United States Government Accountability Office

GAO

Testimony

Before the Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, November 14, 2007

INVESTIGATIVE OPERATIONS

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

Statement of Gregory D. Kutz, Managing Director
Forensic Audits and Special Investigations

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.

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to discuss covert testing activities conducted by the Forensic Audits and Special Investigations (FSI) unit of the GAO. 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. The objectives of these tests are to identify security vulnerabilities and internal control weaknesses at executive branch agencies, including those that could compromise national or homeland security, affect public safety, or have a financial impact on taxpayer's dollars. In brief, my remarks today relate to the processes and procedures FSI uses to conduct this work and the results of some of our operations.

FSI's covert testing operations are typically part of a broader security vulnerability assessment or a forensic audit designed to identify fraud, waste, and abuse related to federal programs. FSI conducts covert tests as "red team" operations, meaning that for these operations, FSI does not notify agencies in advance about our testing. As an example, in 2002 we conducted a red team operation to evaluate the security of federal buildings in Atlanta, Georgia.[1] In this case, we obtained genuine security badges through deception and then counterfeited the badges, allowing several investigators to access the buildings without the knowledge of security personnel or agency officials. In contrast, "blue team" operations involve notifying affected agencies in advance about testing; GAO information technology specialists test executive branch agencies' computer systems using a blue team approach. Although both types of operations uncover valuable information, we are confident that the red team approach provides the Congress with dependable, irrefutable evidence about the actual ability of federal agencies under "live" conditions to deal with security threats and to protect government assets and programs from fraudsters.

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 notifying security screeners at the nation's airports in advance of covert testing operations. Consequently, you requested that we (1) briefly explain FSI's processes and procedures

[1]GAO, *Security Breaches at Federal Buildings in Atlanta, Georgia*, GAO-02-668T (Washington, D.C.: Apr. 30, 2002).

concerning covert testing and (2) provide examples of covert activities we performed and the results.

FSI Covert Testing Processes and Procedures

Because of the sensitive nature of our work, and the fact that our findings can generate information that may compromise national or homeland security, we apply strict processes and procedures when performing covert work. FSI plans and conducts all investigations in accordance with the standards established by the President's Council on Integrity and Efficiency (PCIE). These standards are relevant to the full range of government investigations, including fraud, corruption, white-collar crime, security inquiries, whistleblower issues, and other special investigations. With regard to covert operations specifically, FSI has developed our own internal procedures detailing the requirements related to the planning, execution, and reporting phases of the operations.

Planning a Covert Test

FSI, in conjunction with senior-level GAO management, decides on a case-by-case basis whether to accept written congressional requests requiring covert operations or whether to incorporate covert testing into existing engagements. In making these decisions, a number of factors are considered, including, but not limited to, whether the proposed operations are within the scope of GAO's authority; whether the operations may be performed more appropriately by agency Inspectors General; and whether the requested work presents significant risk of personal injury to individuals or other harm to persons, businesses, or public safety. We also identify the specific aspects of the security system or the government program that are particularly vulnerable to terrorist threats or fraudulent activities. Once the use of covert operations is accepted, the first step in FSI's process involves using the training and experience of our investigators to develop a written investigative plan. Because the average FSI investigator has over 20 years of law enforcement experience, they are uniquely positioned to develop a blueprint for performing the work, while minimizing disruption to the day-to-day operations of the agency being tested and seeking to ensure the safety of all involved.

In general, FSI investigative plans contain the following elements: a statement regarding the investigation's overall objectives; a description of the legal issues involved; and a summary of the allegations that merit investigation or the processes, systems, and controls that will be tested. When covert operations are involved, the plan must also contain a detailed outline of the steps that would be necessary to effectively conduct the operation. In most cases, this step-by-step process will include the

creation of fictitious identities and counterfeit documentation, including items such as birth certificates, driver's licenses, credit cards, billing records, and social security cards. All counterfeit documents that FSI uses are manufactured by FSI using hardware, software, and materials that are available to the general public—this allows us to demonstrate that any security vulnerabilities we find could be exploited by a criminal or terrorist with moderate means and resources and would not require sophisticated insider knowledge or access to sophisticated equipment. In order to obtain the best possible evidence, the plan may also request that GAO management authorize FSI to obtain photographs or video or audio recordings. The investigative plan must be reviewed and approved by an FSI Assistant Director for Investigations, FSI's Managing Director, and two members from GAO's top management team.

Executing a Covert Test

Once the investigative plan has been approved, FSI proceeds with the covert operation. In general, FSI's investigators are the only staff allowed to participate in actual testing activities, although audit and analyst staff are often involved in planning and operational support. Furthermore, if the covert testing is conducted outside GAO headquarters (e.g., the testing of U.S. border security), FSI policy requires that investigators acting in a covert capacity have a "cover team" of investigators to ensure safety. These agents are usually placed strategically about the test site to monitor the situation and to alert the investigators conducting the tests if anything seems out of place. The responsible Assistant Director for Investigations is also present during all covert operations conducted outside of the GAO headquarters building. Before any testing begins, the Managing Director generally receives an itinerary sheet with all the names of the investigators involved and pertinent contact numbers.

During the execution phase, investigators are required to protect investigative information from unauthorized disclosure, protect the rights of all individuals involved, and avoid any action that may give the appearance of coercion or intimidation. In addition, investigators must safeguard any counterfeit documentation against theft or damage. Investigators must document all evidence obtained in accordance with PCIE standards and applicable FSI and GAO policies.

Investigators routinely make dry runs of covert operations tests to determine whether new or enhanced security procedures have been implemented after the development of our testing plan. Because FSI only uses publicly available information to develop our covert tests and does not consult with agency insiders, the specifics of our operations are not

leaked to agency officials. Our belief is that by using only publicly available information, our tests reveal what an actual terrorist or criminal might do during a real security breach or fraud scheme.

Furthermore, our policy is that if an FSI covert operation is uncovered during one of our tests, the backup investigators immediately will identify themselves and alert the proper law enforcement authorities that a test is being conducted and identify all participants as being FSI investigators with the proper authority. Importantly, if investigators discover vulnerabilities that pose a significant and immediate threat to public safety, FSI immediately discontinues its investigation and alert the appropriate government law enforcement agency. Under no circumstances will FSI make publicly available any photograph, videotape, or audiotape that could be used as a road map by criminals or terrorist groups.

Reporting the Results of Covert Testing

Once the operation is complete, investigators immediately brief the congressional requester. Next, FSI conducts a "corrective action briefing" with officials at the tested entity to inform them 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.

After all parties have been briefed, FSI will issue a report or testimony that comports with PCIE and applicable FSI and GAO standards. Because the covert testing is sometimes part of a broader forensic audit, parts of the product may also adhere to U.S. generally accepted government auditing standards. These products contain our findings, the results of the corrective action briefing with the tested entity, and sometimes contain recommendations to agency management. FSI does not usually reveal all details about its covert methodologies in public products. For example, we typically do not reveal the name of any bogus companies that we create or the fictitious identities that we use. Moreover, if our findings relate to issues of national or homeland security, FSI submits a draft product to the agency for a sensitivity review prior to issuance. In some cases, FSI products are issued in conjunction with letters to the tested entity or other law enforcement agencies referring specific instances of wrongdoing, including the criminal activities of agency officials or private citizens.

Examples of FSI Covert Testing

At the request of a number of different congressional committees and subcommittees, FSI has conducted a wide variety of covert testing activities, including evaluations of controls over radioactive materials and security at America's borders, airport security, sales of sensitive and surplus military equipment, public safety, and other issues including fraud prevention controls over federal programs. As demonstrated by the examples below, covert activities are instrumental in identifying important weaknesses that expose the federal government—and most importantly, the American public—to threats to their security and safety, as well as fraud, waste, and abuse related to taxpayer dollars. Following are summaries of several covert activities we performed in recent engagements and the results we obtained.

Controls over Radioactive Materials and Security at America's Borders

The covert activities we performed in these areas include:

- Using the name of a bogus business that existed only on paper, FSI investigators obtained a genuine radioactive materials license from the Nuclear Regulatory Commission (NRC) without leaving the office or actually meeting with or having our nonexistent facility inspected by anybody from the NRC.[2] After altering the maximum quantity of materials listed on the license, FSI investigators faxed these licenses to two suppliers and obtained price quotes and commitments to ship machines containing radioactive materials in quantities that could have been used to produce a dirty bomb. In contrast, a state allowed by the NRC to issue radioactive licenses indicated that it would perform physical verification prior to approving a radioactive materials license for our bogus company. As a result, we informed NRC that we had "financial problems" and withdrew our application.

- Using counterfeit documents and posing as employees of a company with an NRC license, FSI investigators successfully crossed the northern and southern borders with the type of radioactive materials that could be used to make a dirty bomb.[3] While the radiation portal monitors at the two border locations properly signaled the presence of the radioactive materials in our vehicles, the inspectors readily

[2]GAO, *Nuclear Security: Actions Taken by NRC to Strengthen Its Licensing Process for Sealed Radioactive Sources Are Not Effective*, GAO-07-1038T (Washington D.C.: July 12, 2007).

[3]GAO, *Border Security: Inspectors Transported Radioactive Sources across Our Nation's Borders at Two Locations*, GAO-06-583T (Washington, D.C.: Mar. 28, 2006).

accepted our counterfeit documents—including a counterfeit bill of lading and NRC license—which we created using publicly available hardware, software, and materials. As part of this operation, an FSI investigator using the name of a fictitious company ordered by telephone a small amount of radioactive sources to "calibrate personal radiation detection pagers." These radioactive sources were shipped to the Washington, D.C., area to the fictitious company. This test demonstrated that anyone could purchase small quantities of radioactive sources for stockpiling.

- Posing as individuals with simulated contraband including radioactive material, FSI investigators successfully crossed the northern U.S. border at locations that were unmanned and unmonitored.[4] This test showed that the northern border is significantly vulnerable to terrorists or criminals entering the United States undetected.

Airport Security Testing

- In 2006, we reported on the results of covert security vulnerability testing of numerous airports across the country. During these covert tests, our investigators passed through airport security checkpoints carrying prohibited explosive components without being caught by Transportation Security Administration (TSA) security officers. The details of this March 2006 report are classified; however, TSA has authorized this limited discussion.

Sale of Sensitive and Surplus Military Equipment

- 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 (DOD) liquidation sales contractor.[5] Some of these items required us to obtain an "end use certificate", which is intended to provide assurance that sensitive property is sold to legitimate buyers. To obtain these parts we applied for this certificate using fictitious individuals and bogus documents. Subsequently, a DOD official called our investigator (the fictitious individual) asking why he had no credit or other history. Our investigator used social engineering and a copy of a bogus utility bill to

[4]GAO, *Border Security: Security Vulnerabilities at Unmanned and Unmonitored U.S. Border Locations*, GAO-07-884T (Washington, D.C.: Sept. 27, 2007).

[5]GAO, *DOD Excess Property: Control Breakdowns Present Significant Security Risks and Continuing Waste and Inefficiency*, GAO-06-981T (Washington, D.C.: July 25, 2006).

address the questions and our application was then approved. We used this certificate to buy items, including F-14 parts, which are in demand by Iran, the only country currently operating F-14 fleet in the world.

- FSI investigators posing as DOD contractor employees were able to easily penetrate two Department of Defense excess property warehouses. There, they were able to obtain about $1.1 million in sensitive military equipment items, including launcher mounts for shoulder-fired guided missiles, body armor, a digital signal converter used in naval surveillance, and an all-band antenna used to track aircraft. Our cover story was so convincing that DOD and its contractor staff helped our investigators locate targeted items and load them into our rented van.

Public Safety

- Using bogus driver's licenses, FSI investigators successfully gained entry to all 24 Department of Transportation regulated urine collection sites that we tested, which are responsible for providing drug testing of commercial truck drivers in safety sensitive transportation positions.[6] This test shows that individuals required to undergo drug testing can send someone to take a drug test in their place using fake identification. Furthermore, FSI investigators were able to use adulterants at four collection sites and substitute synthetic urine at another four sites without being caught by site collectors. None of the eight synthetic or adulterated urine specimens were detected by the labs.

Other Testing

Activities in this area include obtaining disaster assistance and demonstrating weaknesses in agencies' fraud prevention controls.

- Posing as disaster victims of hurricanes Katrina and Rita, FSI investigators applied for federal assistance using falsified identities, bogus addresses, and fabricated disaster stories to register for assistance under the Individuals and Households Program.[7] Despite the fact that our applications over the Internet were not accepted because

[6]GAO, *Drug Testing: Undercover Tests Reveal Significant Vulnerabilities in DOT's Drug Testing Program*, GAO-08-225T (Washington, D.C.: Nov. 1, 2007).

[7]GAO, *Expedited Assistance for Victims of Hurricanes Katrina and Rita: FEMA's Control Weaknesses Exposed the Government to Significant Fraud and Abuse*, GAO-06-403T (Washington, D.C.: Feb. 13, 2006).

of data validation procedures the Federal Emergency Management Agency (FEMA) had implemented, FSI investigators successfully registered over the phone. As a result, FEMA sent a number of checks to FSI for our fictitious individuals based on our bogus applications. After our investigation was complete, we returned the checks we obtained.

- Using easily obtained data on the Internet, FSI submitted a fictitious travel order for a fictitious individual to a DOD commercial travel office to obtain an airline ticket from Washington, D.C., to Atlanta, Georgia.[8] DOD issued FSI the airline ticket, established an obligation, and paid for the ticket without detecting the fictitious nature of the request. On the day of the scheduled flight, an FSI investigator went to the airline's ticket counter at the airport and, under the name of this fictitious individual, picked up a boarding pass.

- Using entirely false documents and an erroneous IRS taxpayer identification number, FSI pretended to be a charity and applied to three of the Combined Financial Campaign's local 2006 campaigns.[9] The fictitious entity was accepted into all three CFC campaigns. Immediately after our applications were accepted, we notified CFC officials and withdrew our charity from the campaigns in order to prevent federal employees from making donations to our fictitious charity.

Conclusions

The results of FSI's covert testing have been used by Congress and federal agency managers across the government to help strengthen homeland security and minimize fraud, waste, and abuse of taxpayer dollars. We will continue to offer this valuable service to the Congress in a responsible and professional manner and provide the results of our work to agency management, where appropriate, so that they can take concrete steps to improve the federal government's operations.

[8]GAO, *DOD Travel Cards: Control Weaknesses Led to Millions in Fraud, Waste, and Improper Payments*, GAO-04-825T (Washington, D.C.: June 9, 2004).

[9]GAO, *Tax Debt: Some Combined Federal Campaign Charities Owe Payroll and Other Federal Taxes*, GAO-06-755T (Washington, D.C.: May 25, 2006).

Mr. Chairman and Members of the Committee, this concludes my statement. I would be pleased to answer any questions that you or other Members of the Committee may have at this time.

Contacts and Acknowledgments

For further information about this testimony, please contact Gregory D. Kutz at (202) 512-6722 or kutzg@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this testimony.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, jarmong@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548