January 2004

INFORMATION SECURITY

Further Efforts Needed to Address Serious Weaknesses at USDA

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-154, a report to congressional requesters

Why GAO Did This Study

The U.S. Department of Agriculture (USDA) performs critical missions that enhance the quality of life for the American people, relying on automated systems and networks to deliver billions of dollars in programs to its customers; process and communicate sensitive payroll, financial, and market data; and maintain personal customer information. Interruptions in USDA's ability to fulfill its missions could have a significant adverse impact on the nation's food and agricultural production.

In addition, securing sensitive information is critical to USDA's efforts to maintain public confidence in the department. GAO was asked to evaluate the effectiveness of USDA's information security controls.

What GAO Recommends

GAO recommends that the Secretary of Agriculture direct the chief information officer (CIO) to correct a number of weaknesses, including fully implementing a comprehensive security management program. In commenting on a draft of this report, USDA concurred with our recommendations and stated that the department remains committed to improving information security. USDA plans to correct the specific information security weaknesses identified and fully implement a comprehensive security management program.

www.gao.gov/cgi-bin/getrpt?GAO-04-154.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

Significant, pervasive information security control weaknesses exist at USDA, including serious access control weaknesses, as well as other information security weaknesses. Specifically, USDA has not adequately protected network boundaries, sufficiently controlled network access, appropriately limited mainframe access, or fully implemented a comprehensive program to monitor access activity. In addition, weaknesses in other information security controls, including physical security, personnel controls, system software, application software, and service continuity, further increase the risk to USDA's information systems. As a result, sensitive data—including information relating to the privacy of U.S. citizens, payroll and financial transactions, proprietary information, agricultural production and marketing estimates, and mission critical data—are at increased risk of unauthorized disclosure, modification, or loss, possibly without being detected.

A key reason for the weaknesses in information system controls is that the department has not yet fully developed and implemented a comprehensive security management program to ensure that effective controls are established and maintained and that information security receives significant management attention. Although USDA has various initiatives under way, it has not yet fully implemented the key elements of a comprehensive security management program. For example, agency security personnel have lacked the management involvement needed to effectively implement security programs, three agencies have not completed any of the required risk assessments, and security controls have been tested and evaluated for less than half of the department's systems in the past year. USDA has recognized the need to improve information security throughout the department, including in the components that we reviewed.