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

# Final Audit Report

## AUDIT OF THE INFORMATION SYSTEMS GENERAL CONTROLS AT PRESBYTERIAN HEALTH PLAN

Report Number 1C-P2-00-19-016
November 18, 2019

# EXECUTIVE SUMMARY

*Audit of the Information Systems General Controls at Presbyterian Health Plan*

**Report No. 1C-P2-00-19-016** **November 18, 2019**

**Why Did We Conduct The Audit?**

Presbyterian Health Plan (Presbyterian) 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 Presbyterian's information technology (IT) environment.

**What Did We Audit?**

The scope of this audit centered on the information systems used by Presbyterian 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 Presbyterian's IT security controls determined that:

- Presbyterian has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.
- Presbyterian has implemented internal network segmentation to isolate information systems that store and process sensitive data.
- Perimeter firewalls are not routinely reviewed for compliance with approved standards.
- Individuals approved for local administrative privileges on endpoint devices are not monitored for compliance with software policies.
- Presbyterian has adequate policies and procedures to detect and respond to IT security threats.
- System configuration is controlled according to documented policies, procedures, and standards.
- Presbyterian has documented security configuration standards for its servers. However, Presbyterian could improve its enforcement and auditing of those standards.

# ABBREVIATIONS

| | |
|---|---|
| **CFR** | **Code of Federal Regulations** |
| **COBIT** | **Control Objectives for Information and Related Technologies** |
| **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's Special Publication** |
| **OIG** | **Office of the Inspector General** |
| **OMB** | **U.S. Office of Management and Budget** |
| **OPM** | **U.S. Office of Personnel Management** |
| **PHP** | **Presbyterian Health Plan** |
| **PHS** | **Presbyterian Healthcare Services** |
| **Presbyterian** | **Presbyterian Health Plan** |
| **SecCM** | **Security-Focused Configuration Management** |
| **T-Systems** | **T-Systems North America Inc.** |

# TABLE OF CONTENTS

# I. BACKGROUND

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

The audit was conducted pursuant to FEHBP contract CS 2627; 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, indemnity benefits, or comprehensive medical services.

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

- Security management;
- Network security;
- Incident response; and
- Configuration management.

## 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 Presbyterian'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 Presbyterian'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 Presbyterian to process medical insurance claims and/or store the data of FEHBP members. The business processes reviewed are primarily located in Albuquerque, New Mexico.

The onsite portion of this audit was performed in April of 2019. 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 controls in place at Presbyterian as of April 2019.

In conducting our audit, we relied to varying degrees on computer-generated data provided by Presbyterian. 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 Presbyterian's business structure and environment;
- Performed a risk assessment of Presbyterian'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 Presbyterian'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;
- OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- Control Objectives for Information and Related Technologies (COBIT) 5: A Business Framework for the Governance and Management of Enterprise IT;
- GAO's FISCAM;
- National Institute of Standards and Technology's Special Publication (NIST SP) 800-12, Revision 1, An Introduction to Information Security;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-40, Revision 3, Guide to Enterprise Patch Management Technologies;
- 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;

- NIST SP 800-61, Revision 2, Computer Security Incident Handling Guide; and

- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems.

## COMPLIANCE WITH LAWS AND REGULATIONS

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

**The Plan has developed an adequate risk management methodology.**

Presbyterian has implemented a series of formal policies and procedures that govern its security management program. The Plan has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. Presbyterian has also implemented an adequate vendor management program to assess and monitor risks associated with third-party activities.

Nothing came to our attention to indicate that Presbyterian does not have an adequate security management program.

## B. NETWORK SECURITY

Network security includes the policies and controls used to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Presbyterian contracts with a vendor, T-Systems North America Inc. (T-Systems), who manages the technical infrastructure housing for the Plan's claims adjudication systems; we therefore evaluated controls managed by both Presbyterian and T-Systems related to network design, data protection, and endpoint device controls. We also reviewed the results of several automated vulnerability scans that we performed during this audit.

We observed the following controls in place:

- Perimeter controls protecting public and partner network connections;
- Network access controls to prevent unauthorized devices on the internal network; and
- Internal network segmentation to control access to sensitive systems and data.

The following sections document opportunities for improvement related to Presbyterian's network security controls.

## 1. Firewall Configuration Review

T-Systems manages the firewall devices that control access to network segments housing Presbyterian's claims adjudication system and maintains a high level baseline configuration. Presbyterian's policies and procedures state that firewall rules must be reviewed semi-annually. However, it appears that regular audits of firewall rulesets are not being conducted.

**Perimeter firewalls are not routinely reviewed for compliance with approved standards.**

NIST SP 800-41, Revision 1, states that rulesets should be reviewed or tested periodically to make sure that firewall rules are in compliance with the organization's policies. Failure to routinely audit firewall settings increases the risk that unauthorized changes to the firewall's configuration remain undetected.

### Recommendation 1

We recommend that Presbyterian ensure that T-Systems performs routine audits of its current firewall configurations against an approved firewall policy.

### *Presbyterian Response:*

***"T-Systems manages the PHS [Presbyterian Healthcare Services] firewalls at the direction of PHS and is managed through the Change Management process. In response to previous recommendations, we have implemented a process for T-Systems to deliver the firewall rules to PHS on a predefined schedule, providing us with the ability to review configurations against our approved firewall policies.*** [redacted]***."***

### OIG Comments:

As part of the audit resolution process, we recommend that Presbyterian 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 Presbyterian agrees to implement.

## 2. Administrator Device Monitoring

Presbyterian authorizes local administrative privileges for some employees on their assigned workstations. [redacted]

[redacted] Presbyterian has recognized this control gap and stated that a process will be established to audit user systems with local administrator rights on a regular basis. Furthermore, Presbyterian is in the process of acquiring a tool with the ability to audit installed software in the near future.

NIST SP 800-53, Revision 4, advises that "The organization … Establishes … policies governing the installation of software by users … . Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both."

NIST SP 800-40, Revision 3, states that "Enterprise patch management is dependent on having a current and complete inventory of the patchable software (applications and operating systems) installed on each host … ." Failure to monitor local administrator devices increases the risk of employees installing unauthorized and unmanaged software.

**Recommendation 2**

We recommend that Presbyterian implement a process to ensure locally administered systems are monitored for compliance with software and patch management policies.

***Presbyterian Response:***

***"PHP [Presbyterian Health Plan] agrees with the recommendation. Periodic reviews of Local Admin privileges will be performed to ensure only those with legitimate business need have access. Further, with the upcoming implementation of [redacted] we will have increased capability to detect [redacted]. This [redacted]. Finally, PHP will invest in the ability to appropriately restrict [redacted]."***

## 3. OIG Vulnerability Scan

As noted above, the Presbyterian claims adjudication system is housed in a vendor managed data center by T-Systems. T-Systems performs credentialed vulnerability scans of systems at the data center and provides the results to Presbyterian. Presbyterian uploads the results into a tool and uses a risk based approach to rank vulnerabilities. Presbyterian remediates the top [redacted] vulnerabilities based on risk, pervasiveness, and exploitability across its whole environment. However, we conducted credentialed vulnerability and configuration compliance scans on a sample of servers in Presbyterian's network environment and found vulnerabilities that the Plan acknowledged are in need of remediation. The specific

vulnerabilities that we identified were provided to Presbyterian in the form of an audit inquiry, but will not be detailed in this report.

NIST SP 800-53, Revision 4, states that organizations must remediate legitimate vulnerabilities identified in information systems and hosted applications. Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

**Recommendation 3**

We recommend that Presbyterian remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during fieldwork.

***Presbyterian Response:***

***"There were [redacted] vulnerabilities with a risk score of [redacted] … have been remediated since this scan. Of the [redacted] A plan to remediate the remainder of these vulnerabilities will be developed and all items will be [redacted]."***

## C. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

**Presbyterian has adequate policies and procedures to detect and respond to IT security threats.**

Security event monitoring involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the investigation and reporting of such activity. Incident response consists of an incident response plan identifying roles and responsibilities, response procedures, training, and reporting. We evaluated Presbyterian's processes related to monitoring and responding to security and privacy events.

Our review found the following controls in place:

- Security event monitoring throughout the network;
- Policies and procedures for analyzing security events; and
- A documented incident response program.

Nothing came to our attention to indicate that Presbyterian does not have adequate security event monitoring and incident response management programs.

## D. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. We evaluated Presbyterian's policies and procedures that govern its configuration management program. We also reviewed the results of configuration compliance scans to validate the effectiveness of the security management program.

Our review found the following controls in place:

- Documented and approved configuration standards including an exception process for deviations;
- Documented system change control process; and
- Established patch management process.

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

### 1. Security Configuration Enforcement

**Presbyterian could improve the enforcement of its configuration standards.**

T-Systems is responsible for managing the installation of server system software. Once a server is deployed, Presbyterian IT personnel implement and manage security configurations through domain policies. Those settings are documented in Presbyterian's security configuration specifications and standards. Security configuration standards are formally approved documents that list the specific security settings for each operating system that an organization uses to configure its servers.

As part of our configuration compliance testing, we compared the current security configurations of a sample of servers to Presbyterian's documented standards. Our test results show that Presbyterian does not effectively enforce approved security configuration standards on all of its servers.

NIST SP 800-128 states that "The practice of SecCM [security-focused configuration management] for ensuring adequate security and facilitating the management of risk is most effectively realized if it is implemented in a consistent manner across the organization." Furthermore, NIST SP 800-128 provides insight into the potential effects of inadequate configuration enforcement, stating that "If an information system is inconsistent with approved configurations … the organization may be unaware of potential vulnerabilities and not take actions that would otherwise limit those vulnerabilities and protect it from attacks."

**Recommendation 4**

We recommend that Presbyterian develop procedures to enforce system configurations on all information systems in its network environment.

***Presbyterian Response:***

***"T-Systems utilizes automated tools to check for T-Systems standard compliance deviations and communicates with PHS regularly through various methods regarding deviations. PHS will develop a plan that will allow us to use standardized security configurations and leverage T-Systems automated tools for enforcement within the scope of the FEHB contract [redacted]"***

## 2. Security Configuration Auditing

Presbyterian has a process in place with T-Systems to conduct routine configuration compliance scans on its server system software. However, as previously noted, our scan results showed that those servers are not in compliance with the approved standards. Therefore, [redacted]

FISCAM states that "A process and related procedures needs to be established to document the results from monitoring configuration items and ensure that discrepancies are properly corrected." Failure to thoroughly analyze and remediate deviations from security standards could leave servers exposed to known weaknesses.

**Recommendation 5**

We recommend that Presbyterian develop policies and procedures to routinely review the results of security configuration audits to ensure that systems remain in compliance with approved standards.

***Presbyterian Response:***

***"PHP will improve policies and procedures to routinely review the security configurations to ensure that systems remain in compliance with approved standards [redacted]."***

# APPENDIX

**Presbyterian Health Plan Rebuttal Response**

**Audit of the Information Systems General Controls at Presbyterian Health Plan**

**Report Number 1C-P2-00-19-016**

**August 20, 2019**

## A. SECURITY MANAGEMENT

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

Presbyterian has implemented a series of formal policies and procedures that govern its security management program. The Plan has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments. Presbyterian has also implemented an adequate vendor management program to assess and monitor risks associated with third-party activities.

Nothing came to our attention to indicate that Presbyterian does not have an adequate security management program.

## B. NETWORK SECURITY

Network security includes the policies and controls used to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Presbyterian contracts with a vendor, T-Systems North America Inc. (T-Systems), who manages the technical infrastructure housing the Plan's claims adjudication systems; we therefore evaluated controls managed by both Presbyterian and T-Systems related to network design, data protection, and endpoint device controls. We also reviewed the results of several automated vulnerability scans that we performed during this audit.

We observed the following controls in place:

- Perimeter controls protecting public and partner network connections;

- Network access controls to prevent unauthorized devices on the internal network; and
- Internal network segmentation to control access to sensitive systems and data.

The following sections document opportunities for improvement related to Presbyterian's network security controls.

## 1. Firewall Configuration Review

T-Systems manages the firewall devices that control access to network segments housing Presbyterian's claims adjudication system and maintains a high-level baseline configuration. Presbyterian's policies and procedures state that firewall rules must be reviewed semi- annually. However, it appears that regular audits of firewall rulesets are not being conducted.

NIST SP 800-53, Revision 4, states that rulesets should be reviewed or tested periodically to make sure that firewall rules are in compliance with the organization's policies. Failure to routinely audit firewall settings increases the risk that unauthorized changes to the firewall's configuration remain undetected.

### Recommendation 1

We recommend that Presbyterian ensure that T-Systems performs routine audits of its current firewall configurations against an approved firewall policy.

PHP Response: T-Systems manages the PHS firewalls at the direction of PHS and is managed through the Change Management process. In response to previous recommendations, we have implemented a process for T-Systems to deliver the firewall rules to PHS on a predefined schedule, providing us with the ability to review configurations against our approved firewall policies. [redacted]

## 2. Administrator Device Monitoring

Presbyterian authorizes local administrative privileges for some employees on their assigned workstations. Currently, the Plan does not have a process in place to monitor [redacted] Presbyterian has recognized this control gap and stated that a process will be established to audit user systems with local administrator rights on a regular basis. Furthermore, Presbyterian is in the process of acquiring a tool with the ability to audit installed software in the near future.

NIST SP 800-53, Revision 4, advises that "The organization establishes policies governing the installation of software by users. Policy enforcement methods include procedural methods (e.g., periodic examination of user accounts), automated methods (e.g., configuration settings implemented on organizational information systems), or both."

NIST SP 800-40, Revision 3, states that "Enterprise patch management is dependent on having a current and complete inventory of the patchable software (applications and operating systems) installed on each host." Failure to monitor local administrator devices increases the risk of employees installing unauthorized and unmanaged software.

**Recommendation 2**

We recommend that Presbyterian implement a process to ensure locally administered systems are monitored for compliance with software and patch management policies.

PHP Response: PHP agrees with the recommendation. Periodic reviews of Local Admin privileges will be performed to ensure only those with legitimate business need have access. Further, with the upcoming implementation of [redacted] we will have increased capability to detect [redacted]. This will be in place [redacted]. Finally, PHP will invest in the ability to appropriately restrict [redacted].

## 3. OIG Vulnerability Scan

As noted above, the Presbyterian claims adjudication system is housed in a vendor managed data center by T-Systems. T-Systems performs credentialed vulnerability scans of systems at the data center and provides the results to Presbyterian. Presbyterian uploads the results into a tool and uses a risk-based approach to rank vulnerabilities. Presbyterian remediates the top [redacted] vulnerabilities based on risk, pervasiveness, and exploitability across its whole environment. However, we conducted credentialed vulnerability and configuration compliance scans on a sample of servers in Presbyterian's network environment and found vulnerabilities that the Plan acknowledged are in need of remediation. The specific vulnerabilities that we identified were provided to Presbyterian in the form of an audit inquiry but will not be detailed in this report.

NIST SP 800-53, Revision 4, states that organizations must remediate legitimate vulnerabilities identified in information systems and hosted applications. Failure to remediate vulnerabilities increases the risk that hackers could exploit system weaknesses for malicious purposes.

**Recommendation 3**

We recommend that Presbyterian remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided during fieldwork.

PHP Response: There were [redacted] vulnerabilities with a risk score of [redacted] which have been remediated since this scan. [redacted] A plan to remediate the remainder of these vulnerabilities will be developed and all items will be [redacted]

## C. SECURITY EVENT MONITORING AND INCIDENT RESPONSE

Security event monitoring involves the collection, review, and analysis of auditable events for indications of inappropriate or unusual activity, and the investigation and reporting of such activity. Incident response consists of an incident response plan identifying roles and responsibilities, response procedures, training, and reporting. We evaluated Presbyterian's processes related to monitoring and responding to security and privacy events.

Our review found the following controls in place:

- Security event monitoring throughout the network;
- Policies and procedures for analyzing security events; and
- A documented incident response program.

Nothing came to our attention to indicate that Presbyterian does not have adequate security event monitoring and incident response management programs.

## D. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. We evaluated Presbyterian's policies and procedures that govern its configuration management program. We also reviewed the results of configuration compliance scans to validate the effectiveness of the security management program.

Our review found the following controls in place:

- Documented and approved configuration standards including an exception process for deviations;
- Documented system change control process; and
- Established patch management process.

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

## 1. Security Configuration Enforcement

T-Systems is responsible for managing the installation of server system software. Once a server is deployed, Presbyterian IT personnel implement and manage security configurations through domain policies. Those settings are documented in Presbyterian's security configuration specifications and standards. Security configuration standards are formally approved documents that list the specific security settings for each operating system that an organization uses to configure its servers.

As part of our configuration compliance testing, we compared the current security configurations of a sample of servers to Presbyterian's documented standards. Our test results show that Presbyterian does not effectively enforce approved security configuration standards on all of its servers.

NIST SP 800-128, states that "The practice of SecCM [security-focused configuration management] for ensuring adequate security and facilitating the management of risk is most effectively realized if it is implemented in a consistent manner across the organization." Furthermore, NIST SP 800-128 provides insight into the potential effects of inadequate configuration enforcement stating "If an information system is inconsistent with approved configurations … the organization may be unaware of potential vulnerabilities and not take actions that would otherwise limit those vulnerabilities and protect it from attacks."

### Recommendation 4

We recommend that Presbyterian develop procedures to enforce system configurations on all information systems in its network environment.

PHP Response: T-Systems utilizes automated tools to check for T-Systems standard compliance deviations and communicates with PHS regularly through various methods regarding deviations. PHS will develop a plan that will allow us to use standardized security configurations and leverage T-Systems automated tools for enforcement within the scope of the FEHB contract [redacted]

## 2. Security Configuration Auditing

Presbyterian has a process in place with T-Systems to conduct routine configuration compliance scans on its server system software. However, as previously noted, our scan results showed that those servers are not in compliance with the approved standards. Therefore, [redacted]

FISCAM states that "A process and related procedures needs to be established to document the results from monitoring configuration items and ensure that discrepancies are properly corrected." Failure to thoroughly analyze and remediate deviations from security standards could leave servers exposed to known weaknesses.

## Recommendation 5

We recommend that Presbyterian develop policies and procedures to routinely review the results of security configuration audits to ensure that systems remain in compliance with approved standards.

PHP Response: PHP will improve policies and procedures to routinely review the security configurations to ensure that systems remain in compliance with approved standards by the end of Q4 2019.

Presbyterian Health Plan is in receipt of this draft Information Technology Audit and have provided comment.

Brandon Fryar, President, Presbyterian Health Plan — Date: 8.20.19

# 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