United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the House Committee on Homeland Security

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, July 24, 2012

FEDERAL PROTECTIVE SERVICE

Preliminary Results on Efforts to Assess Facility Risks and Oversee Contract Guards

Statement of Mark L. Goldstein, Director
Physical Infrastructure Issues

GAO
Accountability * Integrity * Reliability

G A O
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-12-943T, testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the House Committee on Homeland Security

July 24, 2012

FEDERAL PROTECTIVE SERVICE

Preliminary Results on Efforts to Assess Facility Risks and Oversee Contract Guards

Why GAO Did This Study

FPS provides security and law enforcement services to over 9,000 federal facilities managed by the General Services Administration (GSA). GAO has reported that FPS faces challenges providing security services, particularly completing FSAs and managing its contract guard program. To address these challenges, FPS spent about $35 million and 4 years developing RAMP—essentially a risk assessment and guard oversight tool. However, RAMP ultimately could not be used to do either because of system problems.

This testimony is based on preliminary work for the Chairman and discusses the extent to which FPS is (1) completing risk assessments, (2) developing a tool to complete FSAs, and (3) managing its contract guard workforce. GAO reviewed FPS documents, conducted site visits at 3 of FPS's 11 regions and interviewed officials from FPS, Argonne National Laboratory, GSA, Department of Veterans Affairs, the Federal Highway Administration, Immigration and Customs Enforcement, and guard companies; as well as 4 risk management experts.

What GAO Recommends

GAO is not making any recommendations in this testimony. GAO plans to finalize its analysis and report to the Chairman in August 2012, including recommendations. GAO discussed the information in this statement with FPS and incorporated technical comments as appropriate.

View GAO-12-943T. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov

What GAO Found

GAO's preliminary results indicate that the Department of Homeland Security's (DHS) Federal Protective Service (FPS) is not assessing risks at federal facilities in a manner consistent with standards such as the National Infrastructure Protection Plan's (NIPP) risk management framework, as FPS originally planned. Instead of conducting risk assessments, since September 2011, FPS's inspectors have collected information, such as the location, purpose, agency contacts, and current countermeasures (e.g., perimeter security, access controls, and closed-circuit television systems). This information notwithstanding, FPS has a backlog of federal facilities that have not been assessed for several years. According to FPS's data, more than 5,000 facilities were to be assessed in fiscal years 2010 through 2012. However, GAO was not able to determine the extent of FPS's facility security assessment (FSA) backlog because the data were unreliable. Multiple agencies have expended resources to conduct risk assessments, even though they also already pay FPS for this service.

FPS has an interim vulnerability assessment tool, referred to as the Modified Infrastructure Survey Tool (MIST), which it plans to use to assess federal facilities until it develops a longer-term solution. In developing MIST, FPS generally followed GAO's project management best practices, such as conducting user acceptance testing. However, our preliminary analysis indicates that MIST has some limitations. Most notably, MIST does not estimate the consequences of an undesirable event occurring at a facility. Three of the four risk assessment experts GAO spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess risks. FPS officials stated that they did not include consequence information in MIST because it was not part of the original design and thus requires more time to validate. MIST also was not designed to compare risks across federal facilities. Thus, FPS has limited assurance that critical risks at federal facilities are being prioritized and mitigated.

GAO's preliminary work indicates that FPS continues to face challenges in overseeing its approximately 12,500 contract guards. FPS developed the Risk Assessment and Management Program (RAMP) to help it oversee its contract guard workforce by verifying that guards are trained and certified and for conducting guard post inspections. However, FPS faced challenges using RAMP for guard oversight, such as verifying guard training and certification information, and has recently determined that it would no longer use RAMP. Without a comprehensive system, it is more difficult for FPS to oversee its contract guard workforce. FPS is verifying guard certification and training information by conducting monthly audits of guard information maintained by guard contractors. However, FPS does not independently verify the contractor's information. Additionally, according to FPS officials, FPS recently decided to deploy a new interim method to record post inspections that replaces RAMP.

Chairman Lungren, Ranking Member Clarke, and Members of the Subcommittee:

We are pleased to be here today to discuss the Department of Homeland Security's (DHS) Federal Protective Service's (FPS) efforts to complete risk assessments of the over 9,000 federal facilities under the custody and control of the General Services Administration (GSA) and oversee its contract guards in the absence of its Risk Assessment and Management Program (RAMP), a Web-enabled facility security assessment (FSA) and guard management system. As we reported in July 2011, FPS had spent about $35 million and taken almost 4 years to develop RAMP—$14 million and 2 years more than planned—but still could not use RAMP to complete FSAs because of several factors, including that FPS did not verify the accuracy of the federal facility data used.[1] As a result, FPS's Director decided to stop using RAMP to conduct FSAs and instead pursue an interim tool to replace it. FPS also experienced difficulty using RAMP to ensure that its guards met training and certification requirements, primarily because of challenges in verifying guards' data.[2] In June 2012, FPS also decided to stop using RAMP to help oversee its contract guard program.

For fiscal year 2012, FPS has a budget of $1.3 billion, with over 1,200 full-time employees and about 12,500 contract security guards, to achieve its mission to protect federal facilities. As part of the FSA process, FPS generally attempts to gather and review facility information; conduct and record interviews with tenant agencies; assess threats, vulnerabilities, and consequences to facilities, employees, and the public; and recommend countermeasures to federal tenant agencies. FPS's contract guards are responsible for controlling access to federal facilities, screening access areas to prevent the introduction of weapons and explosives, enforcing property rules and regulations, detecting and reporting criminal acts, and responding to emergency situations involving

[1] GAO, *Federal Protective Service: Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS's Risk Assessment and Management Program*, GAO-11-705R (Washington, D.C.: July 15, 2011).

[2] GAO-11-705R.

facility safety and security. FPS relies on the fees it charges federal tenant agencies in GSA–controlled facilities to fund its security services.[3]

This testimony is based on preliminary results of work we conducted for a report that we plan to issue to the Chairman in August 2012. That report will contain our final evaluation and recommendations. Consistent with the report's objectives, this statement addresses the extent to which FPS is (1) completing risk assessments, (2) developing a tool to complete FSAs, and (3) managing its contract guard workforce. To examine the extent to which FPS is completing risk assessments and overseeing guards without RAMP, we reviewed, among other things, FPS's current FSA procedures and data on completed and planned FSAs for fiscal years 2010 to 2012. Specifically, we reviewed FPS's FSA data aggregated from its 11 regions to determine the extent of its FSA backlog. However, we could not determine the extent of the backlog because FPS's data contained a number of missing and incorrect values which made the data unreliable. We also visited 3 of FPS's 11 regions and interviewed internal and external stakeholders including, among others, FPS, GSA, Department of Veterans Affairs, the Federal Highway Administration, Immigration and Customs Enforcement, and guard companies. We selected these 3 regions based on the number of federal facilities in the region and their security levels, the number of contract guards in the region, and geographic dispersion. Our work is not generalizable to all FPS regions. To determine the status of FPS's efforts to develop an FSA tool, we reviewed, among other things, relevant project documents and federal physical security standards, such as DHS's National Infrastructure Protection Plan's (NIPP) risk management framework. We also interviewed FPS officials, representatives from Argonne National Laboratory, and four risk management experts. We selected our four risk assessment experts from a list of individuals who participated in the Comptroller General's 2007 risk management forum.[4] This work is being conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit

[3] 40 U.S.C. § 586; 41 C.F.R. § 102-85.35; Pub. L. No. 111-83, 123 Stat. 2142, 2156-57 (2009).

[4] GAO, *Highlights of a Forum: Strengthening the Use of Risk Management Principles in Homeland Security*, GAO-08-627SP (Washington, D.C.: April 2008).

objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FPS Does Not Currently Assess Risks at Federal Facilities but Multiple Agencies Are Conducting Their Own Assessments

Our preliminary results indicate that, in the absence of RAMP, FPS currently is not assessing risk at the over 9,000 federal facilities under the custody and control of GSA in a manner consistent with federal standards such as NIPP's risk management framework, as FPS originally planned. According to this framework, to be considered credible a risk assessment must specifically address the three components of risk: threat, vulnerability, and consequence. As a result, FPS has accumulated a backlog of federal facilities that have not been assessed for several years. According to FPS data, more than 5,000 facilities were to be assessed in fiscal years 2010 through 2012. However, we were not able to determine the extent of the FSA backlog because we found FPS's FSA data to be unreliable. Specifically, our analysis of FPS's December 2011 assessment data showed nearly 800 (9 percent) of the approximately 9,000 federal facilities did not have a date for when the last FSA was completed. We have reported that timely and comprehensive risk assessments play a critical role in protecting federal facilities by helping decision makers identify and evaluate potential threats so that countermeasures can be implemented to help prevent or mitigate the facilities' vulnerabilities.[5]

Although FPS is not currently assessing risk at federal facilities, FPS officials stated that the agency is taking steps to ensure federal facilities are safe. According to FPS officials, its inspectors (also referred to as law enforcement security officers) monitor the security posture of federal facilities by responding to incidents, testing countermeasures, and conducting guard post inspections. In addition, since September 2011, FPS's inspectors have collected information—such as location, purpose, agency contacts, and current countermeasures (e.g., perimeter security, access controls, and closed-circuit television systems) at over 1,400 facilities—which will be used as a starting point to complete FPS's fiscal year 2012 assessments. However, FPS officials acknowledged that this approach is not consistent with NIPP's risk management framework. Moreover, several FPS inspectors told us that they received minimal training or guidance on how to collect this information, and expressed

[5] GAO, *Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection*, GAO-10-142 (Washington, D.C.: Oct. 23, 2009).

concern that the facility information collected could become outdated by the time it is used to complete an FSA.

Multiple Federal Agencies Are Conducting Their Own Risk Assessments

We reported in February 2012 that multiple federal agencies have been expending additional resources to conduct their own risk assessments, in part because they have not been satisfied with FPS's past assessments.[6] These assessments are taking place even though, according to FPS's Chief Financial Officer, FPS received $236 million in basic security fees from federal agencies to conduct FSAs and other security services in fiscal year 2011.[7] For example, officials we spoke with at the Internal Revenue Service, Federal Emergency Management Agency, Environmental Protection Agency and the U.S. Army Corps of Engineers stated that they conduct their own risk assessments. GSA is also expending additional resources to assess risk. We reported in October 2010 that GSA officials did not always receive timely FPS risk assessments for facilities GSA considered leasing.[8] GSA seeks to have these assessments completed before it takes possession of a property and leases it to tenant agencies. However, our preliminary work indicates that as of June 2012, FPS has not coordinated with GSA and other federal agencies to reduce or prevent duplication of its assessments.

FPS Efforts to Develop a Risk Assessment Tool Are Evolving, but Challenges Remain

In September 2011, FPS signed an interagency agreement with Argonne National Laboratory for about $875,000 to develop an interim tool for conducting vulnerability assessments by June 30, 2012.[9] According to FPS officials, on March 30, 2012, Argonne National Laboratory delivered this tool, called the Modified Infrastructure Survey Tool (MIST), to FPS on time and within budget. MIST is an interim vulnerability assessment tool that FPS plans to use until it can develop a permanent solution to replace

[6] GAO, *2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings and Enhance Revenue*, GAO-12-342SP (Washington, D.C.: February 2012).

[7] FPS currently charges tenant agencies in properties under GSA control a basic security fee of $0.74 per square foot per year for its security services including physical security and law enforcement activities as per 41 C.F.R. § 102-85.35.

[8] GAO-10-142.

[9] As of March 2012, FPS's total life cycle cost for MIST was estimated at $5 million.

RAMP. According to MIST project documents and FPS officials, among other things, MIST will:

- allow FPS's inspectors to review and document a facility's security posture, current level of protection, and recommend countermeasures;

- provide FPS's inspectors with a standardized way for gathering and recording facility data; and

- allow FPS to compare a facility's existing countermeasures against the Interagency Security Committee's (ISC) countermeasure standards based on the ISC's predefined threats to federal facilities (e.g., blast-resistant windows for a facility designed to counter the threat of an explosive device) to create the facility's vulnerability report.[10]

According to FPS officials, MIST will provide several potential improvements over FPS's prior assessment tools, such as using a standard way of collecting facility information and allowing edits to GSA's facility data when FPS inspectors find it is inaccurate. In addition, according to FPS officials, after completing a MIST vulnerability assessment, inspectors will use additional threat information gathered outside of MIST by FPS's Threat Management Division as well as local crime statistics to identify any additional threats and generate a threat assessment report. FPS plans to provide the facility's threat and vulnerability reports along with any countermeasure recommendations to the federal tenant agencies.

In May 2012, FPS began training inspectors on MIST and how to use the threat information obtained outside MIST and expects to complete the training by the end of September 2012. According to FPS officials,

[10] The ISC is comprised of representatives from more than 50 federal agencies and departments, establishes standards and best practices for federal security professionals responsible for protecting non-military federal facilities in the U.S. FPS is a member agency of the Interagency Security Committee in the Department of Homeland Security, along with other federal agencies such as the General Services Administration, the Federal Aviation Administration, the Environmental Protection Agency, and other components within the Department of Homeland Security. The ISC has defined 31 different threats to federal facilities including vehicle-borne improvised explosive devices, workplace violence, and theft.

inspectors will be able to use MIST once they have completed training and a supervisor has determined, based on professional judgment, that the inspector is capable of using MIST. At that time, an inspector will be able to use MIST to assess level I or II facilities.[11] According to FPS officials, once these assessments are approved, FPS will subsequently determine which level III and IV facilities the inspector may assess with MIST.

FPS Increased Its Use of Project Management Best Practices in Developing MIST

Our preliminary analysis indicates that in developing MIST, FPS increased its use of GAO's project management best practices, including alternatives analysis, managing requirements, and conducting user acceptance testing.[12] For example, FPS completed, although it did not document, an alternatives analysis prior to selecting MIST as an interim tool to replace RAMP. It appears that FPS also better managed MIST's requirements. Specifically, FPS's Director required that MIST be an FSA-exclusive tool and thus helped avoid changes in requirements that could have resulted in cost or schedule increases during development. In March 2012, FPS completed user acceptance testing of MIST with some inspectors and supervisors, as we recommended in 2011.[13] According to FPS officials, user feedback on MIST was positive from the user acceptance test, and MIST produced the necessary output for FPS's FSA process. However, FPS did not obtain GSA or federal tenant agencies' input in developing MIST's requirements. Without this input, FPS's customers may not receive the information they need to make well-informed countermeasure decisions.

[11] FPS uses the ISC's *Facility Security Level Determination for Federal Facilities* to determine the facility security level (FSL). The ISC recommends that level I and II facilities be assessed every 5 years and level III and IV facilities every 3 years. According to the ISC's criteria, a level I facility may be 10,000 or fewer square feet, have fewer than 100 employees, provide administrative or direct service activities, and have little to no public contact; a level II facility may be 100,000 or fewer square feet, have 250 or fewer employees, be readily identifiable as a federal facility, and provide district or state-wide services; a level III facility may be 250,000 or fewer square feet, have 750 or fewer employees, be an agency's headquarters, and be located in an area of moderate crime; and a level IV facility may exceed 250,000 square feet, have more than 750 employees, house national leadership, and be located in or near a popular tourist destination.

[12] GAO-11-705R.

[13] GAO-11-705R.

MIST Has Limitations as an Assessment Tool

FPS has yet to decide what tool, if any, will replace MIST, which is intended to be an interim vulnerability assessment tool. According to FPS officials, the agency plans to use MIST for at least the next 18 months. Consequently, until FPS decides what tool, if any, will replace MIST and RAMP, it will still not be able to assess risk at federal facilities in a manner consistent with NIPP, as we previously mentioned. Our preliminary work suggests that MIST has several limitations:

- *Assessing Consequence.* FPS did not design MIST to estimate consequence, a critical component of a risk assessment. Assessing consequence is important because it combines vulnerability and threat information to evaluate the potential effects of an adverse event on a federal facility. Three of the four risk assessment experts we spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess the risks to a federal facility. However, FPS officials stated that incorporating consequence information into an assessment tool is a complex task. FPS officials stated that they did not include consequence assessment in MIST's design because it would have required additional time to develop, validate, and test MIST. As a result, while FPS may be able to identify a facility's vulnerabilities to different threats using MIST, without consequence information, federal tenant agencies may not be able to make fully informed decisions about how to allocate resources to best protect federal facilities. FPS officials do not know if this capability can be developed in the future, but they said that they are working with the ISC and DHS's Science and Technology Directorate to explore the possibility.

- *Comparing Risk across Federal Facilities.* FPS did not design MIST to present comparisons of risk assessment results across federal facilities. Consequently, FPS cannot take a comprehensive approach to managing risk across its portfolio of 9,000 facilities to prioritize recommended countermeasures to federal tenant agencies. Instead, FPS takes a facility by facility approach to risk management where all facilities with the same security level are assumed to have the same security risk, regardless of their location.[14] We reported in 2010 that FPS's approach to risk management provides limited assurance that the most critical risks at federal facilities across the country are being

[14] GAO-10-142.

prioritized and mitigated.[15] FPS recognized the importance of having such a comprehensive approach to its FSA program when it developed RAMP and FPS officials stated that they may develop this capability for the next version of MIST.

- *Measuring Performance.* FPS has not developed metrics to measure MIST's performance, such as feedback surveys from tenant agencies. Measuring performance allows organizations to track progress toward their goals and, gives managers critical information on which to base decisions for improving their programs. This is a necessary component of effective management, and should provide agency managers with timely, action-oriented information.[16] Without such metrics, FPS's ability to improve MIST will be hampered. FPS officials stated that they are planning to develop performance measures for MIST, but did not give a time frame for when they will do so.

FPS Faces Challenges in Overseeing Its Contract Guards

Our work to date indicates that FPS does not have a comprehensive and reliable system to oversee its approximately 12,500 contract guards. In addition to conducting FSAs, FPS developed RAMP as a comprehensive system to help oversee two aspects of its contract guard program: (1) verifying that guards are trained and certified to be on post in federal facilities; and (2) conducting and documenting guard post inspections.[17] However, FPS experienced difficulty with RAMP because the contract guard training and certification information in RAMP was not reliable. Additionally, FPS faced challenges using RAMP to conduct and document post inspections.[18] For example, FPS inspectors we interviewed reported they had difficulty connecting to RAMP's servers in remote areas and that recorded post inspections disappeared from RAMP's database without explanation. Although we reported some of

[15] GAO, *Homeland Security: Addressing Weaknesses with Facility Security Committees Would Enhance Protection of Federal Facilities,* GAO-10-901 (Washington, D.C.: August 5, 2010).

[16] GAO, *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper its Ability to Protect Federal Facilities,* GAO-08-683 (Washington, D.C.: June 11, 2008).

[17] A post is a guard's area of responsibility in a federal facility.

[18] FPS's inspection requirement for level I and II facilities is two annual inspections of all posts, all shifts. The inspection requirement for level III facilities is biweekly inspections of two posts, any shift, and for level IV, weekly inspections of two posts, any shift.

these challenges in 2011, FPS did not stop using RAMP for guard oversight until June 2012 when the RAMP operations and maintenance contract was due to expire.

In the absence of RAMP, in June 2012, FPS decided to deploy an interim method to enable inspectors to record post inspections. FPS officials said this capability is separate from MIST, will not allow FPS to generate post inspection reports, and does not include a way for FPS inspectors to check guard training and certification data during a post inspection. FPS officials acknowledged that this method is not a comprehensive system for guard oversight. Consequently, it is now more difficult for FPS to verify that guards on post are trained and certified and that inspectors are conducting guard post inspections as required.

Although FPS collects guard training and certification information from the companies that provide contract guards, it appears that FPS does not independently verify that information. FPS currently requires its guard contractors to maintain their own files containing guard training and certification information and began requiring them to submit a monthly report with this information to FPS's regions in July 2011.[19] To verify the guard companies' reports, FPS conducts monthly audits. As part of its monthly audit process, FPS's regional staff visits the contractor's office to select 10 percent of the contractor's guard files and check them against the reports guard companies send FPS each month. In addition, in October 2011, FPS undertook a month-long audit of every guard file to verify that guards had up-to-date training and certification information for its 110 contracts across its 11 regions. FPS provided preliminary October 2011 data showing that 1,152 (9 percent) of the 12,274 guard files FPS reviewed at that time were deficient, meaning that they were missing one or more of the required certification document(s). However, FPS does not have a final report on the results of the nation-wide audit that includes an explanation of why the files were deficient and whether deficiencies were resolved.

FPS's monthly audits of contractor data provide limited assurance that qualified guards are standing post, as FPS is verifying that the contractor-provided information matches the information in the contractor's files. We

[19] For example, guard training and certifications include firearms qualification, cardiopulmonary resuscitation, first aid, baton certification, and x-ray and magnetometer training.

reported in 2010 that FPS's reliance on contractors to self-report guard training and certification information without a reliable tracking system of its own may have contributed to a situation in which a contractor allegedly falsified training information for its guards.[20] In addition, officials at one FPS region told us they maintain a list of the files that have been audited previously to avoid reviewing the same files, but FPS has no way of ensuring that the same guard files are not repeatedly reviewed during the monthly audits, while others are never reviewed. In the place of RAMP, FPS plans to continue using its administrative audit process and the monthly contractor-provided information to verify that qualified contract guards are standing post in federal facilities.

We plan to finalize our analysis and report to the Chairman in August 2012, including recommendations. We discussed the information in this statement with FPS and incorporated technical comments as appropriate. Chairman Lungren, Ranking Member Clarke, and members of the Subcommittee, this completes my prepared statement. I would be happy to respond to any questions you may have at this time.

GAO Contact and Staff Acknowledgments

For further information on this testimony, please contact me at (202) 512-2834, or by e-mail at goldsteinm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony include Tammy Conquest, Assistant Director; Geoffrey Hamilton; Greg Hanna; Justin Reed; and Amy Rosewarne.

[20] GAO, *Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards*, GAO-10-341 (Washington, D.C.: April 13, 2010).

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 website (www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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