BlueCross BlueShield
Association

An Association of Independent
Blue Cross and Blue Shield Plans

Federal Employee Program
1310 G Street, N.W.
Washington, D.C. 20005
202.942.1000
Fax 202.942.1125

March 22, 2021

Julius Rios, Auditor-In-Charge
Information Systems Audits Group
U.S. Office of Personnel Management (OPM)
1900 E Street, NW
Room 6400
Washington, D.C. 20415-1100

Reference: OPM DRAFT IT AUDIT REPORT

Blue Cross Blue Shield of Minnesota (BCBSMN)
Audit Report Number 1A-10-78-20-045
(Dated January 22, 2021)

The following represents the Plan's response as it relates to the recommendations included in the draft report.

A. SECURITY MANAGEMENT

No recommendation noted.

B. ACCESS CONTROLS

Data Center Physical Access Controls

Recommendation 1

We recommend that BCBSMN [redacted]

Plan Response

BCBSMN disagrees with the recommendation and feels that it has adequate controls in place to prevent [redacted]

Recommendation 2

We recommend that BCBSMN [redacted]

Plan Response

BCBSMN agrees with the recommendation. BCBSMN will [redacted]

C. NETWORK SECURITY

No recommendation noted.

D. CONFIGURATION MANAGEMENT

Configuration Management Policies and Procedures

Recommendation 3

We recommend that BCBSMN [redacted]

Plan Response

BCBSMN agrees with the recommendation. BCBSMN will [redacted]

E. CONTINGENCY PLANNING

1. Disaster Recovery Plan

Recommendation 4

We recommend that BCBSMN [redacted]

Plan Response

BCBSMN agrees with the recommendation. BCBSMN [redacted]

2. **Disaster Recovery Plan Testing**

Recommendation 5

We recommend that BCBSMN [redacted]

Plan Response

BCBSMN agrees with the recommendation. BCBSMN [redacted]

F. **Claims Adjudication**

No recommendation noted.

We appreciate the opportunity to provide our response to each of the recommendations in this report and request that our comments be included in their entirety and are made a part of the Final Audit Report. If you have any questions, please contact me at [redacted] or [redacted] at [redacted]

Sincerely,

[redacted]

Managing Director, FEP Program Assurance

cc: Eric Keehan, OPM
[redacted] FEP
[redacted] FEP

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