February 2006

ELECTRONIC GOVERNMENT

Agencies Face Challenges in Implementing New Federal Employee Identification Standard

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-178, a report to the Chairman, Committee on Government Reform, House of Representatives

Why GAO Did This Study

Many forms of identification (ID) that federal employees and contractors use to access government-controlled buildings and information systems can be easily forged, stolen, or altered to allow unauthorized access. In an effort to increase the quality and security of federal ID and credentialing practices, the President directed the establishment of a governmentwide standard—Federal Information Processing Standard (FIPS) 201—for secure and reliable forms of ID based on "smart cards" that use integrated circuit chips to store and process data with a variety of external systems across government. GAO was asked to determine (1) actions that selected federal agencies have taken to implement the new standard and (2) challenges that federal agencies are facing in implementing the standard.

What GAO Recommends

GAO recommends that the Director, OMB monitor FIPS 201 implementation progress by, for example, (1) establishing an agency reporting process to fulfill its role of ensuring FIPS 201 compliance and (2) amending or supplementing guidance to provide more complete direction to agencies on how to address implementation challenges. With the exception of OMB, which disagreed with GAO's second recommendation, agency officials generally agreed with the content of this report.

www.gao.gov/cgi-bin/getrpt?GAO-06-178.

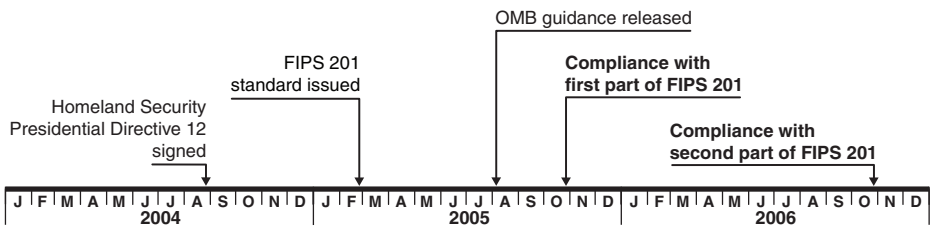
To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6249 or koontzl@gao.gov.

What GAO Found

The six agencies we reviewed—Defense, Interior, Homeland Security, Housing and Urban Development (HUD), Labor, and the National Aeronautics and Space Administration (NASA)—had each taken actions to begin implementing the FIPS 201 standard. Their primary focus has been on actions to address the first part of the standard, which calls for establishing appropriate identity proofing and card issuance policies and procedures and which the Office of Management and Budget (OMB) required agencies to implement by October 27, 2005. Agencies had completed a variety of actions, such as instituting policies to require that at least a successful fingerprint check be completed prior to issuing a credential. Regarding other requirements, however, efforts were still under way. For example, Defense and NASA reported that they were still modifying their background check policies. Based on OMB guidance, agencies have until October 27, 2006, to implement the second part of the standard, which requires them to implement interoperable smart-card based ID systems. Agencies have begun to take actions to address this part of the standard. For example, Defense and Interior conducted assessments of technological gaps between their existing systems and the infrastructure required by FIPS 201 but had not yet developed specific designs for card systems that meet FIPS 201 interoperability requirements.

The federal government faces significant challenges in implementing FIPS 201, including (1) testing and acquiring compliant commercial products—such as smart cards and card readers—within required time frames; (2) reconciling divergent implementation specifications; (3) assessing the risks associated with specific vendor implementations of the recently chosen biometric standard; (4) incomplete guidance regarding the applicability of FIPS 201 to facilities, people, and information systems; and (5) planning and budgeting with uncertain knowledge and the potential for substantial cost increases. Until these implementation challenges are addressed, the benefits of FIPS 201 may not be fully realized. Specifically, agencies may not be able to meet implementation deadlines established by OMB, and more importantly, true interoperability among federal government agencies' smart card programs—one of the major goals of FIPS 201—may not be achieved.

Time Line of FIPS 201-Related Activities



Source: GAO analysis of FIPS 201 guidance.