October 2008

DEFENSE MANAGEMENT

DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-49, a report to Congressional Committees

Why GAO Did This Study

The events of September 11, 2001, and operations in Afghanistan and Iraq have made it critical for military units to identify individuals they encounter and share this information with other units and federal agencies. Biometrics are unique personal aspects such as fingerprints and iris images used to identify an unfamiliar person. Federal agencies with national security missions, such as the Departments of Homeland Security (DHS) and State (DOS), need access to certain biometrics data gathered by the Department of Defense (DOD). GAO was asked to determine to what extent (1) DOD has guidance on the biometrics data to be collected to support military activities, and (2) there may be gaps in biometrics information shared between DOD and DHS. This is a public version of a For Official Use Only report, GAO-08-430NI, issued in May 2008. GAO examined DOD's guidance for field collection of biometrics data, biometrics sharing agreements, and information on national level efforts to enhance data sharing.

What GAO Recommends

GAO recommends that (1) DOD establish guidance specifying a standard set of biometrics data for collection during military operations in the field, and (2) the Secretaries of Defense and Homeland Security address, as appropriate, biometrics data sharing gaps, in accordance with U.S. and international law. DOD partially concurred with the first recommendation and concurred with the second recommendation.

To view the full product, including the scope and methodology, click on GAO-09-49.
For more information, contact Davi D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

What GAO Found

DOD has issued guidance on the biometrics data collected from individuals who are detained or allowed access to U.S. bases in Iraq, but has not issued guidance on data to be collected during field activities where U.S. forces encounter hostile or questionable individuals such as in Afghanistan and Iraq. DOD has allowed commanders to determine the type of data to collect, such as fingerprints or iris images, during their operations. GAO's analysis showed that allowing for this flexibility results in the collection of different data that are not necessarily comparable to each other. Some units may collect iris images while others collect fingerprints, which are not comparable data. Broader national security implications can arise, such as military personnel's inability to identify someone who has harmed or attempted to harm U.S. or coalition forces. These newly collected data are not necessarily comparable with data collected by other units or with federal databases that store biometrics data, such as the FBI's fingerprint database, DOD's biometric database, or the DHS biometric database. Having a standard set of data would help ensure consistent identification and confirmation of an individual's identity thus allowing forces to compare data across multiple databases in different commands. A standard set of data also would allow for comparison of new biometrics data collected in the field with existing biometrics data.

DOD shares biometrics data that it collects on non-U.S. persons with other federal agencies through a variety of inter-agency agreements, but some gaps in data sharing may remain. Since the events of September 11, 2001, the President and Congress have issued policies that require agencies to share counterterrorism information, and agencies have in turn issued their own policies. National efforts to develop policies about such information sharing are still in development. In January 2007, the Deputy Secretary of Defense issued a memo that stated that DOD would immediately adopt the practice of sharing, when asked, unclassified DOD biometrics data records with other U.S. agencies that have counterterrorism missions—this includes data related to terrorism information but excludes data pertaining to U.S. persons. According to a DHS memorandum, DHS is not regularly receiving updates on certain types of DOD biometrics data that it could use. DHS officials told GAO they could use such data in various ways, such as to prohibit individuals from entering the United States who are determined to be inadmissible based on these data and other relevant information. GAO found that DHS officials are consulting with DOD on how to obtain additional biometrics data from DOD. Until national level policies are developed, opportunities to reduce gaps in national security through comprehensive data sharing may be lost unless remaining needs for biometrics data are identified and filled as appropriate and in accordance with U.S. laws and regulations and international agreements.