November 14, 2007

INVESTIGATIVE OPERATIONS

Use of Covert Testing to Identify Security Vulnerabilities and Fraud, Waste, and Abuse

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-286T, a testimony before the Committee on Homeland Security, House of Representatives

Why GAO Did This Study

GAO's Forensic Audits and Special Investigations team (FSI), which was created in 2005 as an interdisciplinary team consisting of investigators, auditors, and analysts, conducts covert tests at the request of the Congress to identify vulnerabilities and internal control weaknesses at executive branch agencies. These vulnerabilities and internal control weaknesses include those that could compromise homeland security, affect public safety, or have a financial impact on taxpayer's dollars. FSI conducts covert tests as "red team" operations, meaning that FSI does not notify agencies in advance about the testing.

Recently, concerns have arisen as to whether top management at the U.S. Transportation Security Administration (TSA) were negatively impacting the results of red team operations by leaking information to security screeners at the nation's airports in advance of covert testing operations. Consequently, GAO was asked to (1) briefly explain FSI's processes and procedures concerning covert testing and (2) provide examples of covert activities performed.

To view the full product, including the scope and methodology, click on GAO-08-286T. For more information, contact Gregory D. Kutz at 512-6722 or kutzg@gao.gov.

What GAO Found

FSI has strict internal procedures related to the planning, execution, and reporting of covert activities. First, FSI and senior GAO management decide on a case-by-case basis whether engagements requiring covert tests are within the scope of GAO's authority. Next, FSI identifies the aspects of the security system or the government program that are particularly vulnerable to terrorist threats or fraudulent activities and relies on the experience of its investigators to develop a written investigative plan. This plan typically includes the creation of fictitious identities and counterfeit documentation. All counterfeit documents that FSI uses are manufactured using hardware, software, and materials that are available to the general public—this allows FSI to demonstrate that any security vulnerabilities it finds could be exploited by a criminal or terrorist with moderate means and resources and would not require sophisticated insider knowledge.

FSI's investigators are the only GAO staff allowed to participate in the execution phase of testing, although audit and analyst staff are often involved in planning and operational support. Importantly, if investigators discover vulnerabilities that pose a significant and immediate threat to public safety, FSI immediately will discontinue its investigation and alert the appropriate government law enforcement agency. Once the operation is complete, FSI conducts a "corrective action briefing" with officials at the tested entity to report that they have been the subject of a covert operation, share the results of the testing and, if necessary, suggest potential remedies for any identified control weaknesses or security vulnerabilities.

The following summarize recent FSI red team operations. These operations provided the Congress with irrefutable evidence about the actual ability of federal agencies under "live" conditions to deal with security threats and to protect government assets from fraudsters.

- Using counterfeit documents and posing as employees of a company with a Nuclear Regulatory Commission license, FSI investigators successfully crossed the U.S. northern and southern borders with the type of radioactive materials that could be used to make a dirty bomb.
- Posing as private citizens, FSI investigators purchased sensitive military equipment—including ceramic body armor inserts, guided missile radar test sets, and microcircuits used in F-14 fighter aircraft—on the Internet from the Department of Defense's liquidation sales contractor.
- Using bogus driver's licenses, FSI investigators successfully gained entry to all 24 Department of Transportation regulated urine collection sites that FSI tested, which are responsible for providing drug testing of commercial truck drivers in safety sensitive transportation positions.
- Using false documents and an erroneous IRS taxpayer identification number, FSI pretended to be a charity and successfully applied to three of the Combined Financial Campaign's local 2006 campaigns.