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.