Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

HIGH-RISK SECURITY VULNERABILITIES IDENTIFIED DURING REVIEWS OF INFORMATION TECHNOLOGY GENERAL CONTROLS AT STATE MEDICAID AGENCIES

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Daniel R. Levinson
Inspector General

March 2014
A-07-14-00433

Office of Inspector General

https://oig.hhs.gov/

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC

at https://oig.hhs.gov

Section 8L of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

EXECUTIVE SUMMARY

High-risk security vulnerabilities we identified during reviews of information system general controls at 10 State Medicaid agencies raise concerns about the integrity of the systems used to process Medicaid claims.

WHY WE DID THIS REVIEW

High-risk security vulnerabilities we identified during previous, restricted reviews of information system general controls at 10 State Medicaid agencies (State agencies) raise concerns about the integrity of the systems used to process Medicaid claims. The integrity of the State agencies' Medicaid systems depends on the effectiveness of the information system general controls, which are critical to the reliability, confidentiality, and availability of Medicaid data. Without effective general controls, State agencies are not able to adequately safeguard sensitive Medicaid systems and data.

The Office of Inspector General's (OIG) review of information system general controls at 10 State agencies conducted from 2010 through 2012 identified pervasive high-risk vulnerabilities. In responding to OIG's work and in agreeing with the vast majority of OIG's recommendations, the State agencies acknowledged the vulnerabilities and committed to addressing them. This report aggregates the data from our series of audits while omitting details that could compromise the security of any specific State agency system we audited. By doing so, the summary information presented in this report may increase public awareness of these pervasive vulnerabilities across State agencies and lead the Centers for Medicare & Medicaid Services (CMS) and all States to strengthen system security. OIG has identified the security of health information systems as a top challenge facing the Department and State agencies.

The objective of this review was to summarize the high-risk security vulnerabilities that we noted as audit findings in our previous, restricted reviews of information system general controls as those vulnerabilities related to the Medicaid Management Information Systems (MMIS) at 10 State agencies between calendar years 2010 and 2012.

BACKGROUND

We have been conducting reviews of the information system general controls at State agencies to assess the integrity of State Medicaid systems for the last 12 years. We conducted these reviews using selected procedures from the Government Accountability Office's *Federal Information Systems Controls Audit Manual*, which provides guidance in evaluating general controls over computer-processed data from information systems. Our audit reports on these reviews made recommendations to the State agencies regarding the vulnerabilities that we had identified; in almost all cases, the State agencies agreed with our recommendations and described corrective actions that they had taken or planned to take. We restricted the distribution of these reports to the State agencies and the CMS action officials because of the sensitivity of the vulnerabilities in the audit findings—vulnerabilities that could have left State agencies' automated data processing systems susceptible to exploitation or attack.

Information system general controls are the structure, policies, and procedures that apply to an entity's overall computer operations, ensure proper operations of information systems, and create a secure environment for application systems. Some primary objectives of general controls are to safeguard data, protect computer applications, prevent unauthorized access to system software, and ensure continued computer operations after unexpected interruptions. General controls are applied at the entitywide level, the system level, and the business process application level.

WHAT WE FOUND

We identified a total of 79 findings in the 10 State Medicaid agencies whose information system general controls we audited between calendar years 2010 and 2012. We grouped these 79 individual findings into 15 security control areas within 3 information system general control categories: entitywide controls, access controls, and network operations controls. In the area of entitywide controls, we identified significant and pervasive findings involving the need to develop or strengthen formal, comprehensive plans for system security, contingency planning, and configuration management, among other findings. Findings in the area of access controls included frequently-noted vulnerabilities related to logical access and user account management, login identification and authentication, and remote access. In the area of network operations controls, we identified significant and pervasive findings regarding the need for formalized policies and procedures for network device management and patch management, among other findings.

In some of the general control areas, we noted findings with similar vulnerabilities in different State agencies, which indicated that the vulnerabilities identified in these findings were systemic and pervasive. However, because we did not test all of the same information system general controls at each State agency and because we did not use a methodology that would permit us to extrapolate our findings to all State agencies, we cannot conclude that all Medicaid information system security environments have similar vulnerabilities.

Officials from several State agencies described some common causes when we discussed these findings with them. They pointed most frequently to resource constraints that made information system security a lower priority. Officials also described a lack of formal policies and procedures when explaining the causes of the vulnerabilities. The effectiveness of these information system general controls directly affects the State agencies' ability to sustain secure Medicaid systems.

WHAT WE CONCLUDE

This review aggregates findings from the individual reports that show serious vulnerabilities in the 10 States' MMIS. The State agencies advised us, in their comments on the individual restricted reports on information system general controls, that they were addressing the vulnerabilities that we had identified. The fact that some of the vulnerabilities were shared among the 10 State agencies suggests that other State Medicaid information systems may be similarly vulnerable. Medicaid agencies' management should make information system security a higher priority. We are continuing to conduct work in this area. This report is intended to provide information to assist those State agencies and CMS in strengthening system security.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

High-risk security vulnerabilities we identified during previous, restricted reviews of information system general controls at 10 State Medicaid agencies (State agencies) raise concerns about the integrity of the systems used to process Medicaid claims. The integrity of the State agencies' Medicaid systems depends on the effectiveness of the information system general controls, which are critical to the reliability, confidentiality, and availability of Medicaid data. Without effective general controls, State agencies are not able to adequately safeguard sensitive Medicaid systems and data.

The Office of Inspector General's (OIG) review of information system general controls at 10 State agencies conducted from 2010 through 2012 identified pervasive high-risk vulnerabilities. In responding to OIG's work and in agreeing with the vast majority of OIG's recommendations, the State agencies acknowledged the vulnerabilities and committed to addressing them. This report aggregates the data from our series of audits while omitting details that could compromise the security of any specific State agency system we audited. By doing so, the summary information presented in this report may increase public awareness of these pervasive vulnerabilities across State agencies and lead the Centers for Medicare & Medicaid Services (CMS) and all States to strengthen system security. OIG has identified the security of health information systems as a top challenge facing the Department and State agencies.

OBJECTIVE

Our objective was to summarize the high-risk security vulnerabilities that we noted as audit findings in our previous, restricted reviews of information system general controls as those vulnerabilities related to the Medicaid Management Information Systems (MMIS) at 10 State agencies between calendar years (CYs) 2010 and 2012.

BACKGROUND

Medicaid Program

The U.S. Department of Health and Human Services (HHS) oversees States' use of Federal entitlement benefits for the Medicaid program. Federal regulations require State agencies to establish the appropriate automated data processing (ADP) security requirements on the basis of recognized industry standards and standards governing security of Federal ADP systems and information processing (45 CFR § 95).

We have been conducting reviews of the information system general controls at State agencies to assess the integrity of State Medicaid systems for the last 12 years. We conducted these reviews using selected procedures from the Government Accountability Office's *Federal Information Systems Controls Audit Manual*, which provides guidance in evaluating general controls over computer-processed data from information systems. Our audit reports on these reviews made recommendations to the State agencies regarding the vulnerabilities that we had identified; in almost all cases, the State agencies agreed with our recommendations and described corrective actions that they had taken or planned to take. We restricted the distribution of these reports to the State agencies and the CMS action officials because of the sensitivity of the vulnerabilities in the audit findings—vulnerabilities that could have left State agencies' ADP systems susceptible to exploitation or attack.

Information System General Controls

Information system general controls are the structure, policies, and procedures that apply to an entity's overall computer operations, ensure proper operations of information systems, and create a secure environment for application systems. Some primary objectives of general controls are to safeguard data, protect computer applications, prevent unauthorized access to system software, and ensure continued computer operations after unexpected interruptions. General controls are applied at the entitywide level, system level, and business process application level.

The effectiveness of general controls is a significant factor in determining the effectiveness of business process application level controls. Without effective general controls at the entitywide and system levels, business process application level controls generally can be rendered ineffective by circumvention or modification. General controls affect the integrity of the program and are critical to ensuring the confidentiality, integrity, and availability of data.

HOW WE CONDUCTED THIS REVIEW

We grouped the high- and moderate-impact audit findings from our previous, restricted reviews of information system general controls at 10 State agencies into 3 core categories of general controls: entitywide controls, access controls, and network operations security controls. Taken together, these groups of high- and moderate-impact audit findings identify high-risk vulnerabilities in the State agencies' MMIS. All of the vulnerabilities presented in this report were noted in the previous reviews that we performed in CYs 2010, 2011, and 2012.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A contains details of our audit scope and methodology, and Appendix B contains a detailed listing of the criteria used in the audits presented in this report.

FINDINGS

We identified a total of 79 findings in the 10 State Medicaid agencies whose information system general controls we audited between CYs 2010 and 2012. We grouped these 79 individual findings into 15 security control areas within 3 information system general control categories: entitywide controls, access controls, and network operations controls. In the area of entitywide controls, we identified significant and pervasive findings involving the need to develop or strengthen formal, comprehensive plans for system security, contingency planning, and configuration management, among other findings. Findings in the area of access controls included frequently-noted vulnerabilities related to logical access and user account management, login identification and authentication, and remote access. In the area of network operations controls, we identified significant and pervasive findings regarding the need for formalized policies and procedures for network device management and patch management, among other findings.

In some of the general control areas, we noted findings with similar vulnerabilities in different State agencies, which indicated that the vulnerabilities identified in these findings were systemic and pervasive. However, because we did not test all of the same information system general controls at each State agency and because we did not use a methodology that would permit us to extrapolate our findings to all State agencies, we cannot conclude that all Medicaid information system security environments have similar vulnerabilities.

Officials from several State agencies described some common causes when we discussed these findings with them. They pointed most frequently to resource constraints that made information system security a lower priority. Officials also described a lack of formal policies and procedures when explaining the causes of the vulnerabilities. The effectiveness of these information system general controls directly affects the State agencies' ability to sustain secure Medicaid systems.

The table on the following page summarizes our findings and totals them by general control area and State agency.

Table: High- and Moderate-Impact Findings Totaled by General Control Area and State Medicaid Agency

	State Medicaid Agency										
General Control Areas	**State A**	**State B**	**State C**	**State D**	**State E**	**State F**	**State G**	**State H**	**State I**	**State J**	**Total Numbers of Findings**
Entitywide Controls											
System security plan		1	1			1	3		1	1	8
Encryption	1	1	1		1	1		1	1	1	8
Contingency planning			1	1	2				1		5
Configuration management		1		1	2				1		5
Inventory tracking	1				1	1					3
Risk assessments			1				1		1		3
Security configuration baselines				1	1						2
Access Controls											
Logical access rights		1		1	1		2		2	1	8
Identification and authentication		1			2	1	1		1		6
Remote access	1		1	1	1	1		1			6
Physical security	1	1	1		1		1				5
Network Operations Controls											
Network device management		1		2	2	1		1	1	1	9
Patch management	1	1		1	1	1			1		6
Antivirus deployment		1		1	1						3
Logging and monitoring				1	1						2
Total Findings	**5**	**9**	**6**	**10**	**17**	**7**	**8**	**3**	**10**	**4**	**79**

ENTITYWIDE CONTROLS

An entitywide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The entitywide information security management program should establish a framework and continuous cycle of assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without effective entitywide general controls, business process application level controls may be rendered ineffective by circumvention or modification. We identified 34 entitywide control findings at the 10 State agencies and grouped these findings into 7 security control areas.

System Security Plan—Eight Findings Identified

System security plans should be formalized at the system and application levels for networks, facilities, and systems or groups of systems, as appropriate. These plans and related policies should cover all major systems and facilities and should outline the duties of those who are responsible for overseeing security and those who own, use, or rely on the State agency's ADP resources.

We identified eight findings in six States related to system security plans. For example, one State agency had not developed a formal, comprehensive system security plan that addressed the general support system and major application elements of the MMIS. Without a formal, comprehensive system security plan, State agencies could experience long-term consequences, including risks to data security, fraud, and monetary loss.

Encryption—Eight Findings Identified

Encryption is used to protect the confidentiality of stored data and data that are being transmitted to and from the secured network via the Internet. Additionally, encryption is extremely important in protecting wireless access to the secured network and on portable storage devices. Establishing encryption where necessary is a basic step for protecting sensitive data.

We identified eight findings in as many States related to encryption vulnerabilities. For example, 1 State agency had not encrypted the hard drives of 14 portable laptop computers, leaving them susceptible to unauthorized access.

Contingency Planning—Five Findings Identified

Contingency plans should be formalized to ensure the availability of critical information systems and the continuity of operations in emergencies. These plans should contain detailed roles, responsibilities, recovery team designations, and procedures associated with the restoration of an information system following a disruption.

We identified five findings in four States related to contingency planning vulnerabilities. For example, in one State agency, management had not established policies and procedures requiring disaster recovery testing and had not tested its disaster recovery plan to recover and reestablish business functions related to its claims processing.

Configuration Management—Five Findings Identified

Configuration management policies, plans, and procedures should be developed, documented, and implemented at the entitywide, system, and application levels to ensure an effective configuration management process. The procedures should cover employee roles and responsibilities, change control and system documentation requirements, establishment of a decisionmaking structure, and configuration management training. Configuration management should be a key part of an entity's Systems Development Life Cycle methodology.[1]

We identified five findings in four States regarding configuration management vulnerabilities. For example, one State agency's network administrator was able to implement system changes as needed without formal management approval or documented procedures for implementation and testing, a practice that could have resulted in a compromise to data confidentiality, integrity, or availability of the system.

Inventory Tracking—Three Findings Identified

State agencies must maintain complete, accurate, and up-to-date inventories of their ADP systems to implement effective security programs and minimize vulnerabilities in those systems. Without an inventory process, an agency cannot effectively manage information security controls across the agency. The inventory is necessary for effective monitoring, testing, and evaluation of information technology controls and for supporting information technology planning, budgeting, acquisition, and management.

We identified three findings in as many States related to inventory tracking vulnerabilities. For example, one State agency had not established any type of formal agencywide inventory mechanism to account for all information system components and devices and was unable to identify all workstations and servers that were authorized to access the secure network and so needed to be properly secured.

Risk Assessments—Three Findings Identified

Risk assessments should consider threats and vulnerabilities at the entitywide level, system level, and application levels. When State agencies perform risk assessments, they should consider (1) risks to data confidentiality, integrity, and availability and (2) the range of risks to their systems and data, including those posed by authorized users and unauthorized outsiders who may try to break into the systems.

We identified three findings in as many States related to risk assessment vulnerabilities. For example, one State agency had not, since implementing its MMIS, performed a risk assessment of the MMIS to identify potential threats and vulnerabilities. By not performing a risk

[1] A Systems Development Life Cycle refers to the policies and procedures that govern software development and modification as a software product goes through each phase of its life cycle.

assessment, the State agency created the possibility that it would not have identified sensitive information or implemented required actions to reduce risks.

Security Configuration Baselines—Two Findings Identified

Each State agency should maintain current configuration information for all systems in a formal configuration baseline that contains the configuration information formally designated at a specific time during a system's life. Past configuration baselines with approved changes from those baselines constitute the current configuration information. There should be a current and comprehensive baseline inventory of hardware, software, and firmware, and it should be routinely validated for accuracy.

We identified two findings in as many States related to security configuration baseline vulnerabilities. For example, one State agency had not established any documented baseline security configurations to dictate the minimum security configuration settings for all deployed workstations, servers, and network devices. That practice allowed system support staff to build and implement new servers and workstations without any oversight or review.

ACCESS CONTROLS

Access controls include physical controls, such as keeping computers in locked rooms to limit physical access, and logical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files. Access controls should be formally developed, documented, disseminated, and periodically updated to provide reasonable assurance that information security resources are protected against unauthorized modification, disclosure, loss, or impairment. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data. It is fundamental that control techniques for both physical and logical access controls be risk based. We identified 25 access control findings at the 10 State agencies that we audited and grouped these findings into 4 security control areas.

Logical Access Rights—Eight Findings Identified

Each State agency's process for managing user accounts should include the identification of the various account types (i.e., individual, group, system), the establishment of conditions for group membership, and the assignment of associated authorizations. Additionally, resource owners should periodically identify authorized users and specify access rights that are granted on the basis of a valid need to know as determined by appropriate officials and should consider the proper segregation of duties. Furthermore, State agencies should notify account managers when users have their employment terminated or are transferred and ensure that associated accounts are removed, disabled, or otherwise secured.

We identified eight findings in six States related to logical access rights. For example, one State agency had not established any formal policies regarding user account management and had not performed periodic reviews of network accounts to ensure that access was appropriately authorized and that accounts were properly configured. Without periodically reviewing user accounts and user access, State agencies run the risk of allowing personnel to gain inappropriate access to sensitive Medicaid data and systems, access that could lead to improper activities.

Identification and Authentication—Six Findings Identified

State agencies should require that users and devices be appropriately identified and authenticated. User authentication establishes the validity of a user's claimed identity, typically at the login to a system or application. Users can be authenticated by using mechanisms such as smart cards; by providing a piece of information that users alone know (e.g., a password or personal identification number); or through a unique means of physical identification such as a biometric fingerprint or retina scan. User identifications and authentications should be designed to restrict access of legitimate users to the specific systems, programs, and files that they need and to prevent others, such as hackers, from entering the system.

We identified six findings in five States related to identification and authentication vulnerabilities. For example, one State agency had not enabled the network user account lockout function after unsuccessful login attempts, an error that could have allowed intruders to successfully run automated login attack tools without detection.

Remote Access—Six Findings Identified

The use of remote access to connect users with the State agencies' secure networks via the Internet places Medicaid systems at a higher risk of compromise than those systems that are restricted to the use of internal network users only. As a result of this increased risk, accepted standards require State agencies to allow remote access only when two-factor authentication (in which one of the factors is provided by a device separate from the computer gaining access) is used and only when the remote access technology conforms to approved encryption standards.

We identified six findings in as many States related to remote access vulnerabilities. For example, one State agency was using an insecure remote access method, which sent unencrypted data (including passwords) across the Internet, to perform system administration functions within its MMIS.

Physical Security—Five Findings Identified

The effectiveness of physical security controls depends on the State agencies' ability to implement effective practices for reviewing access authorizations, controlling entry devices, restricting entry during and after normal business hours, and controlling the entry and removal of resources from the facility. Access to facilities should be limited to those having a legitimate need for access. Inadequate physical access controls diminish the availability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

We identified five findings in as many States related to physical security vulnerabilities. For example, one State agency's physical access control policies and procedures did not address the review of electronic badge access rights; consequently, some terminated employees still had access to the datacenter housing the State agency's MMIS.

NETWORK OPERATIONS CONTROLS

Once a network has been established, anyone with access to any computer on the network could attempt to attack resources on that network. Network administrators configure and monitor network operating systems to ensure that the network is secure against such attacks.

Network operations controls thus consist of the policies and procedures used to maintain, manage, and secure the devices that connect to networks. Policies and procedures that keep devices up to date and configured properly and the monitoring of the network activity and its devices for security and maintenance issues are critical to the overall security and reliability of the network. We identified 20 network operations control findings at 8 of the 10 State agencies that we audited and grouped these findings into 4 security control areas.

Network Device Management—Nine Findings Identified

Network device management consists of the policies and procedures for effectively managing the security configurations on the entities' network firewalls, routers, and switches. Additionally, network device management includes the operation of network management systems, which provide administrators with the ability to control and monitor the network device configurations from a central location. Network management systems obtain status data from network devices, enable network managers to make configuration changes, and alert them of problems.

We identified nine findings in seven States related to network device management. For example, one State agency had not implemented any formal policies and procedures for managing network devices. In the absence of formal network device management policies and procedures, administrators were using shared user accounts to administer the devices and there was no formal process for implementing and tracking configuration changes to network devices.

Patch Management—Six Findings Identified

Patch management is the process of identifying, reporting, and effectively remediating information system flaws in an operating system or program. Timely patching helps organizations maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain stability in the production environment. State agencies should establish a documented, systematic, and accountable process for managing exposure to vulnerabilities through the timely deployment of patches.

We identified six findings in as many States related to patch management vulnerabilities. For example, 1 State agency had not established an automated process for patching its network devices and was attempting to manually patch and monitor more than 500 devices. Additionally, approximately 30 percent of that same State agency's Microsoft servers and workstations did not have the latest patches. Without adequate patch management, systems may be susceptible to exploits that can lead to unauthorized disclosure, modification, or nonavailability of Medicaid data because out-of-date systems are vulnerable to exploitation.

Antivirus Deployment—Three Findings Identified

Antivirus management is the automated process used to effectively identify, isolate, and eliminate malicious software. Antivirus software should be implemented and maintained on computers and critical information system entry points to detect and eradicate malicious software transported by email, removable media, or other methods. Antivirus controls are important for detection and removal of malicious computer viruses, which can infect computers or computer systems.

We identified three findings in as many States related to antivirus deployment vulnerabilities. For example, one State agency had not established formal policies and procedures to address the antivirus software deployment and update requirements. In the absence of formal antivirus deployment policies and procedures, more than 1,000 workstations and 200 servers from the State agency's network were not reporting to the antivirus software control console, which was used to track the antivirus deployment and update status. Without updated antivirus deployment, State agencies expose their networks to known vulnerabilities, which could leave sensitive systems and data susceptible to unauthorized access and exploitation.

Logging and Monitoring—Two Findings Identified

Computer security log management is the process of generating, transmitting, analyzing, storing, and disposing of computer security log data. Computer security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; and applications. Given the number of sources and the volume of log data, an automated log management system is essential for identifying security incidents, policy violations, fraudulent activity, and operational problems.

We identified two findings in as many States related to logging and monitoring vulnerabilities. For example, one State agency had not established network logging and monitoring policies and procedures to address the types of information to be logged, the way in which those logs are to be monitored, and the types of events that should be reported to management. Additionally, that same State agency had not implemented a centralized log management system for all servers and had not deployed any automated software to actively monitor and analyze the log data that were being captured, thereby increasing the risk that inappropriate access to Medicaid data had gone undetected by management.

CONCLUSION

This review aggregates findings from the individual reports that show serious vulnerabilities in the 10 States' MMIS. The State agencies advised us, in their comments on the individual restricted reports on information system general controls, that they were addressing the vulnerabilities that we had identified. The fact that some of the vulnerabilities were shared among the 10 State agencies suggests that other State Medicaid information systems may be similarly vulnerable. Medicaid agencies' management should make information system security a higher priority. We are continuing to conduct work in this area. This report is intended to provide information to assist those State agencies and CMS in strengthening system security.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We grouped the high- and moderate-impact audit findings from our previous, restricted reviews of information security general controls at 10 State agencies into 3 core categories of general controls: entitywide controls, access controls, and network operations security controls. Taken together, these groups of high- and moderate-impact audit findings identify high-risk vulnerabilities in the State agencies' MMIS. All of the vulnerabilities presented in this report were noted in the previous reviews that we performed in CYs 2010, 2011, and 2012.

METHODOLOGY

We conducted the information security general controls audits in 10 States using selected procedures from the Government Accountability Office's *Federal Information Systems Controls Audit Manual*, which provides guidance in evaluating general controls over computer-processed data from information systems. However, the selected procedures performed at the State agencies chosen for this review varied; we did not review all of the control areas in all 10 State agencies. We conducted these audits by observing information security operations, interviewing State agency personnel, testing hardware and software configurations, and analyzing system security reports.

To determine the potential impact of each finding, we used information described in the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 199, which defines the following three levels of potential impact should there be a breach of security:

- **Low** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

- **Moderate** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

- **High** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: FEDERAL REQUIREMENTS FOR INFORMATION SYSTEM SECURITY

The principal criteria used in these reviews included:

- NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*;

- NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*;

- NIST SP 800-16, *Information Technology Security Training Requirements*;

- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*;

- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*;

- NIST SP 800-40, version 2.0, *Creating a Patch and Vulnerability Management Program*;

- NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*;

- NIST SP 800-46, *Guide to Enterprise Telework and Remote Access Security*;

- NIST SP 800-48, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*;

- NIST SP 800-53, revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*;

- NIST SP 800-61, *Computer Security Incident Handling Guide*;

- NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*;

- NIST SP 800-88, *Guidelines for Media Sanitization*;

- NIST SP 800-92, *Guide to Computer Security Log Management*;

- NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*;

- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*;

- NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*;

- NIST SP 800-123, *Guide to General Server Security*;

- NIST SP 800-124, *Guidelines on Cell Phone and PDA [Personal Digital Assistant] Security*;

- NIST FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;

- NIST FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;

- NIST FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*;

- Office of Management and Budget Circular A-130, *Management of Federal Information Resources,* Appendix III, "Security of Federal Automated Information Resources"; and

- Title 45 CFR.