August 2006

INFORMATION SECURITY

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

GAO Accountability · Integrity · Reliability

Highlights

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

Why GAO Did This Study

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

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

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

What GAO Recommends

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

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

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

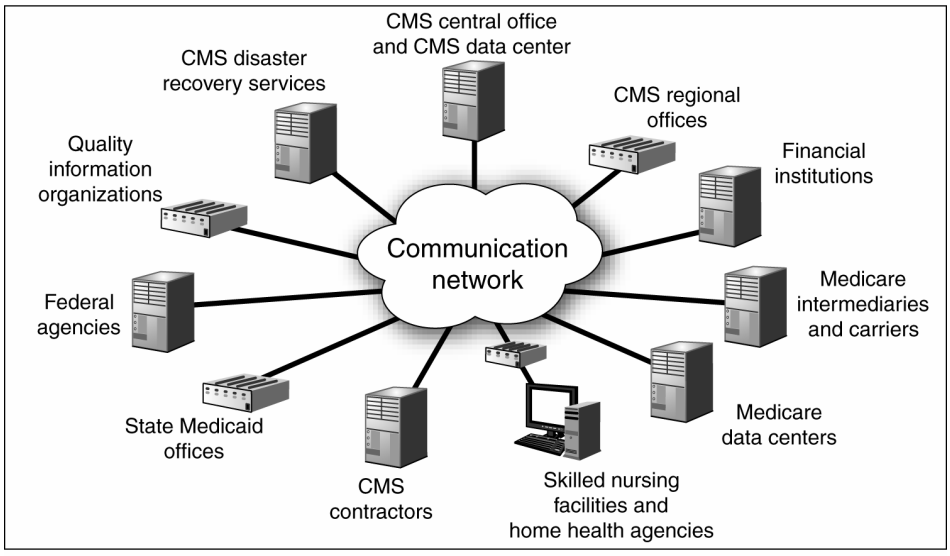
To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

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

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

Communication Network Interconnections



Source: CMS.