United States Government Accountability Office

GAO

Report to the Chairman, Committee on Finance, U.S. Senate

August 2006

INFORMATION SECURITY

The Centers for Medicare & Medicaid Services Needs to Improve Controls over Key Communication Network

GAO-06-750

August 2006

INFORMATION SECURITY

The Centers for Medicare & Medicaid Services Needs to Improve Controls over Key Communication Network

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-750, a report to the Chairman, Committee on Finance, U.S. Senate

Why GAO Did This Study

The Centers for Medicare & Medicaid Services (CMS), a component within the Department of Health and Human Services (HHS), is responsible for overseeing the Medicare and Medicaid programs—the nation's largest health insurance programs—which benefit about one in every four Americans.

CMS relies on a contractor-owned and operated network to facilitate communication and data transmission among CMS business related entities (see figure). Effective information security controls are essential to protecting the confidentiality, integrity, and availability of this sensitive information.

At your request, GAO assessed the effectiveness of information security controls over the communication network used by CMS by conducting a technical assessment of the information security controls that are currently in place.

What GAO Recommends

GAO recommends that the CMS Administrator direct the Chief Information Officer to take steps to ensure that information security policies and standards are fully implemented.

In commenting on a draft of the report, the CMS Administrator stated that CMS has moved aggressively to implement corrective actions for the reported weaknesses.

www.gao.gov/cgi-bin/getrpt?GAO-06-750.

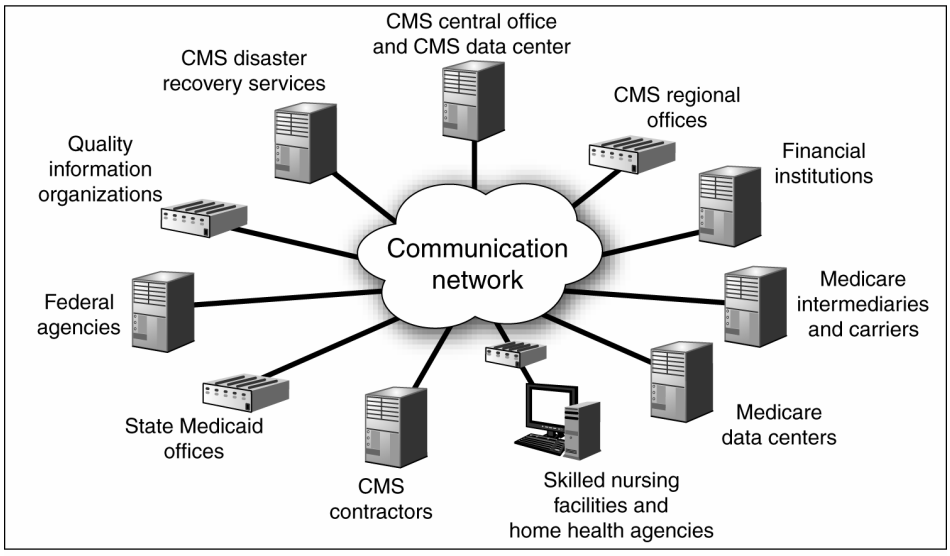
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Although CMS had many key information security controls in place—which had been designed to safeguard the communication network—some were missing, and existing ones had not always been effectively implemented. Significant weaknesses in electronic access and other system controls threatened the confidentiality and availability of sensitive CMS financial and medical information when it was transmitted across the network. CMS did not always ensure that its contractor effectively implemented electronic access controls designed to prevent, limit, and detect unauthorized access to sensitive computing resources and devices used to support the communication network.

GAO discovered numerous vulnerabilities in several areas: user identification and authentication, user authorization, system boundary protection, cryptography, and auditing and monitoring of security-related events. There were also weaknesses in controls that had been designed to ensure that secure configurations would be implemented on network devices and that incompatible duties would be sufficiently segregated. A key reason for these weaknesses is that CMS did not always ensure that its security policies and standards were implemented effectively. As a result, sensitive, personally identifiable medical data traversing the network is vulnerable to unauthorized disclosure and these weaknesses could lead to disruptions in CMS services.

Communication Network Interconnections



Source: CMS.

Contents

Abbreviations

CMS	Centers for Medicare & Medicaid Services
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
HHS	Department of Health and Human Services

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

August 30, 2006

The Honorable Charles E. Grassley
Chairman
Committee on Finance
United States Senate

The Centers for Medicare & Medicaid Services (CMS), a component within the Department of Health and Human Services (HHS), is responsible for overseeing the Medicare and Medicaid programs—the nation's largest health insurance programs—which benefit about one in every four Americans.

CMS relies on a contractor-owned and operated network to facilitate communication and data transmission among CMS business-related entities. Effective information security controls are essential to protecting the confidentiality, integrity, and availability of sensitive information transmitted over the network. A security breach in this communication network could lead to interruptions in the processing of medical claims or to unauthorized access to personally identifiable medical data, seriously diminishing the public's trust in CMS's ability to protect the sensitive beneficiary data it is entrusted with.

At your request, we assessed the effectiveness of information security controls over the communication network used by CMS. This report summarizes the vulnerabilities and information control weaknesses that we identified during our review and our recommendation to help strengthen and improve the communication network. We also issued a separate report, for limited distribution, that contains sensitive information. It describes in more detail the information security weaknesses that we identified and our specific recommendations for correcting them.

Results in Brief

Information security controls over the communication network were ineffective in protecting the confidentiality and availability of information and information resources. Although CMS had many information security controls in place that had been designed to safeguard the communication network, key information security controls were missing. In addition, the controls that were in place had not always been effectively implemented. Specifically, CMS did not always ensure that its contractor effectively

implemented controls designed to prevent, limit, and detect electronic access to sensitive computing resources and to devices used to support the communication network. For example, the network had control weaknesses in areas such as user identification and authentication, user authorization, system boundary protection, cryptography, and audit and monitoring of security-related events. Taken collectively, these weaknesses place financial and personally identifiable medical information transmitted on the network at increased risk of unauthorized disclosure and could result in a disruption in service. A key reason for these weaknesses is that CMS did not always ensure that its security policies and standards were fully implemented.

We are making a recommendation to the CMS Administrator to take steps to ensure that information security policies and standards are fully implemented. In a separate report, for limited distribution, we made recommendations to address the specific weaknesses identified.

In commenting on a draft of the report, the CMS Administrator stated that CMS has moved aggressively to implement corrective actions for the reported weaknesses.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. Without proper safeguards, systems are unprotected from individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. These concerns are well founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks to come.

Computer-supported federal operations are likewise at risk. Our previous reports, and those of agency inspectors general, describe persistent information security weaknesses that place a variety of federal operations at risk of disruption, fraud, or inappropriate disclosure of sensitive data.

We have designated information security as a governmentwide high-risk area since 1997[1]—a designation that remains today.[2]

Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002 to strengthen the security of information and systems within federal agencies. FISMA requires each agency to develop, document, and implement an agencywide information security program to provide information security for the information and systems that support the operations and assets of the agency, including those operated or maintained by contractors or others on behalf of the agency, using a risk-based approach to information security management.

CMS Oversees the Medicare & Medicaid Programs

CMS, a component of HHS, is responsible for overseeing two major health programs. It administers the Medicare program—the nation's largest health insurance program—which covers more than 42 million Americans. This program was enacted to extend affordable health insurance coverage to the elderly and was later expanded to cover some people with disabilities who are under the age of 65 years. CMS also works with the states to administer the Medicaid program, enacted in 1965 as a jointly funded program, in which the federal government matches state spending according to a formula to provide medical and health-related services to low-income Americans.

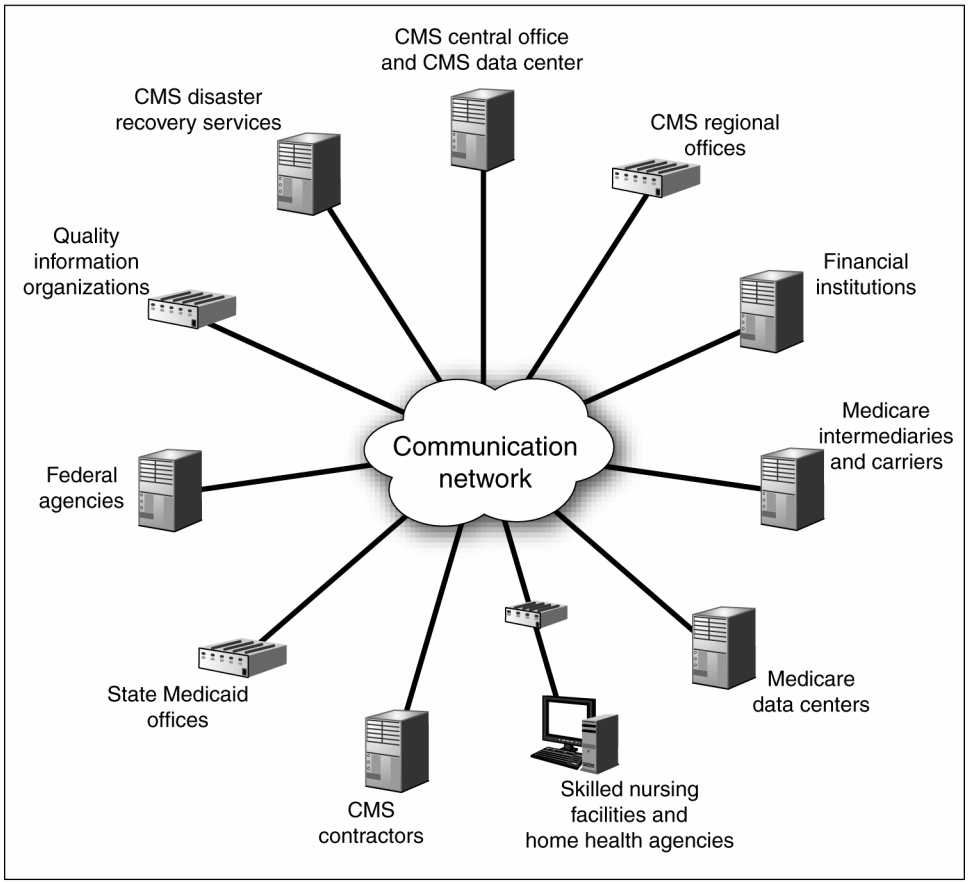
CMS relies extensively on computerized systems to support its mission-critical operations and to transmit and store the sensitive information it collects. In particular, CMS relies on a contractor-owned and operated network from which it purchases networking services to provide connectivity to its business partners. This network supports communication and data transmission between CMS business-related entities, including the CMS central office and data center, CMS regional offices, financial institutions, Medicare intermediaries and carriers, Medicare data centers, skilled nursing facilities and home health agencies,

[1]GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: Feb. 1997).

[2]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: Jan. 2005).

CMS contractors,[3] state Medicaid offices, other federal agencies, quality information organizations, and CMS disaster recovery services (see fig. 1).

Figure 1: Communication Network Interconnections



Source: CMS.

The communication network transmits Medicare claims data containing personally identifiable information such as name, sex, date of birth, social security number, and address. It also transmits medical information, such as a patient's diagnosis, prescribed drug and drug dosage, type of treatment facility—which includes substance abuse facilities or psychiatric treatment centers—requested service, and the physician's

[3]This reference to contractors does not include Medicare intermediaries, carriers, and data centers, which are sometimes also referred to as "contractors."

name and ID number. The communication network also transmits payment information, such as payment amount and billing information. The communication network does not house either Medicare or Medicaid data.

Objective, Scope, and Methodology

The objective of our review was to determine whether CMS has implemented information security controls over the communication network to effectively protect the confidentiality, integrity, and availability of its information and information resources.

To evaluate the effectiveness of the security controls over the communication network, we examined routers, network management servers, switches, firewalls, and administrator workstations, at CMS headquarters, its business partners, and at several network contractor sites. Our evaluation was based on our *Federal Information System Controls Audit Manual* (FISCAM), which provides guidance for reviewing information system controls.

Specifically, we evaluated information security controls intended to

- limit, detect, and monitor electronic access to sensitive computing resources, thereby safeguarding them from misuse and protecting them from unauthorized disclosure and modification;
- maintain operating system integrity through effective administration and control of powerful computer programs and utilities that execute privileged instructions;
- prevent the introduction of unauthorized changes to application or system software; and
- ensure that work responsibilities are segregated, so that one individual does not perform or control all key aspects of computer-related operations and thereby have the ability to conduct unauthorized actions or gain unauthorized access to assets or records.

We did not evaluate controls over servers used to store Medicare or Medicaid data.

We performed our work at three network contractor sites and at the CMS Central Office. This review was performed from January through May 2006 in accordance with generally accepted government auditing standards.

Significant Network Weaknesses Place Medical Data at Risk

Although CMS has many information security controls in place that are designed to safeguard the communication network, there were significant weaknesses in electronic access controls and other controls designed to protect the confidentiality, integrity, and availability of the sensitive, personally identifiable medical information it transmits. Our review of the communication network revealed 47 weaknesses in electronic access controls and other controls. A key reason for these weaknesses was that CMS did not always ensure the effective implementation of its security policies and standards. As a result, sensitive, personally identifiable, medical data traversing this network are vulnerable to unauthorized disclosure, and these weaknesses could lead to disruptions in CMS operations.

Electronic Access Controls Are Inadequate

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing electronic controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, and information. Inadequate electronic access controls diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service. Electronic access controls include those related to user identification and authentication, authorization, boundary protection, cryptography, and auditing and monitoring of security-related events. CMS's contractor did not consistently implement effective electronic access controls in each of these areas, as the following sections demonstrate.

User Identification and Authentication

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system must also establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. CMS policy requires the implementation of automated identification and authentication mechanisms that enable the unique identification and authentication of individual users or processes acting on behalf of CMS information system users.

CMS did not ensure that its contractor adequately identified and authenticated users responsible for managing the communication

network. For example, CMS's contractor did not enforce sufficiently complex passwords for access to certain network devices. This increases the risk that unauthorized users could gain access to CMS systems and sensitive information.

Authorization

Authorization is the process of granting or denying access rights and privileges to a protected resource, such as a network, system, application, function, or file. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic principle for securing computer resources and data. It means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users' access to only those programs and files that they need in order to do their work, organizations establish access rights and permissions. "User rights" are allowable actions that can be assigned to users or to groups of users. File and directory permissions are rules that are associated with a particular file or directory, regulating which users can access it—and the extent of that access. To avoid unintentionally giving users unnecessary access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions. CMS policy requires that each user or process be assigned only those privileges needed to perform authorized tasks.

CMS did not ensure that its contractor sufficiently restricted network access and privileges to only those users and processes requiring them to perform authorized tasks. For example, CMS's contractor did not adequately restrict access paths on certain network devices. In addition, the contractor had several sensitive world-writable files on network management servers, granting inappropriate privileges to these files. These conditions provide more opportunities for an attacker to escalate their privileges and make unauthorized changes to files.

Boundary Protection

Boundary protections demarcate logical or physical boundaries between protected information and systems and unknown users. Organizations physically allocate publicly accessible information system components to separate subnetworks with separate physical network interfaces, and they prevent public access into their internal networks—except as appropriately mediated. Unnecessary connectivity to an organization's network increases not only the number of access paths that must be managed and the complexity of the task, but the risk of unauthorized access in a shared environment. CMS policy requires that automated boundary protection mechanisms be established to monitor and control communications at the external boundary of the information system and at

key internal boundaries within the system. Additionally, CMS requires that any connections to the Internet or to other external systems be through controlled interfaces.

CMS did not ensure that its contractor adequately implemented controls used to protect its external and key internal boundaries. For example, certain network devices did not adequately restrict external communication traffic. In addition, although the communication network was considered a secure closed private network, indirect paths existed between it and the Internet. Consequently, an unauthorized individual could exploit these vulnerabilities to launch attacks against other sensitive network devices.

Cryptography

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. One primary principle of cryptography is encryption. Encryption can be used to provide basic data confidentiality and integrity for data, by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. CMS policy requires that technical controls be established and implemented to protect the confidentiality of sensitive CMS data while it is in transit. CMS also requires the encryption of highly sensitive system files.

CMS did not consistently apply encryption to protect the sensitive data traversing the communication network. In addition, its contractor did not consistently apply encryption to protect network configuration data stored on network devices. For example, medical data and sensitive network management traffic traverse the network unencrypted. This could allow an attacker to view medical information, or system data transmitted over the network, increasing the risk that malicious users could capture this information and use it to gain unauthorized access to network resources.

Audit and Monitoring

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to determine what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that the audit trails can provide. CMS policy requires the enforcement of auditing and accountability by configuring information systems to produce, store, and retain audit records of specific system, application, network, and user

activity. CMS also requires that audit records contain sufficient information to establish what events occurred, when the events occurred, the source of the events, the cause of the events, and the event outcome.

However, CMS's contractor did not provide adequate logging or user accountability on the communication network. For example, certain network devices did not have any users defined, allowing for the execution of unauthorized commands without any means of designating individual accountability for the action.

Other Control Weaknesses

In addition to electronic access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an organization's information and systems. These controls include techniques designed to ensure the implementation of secure configurations on network devices and to provide sufficient segregation of incompatible duties. Our review of the communication network revealed weaknesses in each of these areas. These weaknesses increase the risk that unauthorized individuals can gain access to network devices and inadvertently or deliberately disclose financial and medical data needed to process Medicare claims, or disrupt operations.

Configuration Management

To protect an organization's information, it is important to ensure that only authorized applications and programs are placed in operation. This process, known as configuration management, consists of instituting policies, procedures, and techniques to help ensure that all programs and program modifications are properly authorized, tested, and approved. Patch management, a component of configuration management, is an important element in mitigating the risks associated with software vulnerabilities. Up-to-date patch installation could help mitigate vulnerabilities associated with flaws in software code which could be exploited to cause significant damage—ranging from Web site defacement to the loss of control of entire systems—thereby enabling malicious individuals to read, modify, or delete sensitive information, disrupt operations, or launch attacks against other organizations' systems. CMS policy requires the maintenance of system hardware and software on all CMS information systems. Software maintenance includes the installation of all relevant patches and fixes that are required to correct security flaws in existing software and to ensure the continuity of business operations.

CMS did not ensure the application of timely and comprehensive patches and fixes to system software. For example, certain administrative workstations and network management servers reviewed were missing

critical patches addressing known vulnerabilities. In addition, certain network devices used vulnerable operating system software. Failure to keep system patches up to date could lead to denial-of-service attacks or to individuals gaining unauthorized access to network resources. A malicious user can exploit these vulnerabilities to gain unauthorized access to network resources or disrupt network operations. As a result, there is increased risk that the integrity of these network devices and administrator workstations could be compromised.

Segregation of Duties

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that no single individual can independently control all key aspects of a process or computer-related operation and thereby gain unauthorized access to assets or records. Often, segregation of duties is achieved by dividing responsibilities among two or more individuals or organizational groups. This diminishes the likelihood that errors and wrongful acts will go undetected, because the activities of one individual or group will serve as a check on the activities of the other. Inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. CMS policy requires that separation of duties be observed in order to eliminate conflicts of interest in the responsibilities and duties assigned to individuals.

CMS did not always ensure that its contractor sufficiently segregate incompatible responsibilities and duties. For example, the CMS network contractor allowed developer and test access to production network management servers, potentially allowing unauthorized and unnecessary access to sensitive network management data. Granting this type of access to individuals who do not require it to perform their specific job responsibilities, increases the risk that sensitive information or programs could be improperly modified, disclosed, or deleted. Consequently, increased risk exists that these individuals could introduce software errors into production or perform unauthorized system activities without being detected.

Security Policies Were Not Always Fully Implemented

Although CMS has developed and documented information security policies, a key reason for the communication network weaknesses was that CMS did not always ensure the effective implementation of its security policies and standards.

Establishing and implementing appropriate policies and related controls are key elements of an effective information security program. In order to ensure the implementation of effective information security controls, agencies need to develop comprehensive information security policies that fully address the inherent risks associated with today's highly distributed, interconnected, network-based computing environments. In addition, agencies need to take actions to ensure that the established policies and controls are fully implemented.

CMS has established a set of information security policies, standards, and guidelines that generally provides appropriate guidance to personnel responsible for securing its information systems and data. For example, it has developed information security policies that address topics such as access controls, configuration management, and system integrity.

However, in some instances, CMS did not ensure the effective implementation of its policies and standards. Although CMS had developed policies requiring the use of certain network devices, it did not always ensure that the network contractor followed these policies. In addition, CMS had developed configuration requirements for its operating systems and network devices; however, some of these standards were marked as "draft" and, therefore, had not been distributed to the network contractor.

Conclusions

Although CMS had many information security controls designed to safeguard the communication network, missing controls and ineffective implementation of certain controls, when considered collectively, threaten the confidentiality and availability of the sensitive, personally identifiable medical information it transmits. Further, CMS did not always effectively implement certain information security policies and standards. Until CMS ensures that all information security policies are being fully implemented, there is limited assurance that its sensitive data will be adequately protected against unauthorized disclosure and that network services will not be interrupted.

Recommendation for Executive Action

To help strengthen information security controls over the CMS communication network, we recommend that the CMS Administrator direct the Chief Information Officer to take steps to ensure that information security policies and standards are fully implemented.

Agency Comments

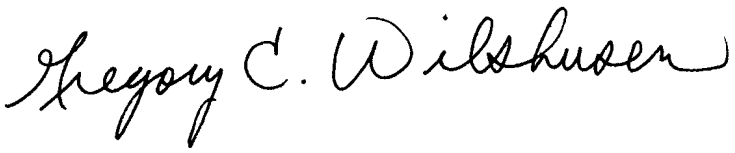
In providing written comments on a draft of the report, the CMS Administrator stated that CMS is taking steps to ensure that information security policies and standards are fully implemented. The Administrator added that CMS had conducted a review of its network security requirements, as well as an evaluation of potential updates in security services requirements provided through its network services contract. The agency is working to enhance the security requirements defined in the current task order to reflect its expectations more precisely and to provide further assurances that controls follow the most current acceptable guidelines.

In addition, the Administrator stated that CMS has moved aggressively to implement corrective actions for the reported weaknesses and that corrective action or new compensating controls had already been completed for 22 of the 47 weaknesses. An additional 19 weaknesses are scheduled for closure. The remaining six weaknesses are under review to determine what additional resources are needed and their financial impact. His written comments are reprinted in appendix I.

CMS also provided technical comments, which we incorporated where appropriate.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to congressional committees with jurisdiction over CMS, the Secretary of the Department of Health and Human Services, the CMS Administrator and Chief Information Officer, the HHS Inspector General, and other interested parties. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact Gregory C. Wilshusen at (202) 512-6244 or Keith A. Rhodes at (202) 512-6412. We can also be reached by e-mail at wilshuseng@gao.gov and rhodesk@gao.gov, respectively. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.



Gregory C. Wilshusen
Director, Information Security Issues

Keith A. Rhodes
Chief Technologist

Appendix I: Comments from the Centers for Medicare & Medicaid Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: JUL 10 2006

TO: Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office

FROM: Mark B. McClellan, M.D., Ph.D.
Administrator
Centers for Medicare & Medicaid Services

SUBJECT: Government Accountability Office (GAO) Draft Report: "INFORMATION SECURITY: The Centers for Medicare & Medicaid Services Needs to Improve Controls over Key Communication Network" *(GAO-06-750)*

Thank you for the opportunity to comment on this draft report. In this report, the Government Accountability Office (GAO) describes weaknesses it has identified in the contractor-owned and contractor-operated network used by CMS to facilitate communications and data transmission to its business partners. We have already directed our contractor to address these weaknesses, and most have already been or will be corrected. We are taking further steps to assure that none result in actual security breaches.

The Centers for Medicare & Medicaid Services (CMS) takes all aspects of data security very seriously, including the contractor-owned and contractor-operated network. As you note, no beneficiary information resides on this network. Because data does not reside on the network, intercepting or compromising information during transit across the network would be difficult. In addition, the GAO found no evidence that confidential or sensitive information had actually been compromised, and our analysis found no instances where beneficiary information had actually been exploited. Nonetheless, security of our beneficiaries' data is paramount and we appreciate GAO's assistance in identifying important opportunities for the contractor to strengthen network security.

For this reason, we were pleased to support GAO's efforts to conduct an independent audit of our contractor's security procedures. We are encouraged that GAO mentioned numerous information security controls in place at CMS that help to safeguard the communications network. These security controls are not delineated in the GAO report, but the current management, operational and technical controls for the network are set forth in the security plan, risk assessment and other network documentation that were made available to GAO during the audit engagement.

The CMS has been aware of potential weaknesses in the network security and has been proactive in addressing them. For the past several years, we have independently tested segments of the communications network. In 2005, the testing was conducted from multiple locations for the first time. The GAO report provided a useful opportunity to validate a number of findings we had already identified in our own testing, and identified other weaknesses that we are already

working to address. Based on our experience, we understand the difficulty of the task undertaken by the GAO in its review.

We are very concerned about the specific control weaknesses and specific aspects of security policy implementation by our contractor that GAO found could create increased risk of unauthorized disclosure, modification, or destruction of our information and computer resources. The deficiencies in the management controls are especially troublesome given that CMS purchases communications and data transmissions services from a shared network that is supposed to maintain the privacy of each customer's data. Our contract with the network vendor requires that the vendor embed security features in the system configuration and controls to protect all data and facilities against potential threats, attacks, or failures. This shared network configuration should address all security requirements, but especially those controls needed to mitigate the fundamental risks of the type set forth in the GAO report (e.g., password and patch management). Security is degraded when generally accepted controls to implement these very basic requirements are not effectively implemented or maintained.

With respect to the individual findings identified by the GAO, upon receipt of the preliminary GAO report we engaged working processes we have in place to mitigate vulnerabilities regardless of risk level. We immediately requested a Corrective Action Plan (CAP) for each weakness from the contractor-owner and contractor-operator of the network. In a series of in-depth meetings with the contractor, CMS reviewed each proposed corrective action to ensure that it would correct not only the immediate issue identified by the GAO, but also the root cause or environment conditions contributing to the weakness. Adjustments were made to the proposed CAPs as a result of these meetings. Concurrently, the contractor-owner and contractor-operator commenced aggressive implementation of the accepted plans.

We are pleased to report that corrective action or new compensating controls have been completed for 22 of the 47 weaknesses. As of the date of this response, the network contractor has provided evidence of implementation acceptable to CMS for 16 of the weaknesses. An additional 6 await validation of closure by CMS. Of the remaining weaknesses, 8 are scheduled for closure by September 30, 2006. An additional 11 are somewhat more complex and are scheduled for closure by January 7, 2007, to coincide with the contractor's 4th quarter update of the network. CMS is awaiting further refinement to estimate the additional resources and the financial impact of 6 of the corrective actions for possible inclusion in the CMS information technology investment review process. The network contractor has been directed to submit monthly reports to CMS on the implementation of the corrective actions until all weaknesses have been remediated.

CMS has also directed its contractor to support an independent test of the completed corrective actions following the 4th quarter update. This special test is in addition to our annual penetration testing of the network, and will be broader in scope. It will cover all weaknesses identified by GAO. The testing will be performed by the same entity responsible for our independent systems testing and evaluation of security controls as a precondition for certification and accreditation. The additional controls put in place will be further reviewed each year as part of our ongoing annual testing program to ensure they are sustained not just for the short-term but the long-run duration of our contract.

In addition to addressing each of the individual weaknesses identified by GAO, we conducted a separate internal assessment of the risk of inappropriate disclosure of financial and personally identifiable medical data traversing the network. Our risk determination included consideration of the likelihood of occurrence and severity of impact. Our determination followed guidelines promulgated by the National Institute of Standards and Technology (NIST) in their Special Publication 800-30, *Risk Management Guide for Information Technology Systems*. Using these criteria, CMS staff categorized the 47 weaknesses as follows: no high risk findings, 22 medium risk findings, and 25 low risk findings.

In arriving at these determinations, we were mindful that the contractor-owned and contractor-operated network is a shared logical network adapted for CMS. We observed that CMS data is not stored in the network, and there are no CMS data file servers or application servers located in the network. The business partners connected to the network have their own controls, such as firewalls and intrusion detection systems, to protect them from the network and other sites. These protections were beyond the scope of the GAO review, but do provide additional assurances to CMS that, in the event of a breach in the network, the local controls would provide a defense in depth for our data. The defense in depth strategy is a basic security principle and one that CMS observes in the security architecture of systems. These controls at the connected sites are tested regularly by CMS and our business partners.

Finally, in conjunction with supporting the GAO's efforts on this report, we have conducted a review of our network security requirements and an evaluation of potential updates in security services requirements provided through the General Services Administration (GSA) network services contract. The CMS is working with GSA on enhancing the security requirements as defined in the current CMS task order to reflect CMS expectations more precisely and to provide further assurances that controls follow the most current acceptable guidelines. The NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, and the CMS acceptable risk safeguards, are the basis for reviewing and amending our network security posture.

In summary, we have been proactive in our oversight of the network but are taking further steps to enhance security. We have provided information that we hope will be helpful in understanding the network, an assessment of the current risk to CMS of the inappropriate disclosure of private health information, and our plans for further reducing the risk of inappropriate disclosure. We have moved aggressively in cooperation with the contractor-operator of the network to identify and implement corrective actions for each of the weaknesses described in the report. We will continue to track and report on these actions using the Office of Management and Budget-approved Plan of Actions and Milestones process until each milestone is completed.

Attachment

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, Director, Information Security Issues, (202) 512-6244
Keith A. Rhodes, Chief Technologist, (202) 512-6412

Acknowledgments

In addition to those named above, Idris Adjerid, Mark Canter, Lon Chin, West Coile, Jeffrey Knott, Joanne Landesman, Duc Ngo, Ronald Parker, and Christopher Warweg made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548