United States Government Accountability Office

GAO

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

February 2006

INFORMATION SECURITY

Department of Health and Human Services Needs to Fully Implement Its Program

GAO-06-267

February 2006

INFORMATION SECURITY

Department of Health and Human Services Needs to Fully Implement Its Program

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-267, a report to the Chairman, Committee on Finance, U.S. Senate

Why GAO Did This Study

The Department of Health and Human Services (HHS) is the nation's largest health insurer and the largest grant-making agency in the federal government. HHS programs impact all Americans, whether through direct services, scientific advances, or information that helps them choose medical care, medicine, or even food. For example, the Centers for Medicare & Medicaid Services (CMS), a major operating division within HHS, is responsible for the Medicare and Medicaid programs that provide care to about one in every four Americans. In carrying out their responsibilities, both HHS and CMS rely extensively on networked information systems containing sensitive medical and financial information.

GAO was asked to assess the effectiveness of HHS's information security program, with emphasis on CMS, in protecting the confidentiality, integrity, and availability of its information and information systems.

What GAO Recommends

GAO recommends that the Secretary of HHS direct the Chief Information Officer to take steps to fully implement key elements of the department's information security program at all operating divisions. In commenting on a draft of this report, HHS supported GAO's emphasis on improvements to its security program, but did not believe the report sufficiently reflected progress made.

www.gao.gov/cgi-bin/getrpt?GAO-06-267.

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

What GAO Found

HHS and CMS have significant weaknesses in controls designed to protect the confidentiality, integrity, and availability of their sensitive information and information systems. HHS computer networks and systems have numerous electronic access control vulnerabilities related to network management, user accounts and passwords, user rights and file permissions, and auditing and monitoring of security-related events. In addition, weaknesses exist in other types of controls designed to physically secure computer resources, conduct suitable background investigations, segregate duties appropriately, and prevent unauthorized changes to application software. All of these weaknesses increase the risk that unauthorized individuals can gain access to HHS information systems and inadvertently or deliberately disclose, modify, or destroy the sensitive data that the department relies on to deliver its vital services.

A key reason for these control weaknesses is that the department has not yet fully implemented a departmentwide information security program. While HHS has laid the foundation for such a program by developing and documenting policies and procedures, the department has not yet fully implemented key elements of its information security program at all of its operating divisions. Specifically, HHS and its operating divisions have not fully implemented elements related to (1) risk assessments, (2) policies and procedures, (3) security plans, (4) security awareness and training, (5) tests and evaluations of control effectiveness, (6) remedial actions, (7) incident handling, and (8) continuity of operations plans. Until HHS fully implements a comprehensive information security program, security controls may remain inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

Contents

Abbreviations

CMS	Centers for Medicare & Medicaid Services
FISMA	Federal Information Security Management Act
HHS	Department of Health and Human Services
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

February 24, 2006

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

Dear Mr. Chairman:

The Department of Health and Human Services (HHS) is the nation's largest health insurer and the largest grant-making agency in the federal government. The department protects and promotes the health and well-being of all Americans and provides world leadership in biomedical and public health sciences. The programs of the department impact all Americans, whether through direct services, scientific advances, or information that helps them choose medical care, medicine, or even food. For example, the Centers for Medicare & Medicaid Services (CMS), a major operating division within HHS responsible for the Medicare and Medicaid programs, oversees the nation's largest health insurance programs, which provide care to about one in every four Americans.

HHS relies on automated information systems and interconnected networks to process and pay medical claims; conduct medical research; manage its wide spectrum of health, disease prevention, and food and safety programs; and support its departmentwide financial and management functions. Effective information security controls are essential for ensuring that information technology resources are adequately protected from inadvertent or deliberate misuse, fraudulent use, or destruction. Interruptions in HHS's financial and information management systems could have a significant adverse affect on the health, welfare, and mental well-being of millions of American citizens who depend on its services.

At your request, we assessed the effectiveness of the HHS information security program, particularly at CMS, in protecting the confidentiality, integrity, and availability of its information and information systems. To accomplish this objective, we evaluated the effectiveness of HHS's information security controls, and whether HHS had developed, documented, and implemented a departmentwide information security program consistent with federal laws and policies. To supplement our work, we analyzed 74 information security-related reports issued during 2004 and 2005 by HHS, its Office of the Inspector General (OIG), and

independent auditors. This review was performed from June through December 2005 in accordance with generally accepted government auditing standards. For further information about our objective, scope, and methodology, refer to appendix I.

Results in Brief

Significant weaknesses in information security controls at HHS and at CMS in particular put at risk the confidentiality, integrity, and availability of their sensitive information and information systems. HHS has not consistently implemented effective electronic access controls designed to prevent, limit, and detect unauthorized access to sensitive financial and medical information at its operating divisions and contractor-owned facilities. Numerous electronic access control vulnerabilities related to network management, user accounts and passwords, user rights and file permissions, and auditing and monitoring of security-related events exist in its computer networks and systems. In addition, weaknesses exist in controls designed to physically secure computer resources, conduct suitable background investigations, segregate duties appropriately, and prevent unauthorized changes to application software. These weaknesses increase the risk that unauthorized individuals can gain access to HHS information systems and inadvertently or deliberately disclose, modify, or destroy the sensitive medical and financial data that the department relies on to deliver its vital services.

A key reason for these weaknesses is that the department has not yet fully implemented its information security program. HHS has laid the foundation for an effective information security program by developing written policies and guiding procedures that designate responsibility for implementation throughout the department. However, it has not yet fully implemented key elements of the program. Specifically, its operating divisions have not fully implemented elements related to (1) risk assessments, (2) policies and procedures, (3) security plans, (4) security awareness and training, (5) tests and evaluations of control effectiveness, (6) remedial actions, (7) incident handling, and (8) continuity of operations plans. Without a fully implemented program, security controls may remain inadequate or inconsistently applied and responsibilities may be unclear, misunderstood, or improperly implemented. This may lead to insufficient protection of sensitive or critical resources, and disproportionately high expenditures on controls over low-risk resources.

In reports by the HHS OIG and other independent auditors, specific recommendations were made to the department to remedy identified

information security control weaknesses. In this report, we are recommending that the Secretary of Health and Human Services direct the HHS Chief Information Officer (CIO) to take steps to ensure full implementation of its information security program across all HHS operating divisions.

In commenting on a draft of this report, HHS supported our emphasis on improvements needed in key information security program elements, but did not believe that the report sufficiently reflected the progress that the department has made in addressing information security. We acknowledge in the report that HHS has made progress in correcting its information security control weaknesses and has begun to implement the foundation for an effective information security program. HHS also provided specific technical comments, which we have incorporated, as appropriate, in the report.

Background

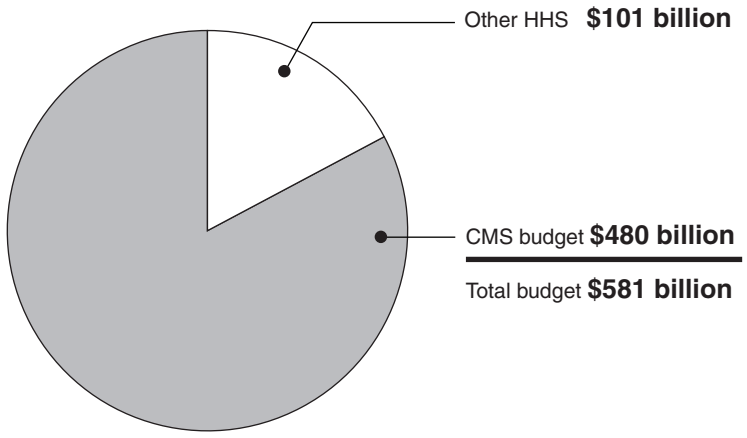
HHS is the federal government's principal agency responsible for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves. The department manages more than 300 programs covering a wide spectrum of activities that include health and social science research, disease prevention, food and drug safety, health information technology, health insurance for elderly and disabled Americans (Medicare), health insurance for low-income people (Medicaid), and comprehensive health services for Native Americans. Other services provided by the department include financial assistance to low-income families, pre-school education programs such as Head Start, child abuse and domestic violence programs, substance abuse treatment and prevention programs, and programs to help older Americans, such as providing home-delivered meals.

HHS has 14 operating divisions (see app. III for a description of each division) to manage its programs and administered more grant dollars than all other federal agencies combined. HHS employs about 67,000 employees and is responsible for managing a fiscal year 2005 budget of approximately $581 billion. Each year HHS handles more than a billion health care claims, supports over 38,000 research projects focusing on diseases, provides funding to treat more than 650,000 persons with serious substance abuse or mental health problems, and serves more than 900,000 pre-school children.

The Centers for Medicare & Medicaid Services (CMS) is an HHS operating division responsible for administering 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 the disabled. In partnership with the states, CMS also administers Medicaid, a means-tested health care program for low-income Americans. Medicaid is the primary source of health care for a large population of medically vulnerable Americans, including poor families, the disabled, and persons with developmental disabilities requiring long-term care. In coordination with the Medicaid program, the State Children's Health Insurance Program provides health care coverage for children. CMS employs about 4,900 employees and has a fiscal year 2005 budget of approximately $480 billion or 83 percent of the HHS budget, as shown in figure 1.

Figure 1: HHS Fiscal Year 2005 Budget



Source: HHS.

HHS relies extensively on computerized systems to support its mission critical operations and store the sensitive information it collects. It uses these systems to support the department's financial and management functions, maintain sensitive employee personnel information, and process financial and medical data for millions of health care recipients. Its local and wide area networks interconnect these systems. In addition, HHS relies on contractor-owned systems to process departmental information and support its mission. For fiscal year 2005, HHS planned to spend nearly $5 billion on information technology—more than any other federal agency

except the Department of Defense. A significant amount of these funds will be spent to facilitate the processing and payment of Medicare claims processed by CMS or its Medicare contractors.

Information system controls are a critical consideration for any organization that depends on computerized systems and networks to carry out its mission or business. Without proper safeguards, there is risk that individuals and groups with malicious intent may intrude into inadequately protected systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks.

In December 2002, Congress enacted the Federal Information Security Management Act of 2002 (FISMA)[1] to strengthen security of information and information 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 provided or managed by another agency, contractor, or other source. In addition, FISMA provides that the Secretary of HHS is responsible for, among other things, (1) providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information systems and information; (2) ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control; and (3) delegating to the agency CIO the authority to ensure compliance with the requirements imposed on the agency under the act.

HHS's CIO is responsible for developing, promoting, and coordinating the departmentwide information security program; developing, promulgating, and enforcing department information resource management policies, standards, and guidelines; and appointing the HHS chief information security officer. Each operating division, including CMS, is responsible for complying with the requirements of FISMA and departmentwide security-related policies, procedures, and standards; reporting on the effectiveness of its information security program; and ensuring that

[1]Title III, E-Government Act of 2002, P.L. 107-347 (Dec. 17, 2002).

information systems operated by or on its behalf by contractors provide adequate risk-based security safeguards.

Weak Controls and Incomplete Implementation Compromise Effectiveness of HHS's Information Security Program

HHS and CMS in particular have significant weaknesses in electronic access controls and other information system controls designed to protect the confidentiality, integrity, and availability of information and information systems. A key reason for these weaknesses is that the department has not yet fully implemented a departmentwide information security program. As a result, HHS's medical and financial information systems are vulnerable to unauthorized access, use, modification, and destruction that could disrupt the department's 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 network management, user accounts and passwords, user rights and file permissions, and auditing and monitoring of security-related events. Our analysis of reports issued by the OIG and independent auditors disclosed that HHS did not consistently implement effective electronic access controls in each of these areas.

Network Management

Networks are collections of interconnected computer systems and devices that allow individuals to share resources such as computer programs and information. Because sensitive programs and information are stored on or transmitted along networks, effectively securing networks is essential to protecting computing resources and data from unauthorized access, manipulation, and use. Organizations secure their networks, in part, by installing and configuring network devices that permit authorized network service requests, deny unauthorized requests, and limit the services that are available on the network. Devices used to secure networks include (1) firewalls that prevent unauthorized access to the network, (2) routers

that filter and forward data along the network, (3) switches that forward information among segments of a network, and (4) servers that host applications and data. Network services consist of protocols for transmitting data between network devices.

Insecurely configured network services and devices, including those without current software patches, can make a system vulnerable to internal or external threats, such as denial-of-service attacks.[2] Because networks often include both external and internal access points for electronic information assets, failure to adequately secure these access points increases the risk of unauthorized disclosure and modification of sensitive information or disruption of service. HHS policy requires that all incoming and outgoing connections from departmental systems and networks to the Internet, intranets,[3] and extranets[4] be made through a firewall and that effective technical controls be implemented to protect computing resources connected to the network.

Our analysis found that HHS did not consistently configure network services and devices securely to prevent unauthorized access to and ensure the integrity of computer systems operating on its networks. The reports we reviewed identified weaknesses in the way that HHS operating divisions and contractors restricted network access, managed antivirus software, configured network devices, and protected information traversing the HHS networks. For example,

- System administrative access was not always adequately restricted, and unnecessary services were available on several network devices, increasing the risk that unauthorized individuals could gain access to the operating system.

- Antivirus software was not always installed or up-to-date on the operating divisions' and contractors' workstations, increasing the risk

[2]A denial-of-service attack is an attack on a network that sends a flood of useless traffic that prevents legitimate use of the network.

[3]An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network.

[4]An extranet is a private network that uses Internet technology and the public telecommunication system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers, or other businesses.

that viruses could infect HHS systems and potentially disable or disrupt system operations.

- Key network devices were not securely configured to prevent unauthorized individuals from gaining access to sensitive system configuration files and router access control lists. These weaknesses could allow an external attacker to circumvent network controls and thereby gain unauthorized access to the internal network.

- HHS did not encrypt certain information traversing its networks. Instead, it used clear text protocols that make network traffic susceptible to eavesdropping.

- HHS's operating divisions and contractors did not consistently patch their computer systems and network devices in a timely manner. For example, the OIG reported that approximately 25 percent (287 of 1,129) of the systems tested at one operating division did not have up-to-date patches installed on them. Thirty of the machines tested were missing nine or more software patches that had been rated as critical by the vendor. At another operating division, over 90 high-risk software patch management vulnerabilities were outstanding from June 1999 through April 2005. Failure to keep system patches up-to-date could lead to denial-of-service attacks or to individuals gaining unauthorized access to network resources. According to the HHS chief information security officer, a patch management subcommittee was formed to address this issue and has formulated and published an approach to the department's patch management problems.

User Accounts and Passwords

A computer system must be able to identify and differentiate among 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. The combination of identification and authentication—such as user account and password combinations—provides the basis for establishing individual accountability and for controlling access to the system. Accordingly, agencies (1) establish password parameters, such as number of characters, type of characters, and the frequency with which users should change their passwords, in order to strengthen the effectiveness of passwords for authenticating the identity of users;

(2) require encryption for passwords to prevent their disclosure to unauthorized individuals; and (3) implement procedures to control the use of user accounts. HHS policy requires that all operating divisions implement and enforce logical password controls for all departmental systems and networks.

Our analysis of reported weaknesses showed that HHS did not adequately control user accounts and passwords to ensure that only authorized individuals were granted access to its systems. For example, the department and its contractors did not always implement strong passwords—using vendor-default or easy to guess passwords. Additionally,

- One CMS Medicare contractor set passwords to never expire for 28 service accounts with powerful administrative privileges. As a result, an unauthorized individual could use a compromised user identification and password for an indefinite period to gain unauthorized access to server resources.

- Firewall administrators for another CMS Medicare contractor used a shared administrative account. As a result, the actions taken by these individuals cannot be traced back to the responsible individual.

- The minimum password length on one operating division's local area network was set to zero. Consequently, users could create short passwords. Short passwords tend to be easier to guess or crack than longer passwords. In addition, passwords on this local area network were not required to be changed at initial logon.

Such weaknesses increase the risk that passwords may be disclosed to unauthorized users and used to gain access to the system. They also diminish the effectiveness of these controls for attributing system activity to individuals. As a result, HHS may not be able to hold these users individually accountable for system activity.

User Rights and File Permissions

The concept of "least privilege" is a basic underlying principle for securing computer systems and data. It means that users are granted only those access privileges needed to perform their official duties. To restrict legitimate users' access to only those programs and files that they need 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 and regulate which users can access them 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. HHS policy requires that access privileges be granted to users at the minimum level required to perform their job-related duties.

Our analysis of OIG reports showed that HHS granted access rights and permissions that gave some users more access to departmental information and medical systems than they needed to perform their jobs. For example, the following vulnerabilities were identified:

- All users could access world-readable start up scripts and files on several Medicare contractor systems. A malicious user could use this information to increase their system privileges.
- Members of the "Everyone" group were granted access to sensitive Windows directories, files, and registry settings, even though some did not have a legitimate business need for this access.
- Twenty-two groups or users without a legitimate need could access and update mainframe production data at one CMS Medicare contractor facility.
- Six of 15 employees reviewed at one operating division retained access privileges to the local area network after their separation from the department.

Inappropriate access to sensitive files and directories provides opportunities for individuals to circumvent security controls to deliberately or inadvertently read, modify, or delete critical or sensitive information and computer programs.

Auditing and Monitoring of Security-Related Events

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 can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track

security-related events. HHS policy requires that audit logging be enabled for all departmental systems and networks so that security-related events—the manipulation, modification, or deletion of data—can be monitored and analyzed for unauthorized activity.

HHS has not consistently audited and monitored security-related system activity on their systems. For example, the OIG reported that logging on some UNIX systems was either disabled or configured to overwrite these events, firewall and router logs were not routinely monitored, and procedures for classifying and investigating security–related events had not been documented at several HHS operating divisions and CMS Medicare contractors. As a result, if a system was modified or disrupted, the department's ability to trace or recreate events could be diminished. In addition, these weaknesses could allow unauthorized access to go undetected.

In response to weaknesses identified in electronic access controls, the HHS chief information security officer indicated that significant progress has been made in correcting these weaknesses and that preliminary results of fiscal year 2005 audits, by independent auditors, show a reduction in the number of weaknesses. In addition, the independent auditor of HHS's financial statements for fiscal year 2005 reported that HHS had made significant progress in strengthening system controls, although it continued to identify general controls issues that represent significant deficiencies in the design and operation of electronic access controls.

Other Information System Controls Are Ineffective

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 policies, procedures, and techniques to physically secure computer resources, conduct appropriate background investigations, provide sufficient segregation of duties, and prevent unauthorized changes to application software. Our analysis of reports issued by the OIG and independent auditors disclosed significant weaknesses in each of these areas. These weaknesses increase the risk that unauthorized individuals can gain access to HHS information systems and inadvertently or deliberately disclose, modify, or destroy the sensitive medical and financial data that the department relies on to deliver its vital services.

Physical Security

Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft. These controls

restrict physical access to computer resources, usually by limiting access to the buildings and rooms in which the resources are housed and by periodically reviewing the access granted, in order to ensure that access continues to be appropriate. HHS policy requires that physical access to rooms, work areas and spaces, and facilities containing departmental systems, networks, and data be limited to authorized personnel; controls be in place for deterring, detecting, monitoring, restricting, and regulating access to sensitive areas at all times; and controls be commensurate with the level of risk and sufficient to safeguard these resources against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

Our analysis showed that HHS did not effectively implement physical controls as the following examples illustrate:

- One CMS Medicare contractor used a privately owned vehicle and an unlocked container to transport approximately 25,000 Medicare check payments over a 1-year period.
- Four hundred forty individuals were granted unrestricted access to an entire data center, including a sensitive area within the data center—although their jobs functions did not require them to have such access.
- Surveillance cameras used for monitoring a facility were not functioning, leading to blind spots in the data center's perimeter security.
- Three individuals with access to an operating division's data center did not have management approval for such access.

These weaknesses in physical security increase the risk that unauthorized individuals could gain access to sensitive computing resources and data and inadvertently or deliberately misuse or destroy them.

Background Investigations

According to Office of Management and Budget (OMB) Circular A-130,[5] it has long been recognized that the greatest harm to computing resources has been done by authorized individuals engaged in improper activities—whether intentionally or accidentally. Personnel security controls (such as

[5]Office of Management and Budget, Circular A-130, appendix III, *Security of Federal Automated Information Resources* (Nov. 28, 2000).

screening individuals in positions of trust) are particularly important where the risk and magnitude of potential harm is high. The National Institute of Standards and Technology (NIST) guidelines suggest that agencies determine the sensitivity of particular positions, based on such factors as the type and degree of harm that the individual could cause by misusing the computer system and on more traditional factors, such as access to classified information and fiduciary responsibilities. Background investigations help an organization to determine whether a particular individual is suitable for a given position by attempting to ascertain the person's trustworthiness and appropriateness for the position. The exact type of screening that takes place depends on the sensitivity of the position and any applicable regulations by which the agency is bound.

HHS policy requires that all information security employees and contractor personnel be designated with position-sensitivity levels that are commensurate with the responsibilities and risks associated with their position. In addition, it requires suitability background investigations to be completed and favorably adjudicated for all personnel assigned to these positions prior to allowing them access to sensitive HHS systems and networks.

Our analysis of prior reports showed that background investigations were not always performed. For example, 13 CMS Medicare contractors had weaknesses in their background investigation policies and procedures. Six of the contractors reviewed were not adhering to established policies, while the remaining seven were not performing background investigations in a consistent manner. In addition, one operating division was unable to provide the background investigation status for any of the 49 contractor personnel working at its data center or for any of the 28 contractor personnel supporting one of its general support systems. Additionally, background investigations at three operating divisions were considered inadequate because they were not performed at the appropriate sensitivity level. Granting people access to sensitive data without appropriate background investigations increases the risk that unsuitable individuals could gain access to sensitive information, use it inappropriately, or destroy it.

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 be implemented, and computer resources could be damaged or destroyed. HHS policy requires operating divisions to ensure that responsibilities with a security impact be shared among multiple staff by enforcing the concept of separation of duties, which requires that individuals do not have control of the entirety of a critical process.

Our analysis of OIG reports showed that HHS did not always sufficiently segregate computer functions. For example, some software developers had full access to both development and production software libraries. To illustrate, UNIX developers at one facility used a shared user account to promote development changes into the production environment. In another instance, two individuals with full access to development source code also had update capabilities to production libraries. Consequently, increased risk exists that these individuals could introduce software errors into production or perform unauthorized system activities without being detected.

Application Change Controls

It is important to ensure that only authorized and fully tested application programs are placed into operation. To ensure that changes to application programs are necessary, work as intended, and do not result in the loss of data or program integrity, such changes should be documented, authorized, tested, and independently reviewed. In addition, test procedures should be established to ensure that only authorized changes are made to the application's program code. HHS policy requires that operating divisions establish, implement, and enforce change management and configuration management controls on all departmental systems and networks that process, store, or communicate sensitive information.

However, our analysis showed that HHS did not always document or control changes to application programs as the following examples demonstrate:

- Authorization forms did not exist for each of the 21 application control changes reviewed at one Medicare contractor facility. In addition, change control procedures were out-of-date and did not reflect current process and practice.

- Testing documentation at one operating division was not maintained for 4 of 15 change requests reviewed.

Without adequately documented or controlled application change control procedures, changes may be implemented that are not authorized, tested, or approved. Further, the lack of adequate controls place HHS at greater risk that software supporting its missions will not produce reliable data or effectively meet its business needs.

In response to weaknesses identified in other information security controls, the HHS chief information security officer indicated that significant progress has been made in correcting these weaknesses and that preliminary results of fiscal year 2005 audits, by independent auditors, show a reduction in the number of weaknesses. In addition, the independent auditor of HHS's financial statements for fiscal year 2005 reported that HHS had made significant progress in strengthening system controls, although it continued to identify general controls issues that represent significant deficiencies in the design and operation of key controls such as physical access, system software, and application development and program change controls.

Information Security Program Is Not Yet Fully Implemented

A key reason for the information security weaknesses identified at HHS was that the department had not yet fully implemented its information security program. A departmentwide security program provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. Without such a program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

FISMA[6] requires each agency to develop, document, and implement an information security program that includes the following key elements:

- periodic assessments of the risk and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;
- policies and procedures that (1) are risk-based, (2) cost-effectively reduce risks, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;
- plans for providing adequate information security for networks, facilities, and systems;
- security awareness training to inform personnel—including contractors and other users of information systems—of information security risks and of their responsibilities in complying with agency policies and procedures;
- at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices relating to management, operational, and technical controls of every information system identified in the agency's inventory;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security policies, procedures, or practices;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

[6]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. 44 USC § 3544(b).

FISMA also requires each agency to (1) annually report to OMB, selected congressional committees, and the Comptroller General on the adequacy of information security policies, procedures, and practices and compliance with requirements, and (2) its OIG or independent external auditor perform an independent annual evaluation of the agency's information security program and practices.

HHS has begun to implement the foundation for an effective information security program through its Secure One initiative by developing and documenting policies and procedures that designate implementation responsibilities. For example, HHS information security program provides baseline security policies and standards for the department. Operating divisions are required to comply with departmental standards or develop specific standards that exceed them. In addition, HHS uses an automated security management tool to collect, analyze, and report FISMA data. Similarly, CMS has made progress in developing and documenting its information security policies and procedures.

Although HHS has made progress in developing and documenting a departmentwide information security program, it has not fully implemented the following key elements: risk assessments, policies and procedures, system security planning, security and awareness training, periodic testing and evaluation of controls, remedial action plans, incident handling, and continuity of operations. These weaknesses limit HHS's ability to protect the confidentiality, integrity, and availability of its information and information systems.

Risk Assessments

Identifying and assessing information security risks are essential to determining what controls are required. By increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted. OMB Circular A-130, appendix III, prescribes that risk be reassessed when significant changes are made to computerized systems—or at least every 3 years, as does HHS policy. Consistent with NIST guidance, HHS requires that risk assessments characterize the system, identify information sensitivity and threats, determine the risk level of those threats and corresponding vulnerabilities, and analyze the potential business impact of exploited vulnerabilities.

HHS's performance in conducting risk assessments has varied across the department. Our review of 10 CMS risk assessments found that they generally complied with applicable federal and departmental guidance. By contrast, two of the three Office of the Secretary risk assessments reviewed did not fully address key elements. For example, the risk assessments did not identify threat sources, threat actions, or risk levels, as described in NIST SP 800-30.[7] Nor did they detail whether or not a business impact analysis had been completed. HHS's OIG also identified weaknesses in the department's risk assessments. In its 2005 FISMA evaluation, the OIG reported that risk assessments had not been performed on two major systems—one at the Administration for Children and Families, and one at the Administration on Aging.

In response to these weaknesses identified in the department's information security program, the HHS chief information security officer stated that risk assessments are currently being tracked using the department's FISMA data management tool, which compiles information security management data for monitoring and review. All operating divisions are required to enter their FISMA data into this automated tool so that it can be reviewed and validated by the Secure One program staff. The combination of this tool and feedback from the Secure One program is designed to improve the completion rate and quality of risk assessments. The lack of or incomplete risk assessments could result in HHS's systems having inadequate or inappropriate security controls that might not address those systems' true risk, and result in costly efforts to subsequently implement effective controls.

Policies and Procedures

Another key task in implementing an effective information security program is to develop and document risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. If properly implemented, policies and procedures should help to cost-effectively reduce the risk of unauthorized access, modification, and destruction of information and systems. Technical security standards should provide consistent implementing guidance for each computing environment. Because security policies are the primary mechanism by which management communicates its views and requirements, it is important to develop and document them. FISMA requires each agency to develop minimally acceptable system configuration requirements and

[7]NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

ensure compliance with them. Systems with secure configurations have less vulnerabilities and are better able to thwart network attacks.

HHS has not developed departmentwide policies regarding minimally acceptable configuration requirements. According to HHS's chief information security officer, HHS has neither developed nor documented such configuration requirements for its operating systems. The OIG reported in its fiscal year 2005 FISMA evaluation that these requirements were being maintained at the operating division level. In addition, the OIG found that three of the six operating divisions had not implemented minimum acceptable configuration requirements for their operating systems. Without departmentwide policies for developing minimally acceptable configuration requirements for its information systems, HHS may not be able to cost-effectively reduce information security risks to an acceptable level.

Security Plans

The objective of system security planning is to improve the protection of information technology resources. A system security plan is to provide a complete and up-to-date overview of the system's security requirements and describe the controls that are in place or planned to meet those requirements. FISMA requires that agency information security programs include subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate. OMB Circular A-130 specifies that agencies develop and implement system security plans for major applications and for general support systems and that these plans address policies and procedures for providing management, operational, and technical controls. According to NIST, security plans should include existing or planned security controls, the individual responsible for the security of the system, a description of the system and its interconnected environment, and rules of behavior. HHS policy requires all of its operating divisions to develop and document system security plans for all departmental systems and networks in accordance with NIST guidance[8] and to update such plans at least once every 3 years or when significant changes occur to the system.

Our review found that HHS and CMS system security plans generally complied with applicable federal and departmental guidance. We examined seven plans and determined that they were up-to-date, addressed existing

[8]NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

controls, identified responsible security personnel, described the system and its interconnections, and included rules of behavior. However, our analysis of OIG reports found that security plans had not been completed for two major systems—one at the Administration for Children and Families, and one at the Administration on Aging. Until its operating divisions complete security plans for all systems, HHS cannot ensure that appropriate controls are in place to protect its systems and critical information.

Awareness and Security Training

Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees and contractors who use computer resources in their day-to-day operations be made aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality, integrity, and availability. FISMA requires that an information security program promote awareness and provide training for users (federal employees and contractors) so that they can understand the system security risks and their role in implementing related policies and controls to mitigate those risks. HHS policy requires the establishment of an annual security awareness training program for all employees and contractors. In the event that a security breach occurs, amply trained security personnel are vital to a timely and appropriate response. Depending on an employee's specific security role, specialized training could include training in incident detection response, physical security, or firewall configuration. FISMA requires agency chief information officers to ensure that personnel with significant information security responsibilities receive specialized security training. HHS policy also require specialized security education and awareness training for all individuals with significant security responsibilities.

Although the department has made progress in security awareness training, the department had not provided adequate security training to employees with significant security related responsibilities. In fiscal year 2005, HHS reported that 98 percent of its employees, including contractors, had received security awareness training. However, it reported that 32 percent of its employees with significant security related responsibilities had not received specialized security training. Conversely, CMS reported that 100 percent of its employees with significant security related responsibilities had received such training. Without sufficiently trained security personnel, security lapses are more likely to occur and could contribute to information security weaknesses at HHS.

Tests and Evaluations

Another key element of an information security program is testing and evaluating system controls to ensure that they are appropriate, effective, and comply with policies. An effective program of ongoing tests and evaluations can be used to identify and correct information security weaknesses. This type of oversight demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests may encourage compliance with security policies, the full benefits of testing are not achieved unless the test results are analyzed by security specialists and business managers and used as a means of identifying new problem areas, reassessing the appropriateness of existing controls, and identifying the need for new controls.

FISMA requires that agencies test and evaluate the information security controls of their systems, and that the frequency of such tests be based on risk, but occur no less than annually. HHS requires systems and networks that contain sensitive or mission critical information to undergo vulnerability scanning and/or penetration testing to identify security threats at least annually or when significant changes are made to the system or network. HHS also requires that a self-assessment be conducted of all departmental systems and networks at least annually in accordance with NIST SP 800-26.[9] Consistent with FISMA provisions and HHS guidance, CMS policy also requires periodic testing and evaluation of its information systems' security controls.

Although HHS has initiatives under way to improve its testing and evaluation of controls, it has not fully implemented an ongoing program of tests and evaluations. Our analysis of the OIG's fiscal year 2005 FISMA report found that several operating divisions had not tested and evaluated security controls for all their systems. For example, three systems at three different operating divisions had not undergone system testing and evaluation. At another operating division, system tests and evaluations for three of its six major applications had not been completed.

Without comprehensive tests and evaluations of security controls, HHS cannot be assured that employees and contractors are complying with

[9]NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Services*, July 2002.

established policies or those policies and controls are appropriate and working as intended.

Remedial Actions

Remedial action plans, also known as plans of actions and milestones, can assist agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses in information systems. According to OMB Circular A-123, agencies should take timely and effective action to correct deficiencies that they have identified through a variety of information sources. To accomplish this, remedial action plans should be developed for each deficiency, and progress should be tracked for each. In compliance with OMB policy, HHS requires the capture of all information security program and system control weaknesses that require mitigation in remedial action plans. In addition, HHS has provided information security managers and system owners guidance for developing, maintaining, and reporting their remedial action plans.

Our review of OIG reports on selected operating divisions identified shortcomings in the HHS remedial action process. For example, the remedial action plans for three operating divisions did not include weaknesses previously identified in the operating divisions' risk assessments, OIG audits, or other independent audits. Moreover, the remedial action plans for four operating divisions contained overdue corrective action items and lacked key corrective action information, such as the risk level assigned to weaknesses, resources needed to remedy the weaknesses, and adequate support to demonstrate closed weaknesses. Our review of CMS remedial action plans yielded similar results. Specifically, we found 20 percent of the corrective actions did not identify the resources needed to correct those weaknesses.

Without a sound remediation process, HHS cannot be assured that weaknesses in its information security program will be efficiently and effectively corrected.

Incident Handling

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they take steps to promptly detect and respond to them before significant damage is done. In addition, analyzing security incidents allows organizations to gain a better understanding of the threats to their information and the costs of their security-related problems. Such analyses can pinpoint vulnerabilities that need to be eliminated so that they will not be exploited again. Incident reports can be used to provide valuable input for risk assessments, help in prioritizing security improvement efforts, and illustrate risks and related

trends for senior management. FISMA requires that agency information security programs include procedures for detecting and reporting security incidents. To ensure effective handling of incidents, HHS policy requires the establishment and maintenance of an incident response capability that includes preparation, identification, containment, eradication, recovery, and follow-up capabilities.

HHS operating divisions did not always employ adequate incident detection capabilities. Our analysis of OIG reports found, for example, that 13 CMS Medicare contractors had weaknesses in their intrusion detection policies and procedures. Five of the contractors did not have intrusion detection systems in place, while six were cited for either not reporting incidents in accordance with FISMA guidance or not reporting incidents to CMS. The remaining two contractors exhibited weaknesses in their incident monitoring process and procedures. Finally, one operating division used router and firewall logs for troubleshooting instead of for intrusion detection.

The wide disparity in the reporting of security incidents[10] and events[11] at HHS and its operating divisions also raises concern. For example, the Food and Drug Administration reported over 16 million events while the Centers for Medicare & Medicaid Services and the Centers for Disease Control and Prevention combined reported less than 1,600, as indicated in table 1.

[10]HHS defines a security incident as the violation of an explicit or implied security policy in a computing or telecommunications system or network.

[11]HHS defines an event as a notable occurrence in a network or system.

Table 1: Reported Incidents among HHS Operating Divisions

September 2005 Event Summary		
Operating division	**Number of events**	**Number of incidents**
Food and Drug Administration	16,515,911	1
National Institutes of Health	1,142,424	0
Health Resources and Services Administration	348,346	0
Office of the Secretary	162,197	1
Indian Health Service	79,911	2
Program Support Center	9,125	0
Office of the Inspector General	8,839	0
Agency for Healthcare Research and Quality	1,682	0
Administration for Children and Families	1,560	0
Centers for Disease Control and Prevention	1,074	0
Centers for Medicare & Medicaid Services	429	1
Administration on Aging	244	0
Substance Abuse and Mental Health Services Administration	0	0

Source: HHS.

Notes: Incidents were reported to the U.S. Computer Emergency Response Team. No data were available for the Agency for Toxic Substances and Disease Registry.

HHS operating divisions collectively reported over 18 million events during September 2005 but less than 10 incidents. We did not attempt to assess the accuracy of the reported events and incidents. However, the disparity in the number of reported events among the operating divisions of relatively similar size raises concerns. This disparity may be an indication of inconsistency among criteria settings and configuration requirements for the respective intrusion detection systems. The reporting disparities may also be influenced by the type and location of the intrusion detection systems. For example, an intrusion detection system located behind a firewall detects fewer events than one located on the perimeter in front of a firewall because of the firewall's ability to block certain network traffic. Intrusion detection systems' visibility to the Internet also increases the potential exposure to security events. Without consistent detection and reporting, HHS cannot be assured that it is handling incidents in an effective manner.

Continuity of Operations

Continuity of operations controls can enable systems to be recovered quickly and effectively following a service disruption or disaster. Such controls include plans and procedures designed to protect information resources and minimize the risk of unplanned interruptions, along with a plan to recover critical operations should interruptions occur. These controls should be designed to ensure that when unexpected events occur, key operations continue without interruption or are promptly resumed, and critical and sensitive data are protected. They should also be tested annually or as significant changes are made. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. Consistent with federal guidance, HHS policy requires operating divisions to identify, prioritize, and document disaster recovery planning requirements for all critical departmental systems, networks, data, and facilities. CMS's information security policy complies with the departmentwide policy. CMS's Information Security Handbook provides additional guidance as to what key elements should be included in contingency plans. These elements are further detailed in its guidance to CMS contractors.

HHS has various efforts underway to address continuity of operations. In its fiscal year 2005 FISMA report, the OIG noted the elimination of the department's significant deficiency relating to contingency planning and disaster recovery. However, shortcomings in continuity of operations still exist. In its FISMA report to OMB for fiscal year 2005, HHS reported that 19.2 percent of its FISMA inventoried systems (34 out of 177) did not have tested contingency plans. Furthermore, the OIG also identified deficiencies in continuity of operations plans developed at HHS's operating divisions. For example,

- contingency plans for four major applications at one operating division were not application specific, but were actually the same plan originally developed for the server recovery;
- contingency plans did not exist for the local area networks of four operating divisions;
- another operating division did not prioritize the recovery of its systems in the divisionwide contingency plan; and
- inadequate documentation existed to determine whether testing had been performed for one of another division's contingency plans.

As a result of these weaknesses, the department has limited assurance that operating divisions will be able to protect critical and sensitive information and information systems and resume operations promptly when unexpected events or unplanned interruptions occur. If continuity of operations controls are inadequate, even a relatively minor interruption could result in significant adverse impact on HHS operating divisions' ability to recover and resume operations.

Conclusions

Given the size and significance of HHS's information technology investments, and the sensitivity of the medical, personal, and financial data it maintains through these investments, it is imperative that the department develops strong information security controls and implements a comprehensive information security program. While HHS has made progress toward developing and documenting a departmentwide information security program, significant weaknesses in information security controls could lead to the unauthorized disclosure, modification, or destruction of the sensitive data that HHS relies on to accomplish its vital mission. A key reason for these weaknesses is that HHS has not yet fully implemented a departmentwide information security program that can establish and maintain effective controls. Full implementation of such a program would provide for periodically assessing risks, establishing appropriate policies and procedures, developing and implementing security plans, promoting security awareness training, testing and evaluating the effectiveness of controls, implementing corrective actions, responding to incidents, and ensuring continuity of operations. Implementing such a program across all operating divisions requires effective management oversight and monitoring, especially at a department as diverse as HHS. Until HHS strengthens information security controls and fully implements its information security program, it will have limited assurance that its operations and assets are adequately protected.

Recommendations for Executive Action

To help HHS fully implement its departmentwide information security program, we recommend that the Secretary of HHS direct the Chief Information Officer to develop and implement policies and procedures to ensure the establishment of minimum acceptable configuration requirements. In addition, we recommend that the Secretary direct the Chief Information Officer to take the following seven steps to ensure that operating divisions

- develop comprehensive risk assessments that address key elements;
- complete system security plans for all systems;
- provide specialized training to all individuals with significant security responsibilities;
- conduct tests and evaluations of the effectiveness of controls on operational systems, and document results;
- review remedial action plans to ensure that they address all previously identified weaknesses and key corrective action information;
- implement intrusion detection systems and configure them to use consistent criteria for the detection and reporting of security incidents and events; and
- develop and test continuity of operations plans for all of their systems.

Agency Comments and Our Evaluation

The Department of Health and Human Services's Inspector General transmitted the department's written comments on a draft of this report (reprinted in app. II). In these comments, HHS supported our emphasis on improvements needed in key information security program elements, but stated that our report did not appropriately reflect the progress that the department has made in addressing information security.

Specifically, HHS expressed concerns that our evaluation approach did not provide an accurate or complete appraisal of the department's information security program, in that the report does not mention the department's defense-in-depth strategy or accomplishment of two major goals—the department's campaign to mitigate its deficiency pertaining to contingency planning and reduce its number of reportable conditions by 25 percent. According to HHS, it employs a defense-in-depth strategy to ensure threats are effectively addressed and mitigated. We acknowledge HHS's statement on its defense-in-depth strategy, but note that the significant control weaknesses identified in this report and by independent auditors indicate that this strategy is not fully working as intended. With regard to the two major goals, we have revised the report to reflect the elimination of the contingency planning deficiency. Regarding the department's reduction in

the number of reportable conditions, in its report on internal controls,[12] the OIG's independent auditor reported progress made in strengthening security controls; however, it still reported weaknesses in several information security areas, including the entitywide security program, access controls, application development and program change controls, system software, and service continuity.

HHS also noted that our report did not mention recent improvements or progress made in information security until a brief statement in the conclusion of the report, and that the report was predicated on findings originally documented by the HHS OIG in fiscal year 2005. However, throughout the report we acknowledge HHS's improvements and progress made in correcting information security weaknesses and have added additional statements based on these comments. In addition, as noted in our scope and methodology, our evaluation included the most recent reports issued at the time of our review.

In its comments, HHS also expressed concern over our use of the word "significant" to describe the reported weaknesses. In their most recent report on internal controls, the OIG's independent auditor reported information security as a "reportable condition"[13] at the department. The auditors concluded that "the cumulative effect of these weaknesses represents significant deficiencies in the overall design and operation of internal controls." Based on the findings in our report, the definition of "reportable condition," and the comments of the independent auditors, we believe the use of the word "significant" is appropriate to describe these weaknesses.

HHS also took exception to our conclusion that it had not fully implemented a departmentwide information security program, and stated that our findings instead indicate that the full integration or maturity of the program has not been achieved. FISMA requires that agencies develop, document, and implement an information security program. As stated in our report, we acknowledged that HHS has made progress in developing and documenting its program. However, elements of the program have not

[12]Included in HHS's *Fiscal Year 2005 Performance and Accountability Report*, section III.

[13]The American Institute of Certified Public Accountants' standards define "reportable conditions" as significant deficiencies in the design or operation of internal control that could adversely affect the entity's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

been fully or consistently implemented. For example, three systems at three different operating divisions had not undergone system testing and evaluation. As a result, we believe that the use of the phrase "not fully implemented" is appropriate for describing HHS's shortcomings in its information security program.

Additionally, the department stated that our assessment of its security program was based on a small percentage of HHS systems. However, as noted in our scope and methodology, we selected applications and general support systems because they support HHS's departmentwide financial reporting and communications, or Medicare payment and communication functions at CMS and its contractors—operations that are critical to the department. These included the Medicare Claims Processing Systems that processed over one billion claims and $294 billion in claims payments in 2004; the CMS Communication Network that provides connectivity between CMS and its business-related entities; and the HHS Enterprise Services Network that provides a shared network backbone for several HHS operating divisions.

The department also noted that our statement that HHS had not developed departmentwide policies regarding minimally acceptable configuration requirements was inaccurate. In its comments, HHS states that "plans are in place" to standardize implementation in fiscal year 2006 and that the divisional chief information security officers formed a subcommittee to develop configuration standards. Although these are positive efforts, we believe that such statements support our conclusion that such policies have not yet been developed.

In addition, the department noted that we did not acknowledge progress made relating to contingency planning. HHS stated that it had completed and tested contingency plans for 100 percent of its high-risk FISMA systems. However, the HHS OIG did not concur with this statement, reporting that one of the seven high-risk systems that they evaluated did not have tested contingency plans. As mentioned previously, the department also stated that we did not acknowledge the elimination of their sole existing significant deficiency relating to contingency planning and disaster recovery. We have revised the report to reflect the elimination of this deficiency.

Finally, the department noted additional improvements specific to CMS that were not included in our report. The department cited the elimination of a long standing CMS material weakness in Medicare electronic access

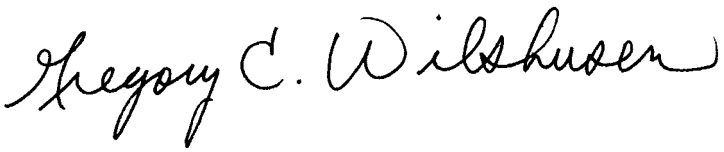
controls. However, this material weakness was downgraded to a reportable condition, indicating that significant deficiencies still exist. The department also stated that we did not acknowledge significant progress in FISMA compliance made by its fiscal intermediaries and carriers and that they provided these results to the HHS OIG in early December 2005. However, these reports were not available for release to us at that time. Additionally, the department stated that we did not acknowledge CMS's significant achievements in meeting it statutory responsibilities under FISMA, as reported by the HHS OIG. We acknowledge in the report that HHS, which includes CMS, has begun to implement the foundation for an effective information security program. While the HHS OIG FISMA report cited some achievements made by CMS, the HHS OIG also noted 28 exceptions in the CMS information security program.

HHS also provided specific technical comments, which we have incorporated, as appropriate, in the report.

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 of this report to the Secretary of Health and Human Services. 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 me at (202) 512-6244 or by e-mail at wilshuseng@gao.gov. 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 IV.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues

Objective, Scope, and Methodology

The objective of our review was to assess the effectiveness of the HHS information security program, particularly at CMS, in protecting the confidentiality, integrity, and availability of its information and information systems. To accomplish this objective, we evaluated the effectiveness of HHS's information security controls, and whether HHS had developed, documented, and implemented a departmentwide information security program consistent with federal laws and policies.

To evaluate the effectiveness of HHS's information security controls, we examined 74 management and audit reports pertaining to information security practices and controls at 13 operating divisions issued by the department, its Office of the Inspector General (OIG), and independent auditors during 2004 and 2005. These reports identified information security control weaknesses at HHS, the operating divisions, and contractor-owned facilities, which we then classified according to the general control categories specified in our Federal Information System Controls Audit Manual (FISCAM).[1] Further, these reports contained specific recommendations to the department to remedy identified information security control weaknesses.

To evaluate whether HHS had developed and documented a departmentwide information security program consistent with federal laws and policies, we examined related documents, such as policies and procedures, handbooks, various types of security-related reports, and HHS's information systems inventory. We assessed whether its program was consistent with the requirements of FISMA, as well as applicable Office of Management and Budget policies and National Institute of Standards and Technology guidance related to risk assessments, risk-based policies and procedures, information security plans, security awareness training, testing and evaluating security controls, remedial action plans, handling security incidents, and continuity of operations for information systems. We also held discussions with CMS and contractor officials responsible for information security management and with the HHS Inspector General staff regarding any related prior, ongoing, or planned work in these areas.

To evaluate whether HHS had implemented an information security program consistent with federal laws and policies, we focused our review

[1]GAO/AIMD-12.19.6 (Washington, D.C.: January 1999). FISCAM contains guidance for reviewing information system controls that affect the security of computerized data.

on CMS—the operating division with the largest budget in the department—as well as the Office of the Secretary, an operating division with a departmentwide perspective. We compared their documented practices and controls to the departmentwide information security program as well as applicable FISMA requirements, OMB policy, and NIST guidance. To determine how well the operating divisions were implementing their own policies and procedures, we evaluated available risk assessments, security plans, security and awareness training, system tests and evaluations, remedial actions, and continuity of operations for the following major applications and general support systems:

- Automated Financial Statement System—a system to collect operating divisions' financial statement data to generate the departmentwide year-end and quarterly statements.

- Information Collection Review and Approval System—a web-based database application used by HHS, the Securities and Exchange Commission and OMB to help federal agencies electronically administer and manage its information collection clearance responsibilities under the Paperwork Reduction Act.

- HHS's Enterprise Services Network—the enterprise network for the department. It is comprised of a combination of very high performance network services provided by a public communications carrier.

- Medicare Claims Processing Systems—a CMS contractor operated group of systems used to process Medicare claims—including inpatient hospital care, nursing facilities, home health care, and other health care services.

- CMS communications network—a private network that provides connectivity between CMS and its business-related entities that provide Medicare services.

We selected these applications and systems because they support either (1) HHS's enterprisewide financial reporting and communication functions, or (2) CMS's and its contractors' Medicare payments and communication functions.

We performed our work at HHS headquarters in Washington, D.C., and the CMS Central Office, located in Baltimore, Maryland. This review was performed from June through December 2005 in accordance with generally accepted government auditing standards.

Comments from the Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of Inspector General

Washington, D.C. 20201

FEB 14 2006

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

Enclosed are the Department's comments on the U.S. Government Accountability Office's (GAO) draft report entitled, "INFORMATION SECURITY: Department of Health and Human Services Needs to Fully Implement Its Program" (GAO-06-267). These comments represent the tentative position of the Department and are subject to reevaluation when the final version of this report is received.

The Department provided several technical comments directly to your staff.

The Department appreciates the opportunity to comment on this draft report before its publication.

Sincerely,

Daniel R. Levinson

Daniel R. Levinson
Inspector General

Enclosure

The Office of Inspector General (OIG) is transmitting the Department's response to this draft report in our capacity as the Department's designated focal point and coordinator for U.S. Government Accountability Office reports. OIG has not conducted an independent assessment of these comments and therefore expresses no opinion on them.

COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES ON THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED, "INFORMATION SECURITY: DEPARTMENT OF HEALTH AND HUMAN SERVICES NEEDS TO FULLY IMPLEMENT ITS PROGRAM" (GAO-06-267)

The Department of Health and Human Services (HHS) appreciates the opportunity to comment on the draft report. We appreciate the efforts GAO undertook to examine HHS's information security program. The comments that follow represent HHS's responses to the draft report.

The evaluation approach utilized by GAO does not provide an accurate or complete appraisal of the HHS enterprise-wide information security program. The GAO "Results in Brief" section and the majority of the remaining document focus exclusively on security control weaknesses that could place the confidentiality, integrity, and availability of sensitive information and information systems at risk. Yet, there is no mention of HHS's defense-in-depth strategy which is employed throughout the enterprise and results in layering of safeguards to ensure threats to confidentiality, integrity, and availability are effectively addressed and mitigated, thereby reducing the probability of single points of failure. Nor is there recognition of the ambitious campaign HHS launched in fiscal year (FY) 2005 to accomplish two major goals — address and mitigate its sole existing significant deficiency pertaining to contingency planning and disaster recovery and reduce its number of reportable conditions by 25 percent. In fact, HHS exceeded this goal, eliminating its sole significant deficiency and reducing the number of reportable conditions by 57 percent from FY 2004 to FY 2005. These accomplishments were documented in the FY 2005 Office of Inspector General (OIG) Federal Information Security Management Act (FISMA) Executive Summary, but not recorded in this draft GAO report. We request that these successes be noted in the GAO report.

There is no mention of HHS's information security improvements or progress until the brief statement in the conclusion of the report. The majority of the GAO report is predicated on the findings originally documented by HHS OIG in FY 2005, (between January and June 2005) and is representative of activities carried out in support of the information security program throughout 2004 and 2005. This GAO assessment is scheduled for publication in February 2006, but will not reflect at least seven additional months of progress and maturity in HHS's security posture. Please consider including the additional points and evidence provided in this draft GAO assessment response as confirmation of further strides made in support of HHS's information security program implementation in the months following the FY 2005 OIG evaluation.

The frequent use of the word "significant" to describe control weaknesses documented throughout this GAO assessment evokes a negative connotation that is not reflective of the progress or current state of HHS's information security program. In light of HHS's

1

successful elimination of its sole significant deficiency, HHS requests the removal of the word "significant" to describe the depth of control weaknesses in this assessment. Alternatively, we recommend use of "noteworthy" or "important" to describe these weaknesses.

HHS, consistent with the National Institute of Standards and Technology (NIST), defines implementation as observed consistency with policies and procedures. Evidence of general compliance with policy and procedures exists at the enterprise and OPDIV levels. In 2003, HHS formally established the foundation of its information security program to ensure the confidentiality, integrity, and availability of the information it collects, stores, and processes to meet its strategic missions on behalf of the American citizenry. Since 2003, the HHS information security program has continued to evolve, resulting in standard, repeatable security processes disseminated throughout its 14 Operating Divisions (OPDIVs). HHS, as acknowledged in the FY 2005 OIG FISMA Executive Summary, issued an overarching information security policy, an information security program handbook, and numerous guides. HHS initiated a variety of analysis and oversight activities, continuously monitoring and improving current security practices. The observations in this GAO assessment identify information security areas in which improvements can be made but, when considered collectively, do not equate to HHS having "not fully implemented a Department wide information security program."[1] Instead, these findings indicate that full integration, or maturity, has not yet been achieved. Integration represents a level of growth beyond implementation in which HHS tests security practices and controls for compliance and mitigates the results of these tests to demonstrate continued improvement. HHS, through its increasing oversight activities, strives towards such integration. Therefore, HHS agrees that full *integration* has not yet been achieved, but requests that the *implementation* of the security program be recognized in this report.

The HHS information security program addresses each of the key elements required by FISMA. HHS assesses risk periodically; disseminates necessary policies and procedures; develops security plans; delivers security awareness and training; tests and evaluates system controls at least annually; detects, responds to and reports incidents; plans continuity of operations; and maintains reliable monitoring and reporting capabilities. This programmatic structure, as mandated by law and proven in practice, led to the development of sound security practices and continuous improvement in HHS's overall security posture. On page 17, the GAO assessment implies that the HHS information security program is not "well-designed." The program, however, adheres to law and is acknowledged in the FY 2005 OIG FISMA Executive Summary as a program intended to "improve the Department's overall IT security posture, ensure adequate enterprise-wide security standards, support integration of IT security into lines of business, and promote an environment in which employee actions reflect the importance of IT security."[2] HHS requests that the terms "well-designed" and "fully implemented" be revised to read "fully integrated" to more accurately describe the HHS information security program posture.

---

[1]Report GAO-06-267, *Department of Health and Human Services Needs to Fully Implement Its Program*, page 6.
[2] *FY 2005 OIG Annual FISMA Executive Summary*, page 10.

2

The *HHS Information Security Program Policy*, signed by the HHS Chief Information Officer (CIO) and released to the HHS OPDIVs on January 26, 2004, articulates the roles and responsibilities for each category of security personnel and addresses each information program area required by FISMA. Compliance with this policy is mandatory. HHS developed an information security program handbook to complement this overarching security policy and to recommend procedures for implementation of policy stipulations. Therefore, the statement on page 19 asserting that "Operating divisions are expected to comply with departmental standards or develop specific standards that exceed them" is not accurate and should be revised. As stated on page v of the *Information Security Program Policy*, "compliance with this document is *mandatory*. It is HHS policy that Department personnel abide by or exceed the requirements outlined in this document." HHS requests that the word "expected" be replaced with "required" to reinforce the stringency of HHS's policy compliance.

In some instances, determinations were made regarding enterprise-wide weaknesses based on small percentages of HHS FISMA systems. Documentation pertaining to six or fewer percent of HHS's total FISMA systems is not evidence of incomplete implementation of an enterprise-wide security program. Nor does it indicate systematic problems in HHS's certification and accreditation (C&A) processes. The GAO assessment references four OPDIV risk assessments that lacked information or had not been completed. These four systems' risk assessments represent only two percent of HHS's 177 total FISMA systems. Two incomplete security plans were cited to constitute an overarching system security plan finding, although these two plans represent a mere one percent of the 177 HHS's FISMA systems. The GAO assessment identified six OPDIV systems for which annual system security control tests and evaluations were not completed, equaling only three percent of HHS's FISMA systems. The FY 2005 OIG FISMA findings document that 83.3 percent of the OPDIV system sample reviewed had completed C&A packages, including satisfactory risk assessments, system security plans, and annual security control tests and evaluations. In addition, in FY 2005, OIG deemed the Department's C&A process "satisfactory" for the first time. We believe that the statistics cited above more accurately reflect the current state of HHS's information security and that the related GAO findings should be excluded from the report.

The *HHS Information Security Program Policy* documents the following policy pertaining to change management and configuration management controls, "*3.6 Change Management Control*: Establish, implement, and enforce change management and configuration management controls on all Departmental systems and networks that process, store, or communicate sensitive information, to include the preparation of configuration control plans for all Departmental systems and networks."[3] The GAO assessment, on page 21, stating "HHS has not developed Department wide policies regarding minimally acceptable configuration requirements" is inaccurate and should be revised. Plans are in place to standardize, monitor, and enforce the extent of implementation according to OMB standards in FY 2006. OPDIV Chief Information Security Officers (CISO) also formed a

[3] *HHS Information Security Program Policy*, January 26, 2004, page 18.

3

configuration management subcommittee to develop configuration standards specific to the most predominant operating systems in the HHS security environment.

HHS, as noted in the FY 2005 OIG FISMA Executive Summary and above, "initiated procedures that resulted in the elimination of a previously identified significant deficiency." The Department established and completed contingency plans and performance testing at system levels, thereby eliminating this deficiency, related to Department level contingency planning and disaster recovery. HHS's role as the lead agency for public health services — including prevention, surveillance, laboratory services, and personal health services — made the elimination of this significant deficiency vital. Additionally, HHS completed and tested contingency plans for 100 percent of its high-risk FISMA systems, or those systems that would result in a catastrophic loss of confidentiality, integrity, and availability should their security be compromised. These accomplishments and their significance to the overall HHS mission should be noted in the GAO assessment.

In addition to our comments pertaining to the HHS enterprise-wide information security program, there are three additional points pertaining to the Centers for Medicare & Medicaid Services (CMS):

- In FY 2005, CMS initiated an aggressive initiative to rid itself of a material weakness attributable to Medicare Electronic Data Processing (EDP) based on Federal Information System Controls Audit Manual (FISCAM) audits performed in FY 2004. Our progress toward this goal was tracked monthly as a part of the HHS Risk Management and Financial Oversight Committee. The Medicare Claims Processing System (MCPS) was the primary focus of the GAO review. The FY 2005 Report of the Independent Auditors on Internal Control, also focused primarily on the MCPS, found that CMS had made improvements in its entity-wide security program, systems software, and service continuity planning and testing. There was a significant 63 percent reduction in high-risk findings in FY 2005 over FY 2004. The progress was such that the long-standing material weakness in Medicare EDP controls based on FISCAM was eliminated. The progress noted in the FY 2005 Report of the Independent Auditors on Internal Control was provided and discussed with the GAO auditors.

- In FY 2005, CMS also made significant progress in its compliance with the requirements of FISMA. Under section 912 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 CMS is required to evaluate our fiscal intermediaries and carriers for compliance with FISMA. Similar to the FISCAM findings, GAO based its conclusions, at least in part, on evaluations that were a year old. Again, CMS made significant strides in FY 2005. In fact, the FY 2005 evaluation results, provided to OIG in early December 2005, and offered to GAO, reflect a 70 percent reduction in high-risk findings over FY 2004, with significant improvement in the areas of Policies and Procedures, Systems Security Plans, Incident Handling, and Continuity of Operations.

- The FY 2005 OIG report of CMS's FISMA compliance also noted that CMS had made "significant achievements in meeting its statutory responsibilities under FISMA."

4

Accomplishments in security policy, contingency plans, and training were cited by OIG. Again, this documented improvement in CMS' FISMA compliance was not acknowledged in the GAO report, although the report was made available.

In summary, HHS is proud of its information security program and the progress it has made over the last fiscal year, specifically in its improved satisfaction of FISMA requirements. HHS proactively measures and tests compliance with information security policies, processes, Federal standards, and requirements. Testing indicates consistent improvements throughout the enterprise, but given such rigorous and aggressive testing, there will invariably be findings. HHS's emphasizes risk management and the strong remediation of discrepancies once identified. HHS places great importance on achieved progress and positive results. The Department utilizes such successes to build momentum within the program itself. HHS's proactive approach to security program implementation and management resulted in a substantial reduction in findings and risks, both at odds with the GAO report. We regret the GAO report did not consider the more recent data available.

HHS supports the GAO's emphasis on improvements in the eight areas of FISMA, since continuous improvement in system security exemplified through the system development lifecycle is a must for all government agencies. HHS endeavors to further improve its information security program, staying in step with existing and emerging Federal requirements and industry best practices.

5

HHS Operating Divisions

Administration for Children and Families—responsible for some 60 programs that promote the economic and social well being of children, families and communities.

Administration on Aging—supports a nationwide network providing services to the elderly, especially to enable them to remain independent.

Agency for Healthcare Research and Quality—supports research on health care systems, health care quality and cost issues, access to health care, and effectiveness of medical treatments. It provides evidence-based information on health care outcomes and quality of care.

Agency for Toxic Substances and Disease Registry—responsible for preventing exposure to hazardous substances from waste sites on the U.S. Environmental Protection Agency's National Priorities List and develops toxicological profiles of chemicals at these sites.

Centers for Disease Control and Prevention—provides a system of health surveillance to monitor and prevent disease outbreaks, implements disease prevention strategies, and maintains national health statistics. The centers also provide for immunization services, workplace safety, and environmental disease prevention. In addition, the centers guard against international disease transmission, with personnel stationed in more than 25 foreign countries.

Centers for Medicare & Medicaid Services—administers the Medicare and Medicaid programs, which provide health care to about one in every four Americans. Medicare provides health insurance for more than 42.1 million elderly and disabled Americans. Medicaid, a joint federal-state program, provides health coverage for some 44.7 million low-income persons, including 21.9 million children, and nursing home coverage for low-income elderly. CMS also administers the State Children's Health Insurance Program that covers more than 4.2 million children.

Food and Drug Administration—responsible for assuring the safety of foods and cosmetics, and the safety and efficacy of pharmaceuticals, biological products, and medical devices—products that represent almost 25 cents of every dollar in U.S. consumer spending.

Health Resources and Services Administration—provides access to essential health care services for people who are low-income, uninsured or who live in rural areas or urban neighborhoods where health care is scarce.

The agency helps prepare the nation's health care system and providers to respond to bioterrorism and other public health emergencies, maintains the National Health Service Corps, and helps build the health care workforce through training and education programs.

Indian Health Service—provides health services to 1.6 million American Indians and Alaska Natives of more than 550 federally recognized tribes. The Indian health system includes 49 hospitals, 247 health centers, 348 health stations, satellite clinics, residential substance abuse treatment centers, Alaska Native village clinics, and 34 urban Indian health programs.

National Institutes of Health—a medical research organization, supporting over 38,000 research projects nationwide in diseases including cancer, Alzheimer's, diabetes, arthritis, heart ailments, and AIDS.

Office of Inspector General—The OIG is responsible for protecting the integrity of HHS programs, as well as the health and welfare of the beneficiaries of those programs. It is also responsible for reporting program and management problems and recommendations to correct them to both the Secretary of HHS and to Congress. The OIG's duties are carried out through a nationwide network of audits, investigations, inspections, and other mission-related functions performed by OIG components.

Office of the Secretary—provides counsel to the secretary on such issues as public affairs, legislation, budget, technology, and finance.

Program Support Center—The Program Support Center was created in 1995 to provide a wide range of administrative support within the Department of Health and Human Services, allowing the department operating divisions to concentrate on their core functional and operational objectives.

Substance Abuse and Mental Health Services Administration— works to improve the quality and availability of substance abuse prevention, addiction treatment, and mental health services.

GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen (202) 512-6244

Acknowledgments

In addition to the person named above, Idris Adjerid, Larry Crosland, Jeffrey Knott, Carol Langelier, Ronald Parker, Amos Tevelow, and William Thompson 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