July 2007

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-870, a report to congressional requesters

INFORMATION SECURITY

Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program

Why GAO Did This Study

Intended to enhance the security of U.S. citizens and visitors, United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program encompasses the pre-entry, entry, status management, and exit of foreign national travelers who enter and leave the United States at 285 air, sea, and land ports of entry.

GAO was asked to determine whether Department of Homeland Security (DHS) has implemented appropriate controls to protect the confidentiality, integrity, and availability of the information and systems used to support the US-VISIT program. To do this, GAO examined the controls over the systems operated by Customs and Border Protection (CBP) that support the US-VISIT program.

What GAO Recommends

GAO recommends that the Secretary of Homeland Security direct CBP to fully implement information security program activities for systems supporting the US-VISIT program. In commenting on a draft of this report, DHS stated that it has directed CBP to complete remediation activities to address each of the recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-870.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov or Keith A. Rhodes, (202) 512-6412, rhodesk@gao.gov.

What GAO Found

The systems supporting the US-VISIT program have significant information security control weaknesses that place sensitive and personally identifiable information at increased risk of unauthorized and possibly undetected disclosure and modification, misuse, and destruction. Weaknesses existed in all control areas and computing device types reviewed. Deficiencies in access controls and other system controls exposed mainframe computer, network infrastructure, servers, and workstations to insider and external threats. For example, CBP did not implement controls to effectively prevent, limit, and detect access to computer networks, systems, and information. To illustrate, it did not (1) adequately identify and authenticate users in systems supporting US-VISIT; (2) sufficiently limit access to US-VISIT information and information systems; (3) ensure that controls adequately protected external and internal network boundaries; (4) effectively implement physical security at several locations; (5) consistently encrypt sensitive data traversing the communication network; and (6) provide adequate logging or user accountability for the mainframe, workstations, or servers. In addition, CBP did not always ensure that responsibilities for systems development and system production were sufficiently segregated and did not consistently maintain secure configurations on the application servers and workstations at a key data center and ports of entry.

These weaknesses collectively increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information, including personally identifiable information, and disrupt the operations of the US-VISIT program. They make it possible for intruders, as well as government and contractor employees, to bypass or disable computer access controls and undertake a wide variety of inappropriate or malicious acts. These risks are not confined to US-VISIT information. The CBP mainframe and network resources that support US-VISIT also support other programs and systems. As a result, the vulnerabilities identified in this report could expose the information and information systems of the other programs to the same increased risks.

A key reason for these weaknesses is that, although CBP has made important progress in implementing elements of the department's information security program, it did not effectively or fully implement essential program activities. For example, CBP did not fully characterize the risks facing critical systems, update interconnection security agreements in security plans, sufficiently test and evaluate security controls, incorporate required elements in remedial action plans, adequately implement incident detection and handling procedures, and consistently address privacy issues. Until DHS and CBP act to mitigate the weaknesses in CBP systems supporting the US-VISIT program and CBP effectively and fully implements its information security program, limited assurance exists that the US-VISIT program will achieve its goal of enhancing the security of U.S. citizens and its visitors.