GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 22, 2006

The Honorable Christopher Shays
Chairman
Subcommittee on National Security, Emerging Threats and International Relations
Committee on Government Reform
House of Representatives

Subject: *Military Operations: Background Screenings of Contractor Employees Supporting Deployed Forces May Lack Critical Information, but U.S. Forces Take Steps to Mitigate the Risk Contractors May Pose.*

Dear Mr. Chairman:

Force protection has long been a challenge for Department of Defense (DOD) in the Middle East and elsewhere. Since the 1996 Khobar Tower attack in Saudi Arabia, which killed 19 U.S. servicemembers, DOD and the U.S. Central Command (CENTCOM) have issued policies and procedures to help commanders, who are responsible for the safety and security of their installations, reduce the risk of terrorist attack and mitigate those risks that cannot be eliminated. However, DOD recognizes that all risks cannot be eliminated and terrorist attacks will still occur. To help installation commanders address force protection challenges, DOD, CENTCOM, and others, such as the Multi-national Forces- Iraq (MNF-I), provide guidance and assistance to installation commanders. For example DOD and CENTCOM have developed force protection standards that apply to installations in CENTCOM's area of responsibility, including Iraq and Afghanistan. These standards describe specific actions commanders should take to help prevent terrorist attacks. MNF-I has issued guidance to its subordinate commands directing among other things, the development of anti-terrorism plans, which include specific physical security measures. In addition, the Joint Staff periodically visits installations in Iraq and elsewhere to complete antiterrorism vulnerability assessments. The expert teams assess an installation for potential areas of attack and suggest actions the installation commander can take to reduce risks. Commanders are also provided with threat assessments which are updated as necessary, and routinely receive intelligence information, which could affect the security of their installations and forces.

The U.S. military has long relied on contractors to provide a variety of goods and services to U.S. forces around the world, including those located in Iraq and Afghanistan. These services range from maintaining advanced weapon systems and setting up and operating communications networks to providing gate and perimeter

security, interpreting foreign languages, preparing meals and doing laundry for the troops. DOD uses contractors for a variety of reasons, including a lack of skilled and qualified military personnel and the need to conserve scarce skills to ensure that they will be available for future deployments. DOD estimates that it has more than 50,000 contractor employees in support of operations in Afghanistan and Iraq.[1] Depending on the types of services being provided contractor employees may be U.S. citizens or third country nationals from countries such as the United Kingdom, the Philippines, Bangladesh, India, or Pakistan.[2] In addition, contractors are often encouraged to hire host country nationals from, for example, Iraq to help rebuild local economies and get local nationals back to work.

While contractor employees can provide significant benefits to U.S. forces, contractor employees can also pose a risk to U.S. troops. For example, the terrorists who attacked the U.S.S. Cole were suspected to be contractor employees associated with its refueling operations. This attack led military officials to realize the risk that contractors could pose to the safety and security of U.S. installations and military personnel. The risk is increased when U.S. forces are involved in a military operation against an insurgency, as they are in Iraq. Military officials we spoke with from three units who served in Iraq told us that they believed they observed contractor employees pacing off military facilities in an attempt to provide information on the location of critical facilities to hostile forces operating outside of installations. Force protection officials from another unit told us that they found a contractor employee with sensitive information that could aid hostile forces. Additionally, contractor employees have been responsible for additional illegal activities, including acts of theft and black market activities.

Background screenings of contractor employees can provide some insight into the likelihood that the employee may cause harm to U.S. troops and may deter some criminals and terrorists from working at U.S. installations. Although DOD is not required to screen contractor employees, in some situations, such as in Iraq, DOD is using biometrics to screen contractor employees for past criminal activity and security threats.[3] Contractors that screen their employees generally do not use biometrics and depend on public records and commercial databases to screen potential employees.

You asked that we review the process used to screen contractor employees who support U.S. deployed forces. Our objective was to determine the ability of DOD and

---

[1]Neither DOD nor the services know the exact number of contractors working in Iraq and Afghanistan. We are issuing a report in fall 2006 that will discuss this and other contractor-on- the- battlefield issues in more detail. See also GAO, *Military Operations: Contractors Provide Vital Services to Deployed Forces but Are Not Adequately Addressed in DOD Plans*, GAO-03-695 (Washington, D.C.: June 24, 2003).

[2]A third country national is a person working for a contractor who is neither a citizen of the United States nor the host country. Data from our survey of contractors who provide support to deployed forces revealed that contractors hired employees from 18 different nations, including the United Kingdom, Russia, South Africa, Egypt, Bangladesh, India, the Philippines, and Nepal.

[3] A biometric measures a person's unique physical characteristics (such as fingerprints, hand geometry, facial patterns, or iris and retinal scans) or behavioral characteristics (voice patterns, written signatures, or keyboard typing techniques) and can be used to recognize the identity, or verify the claimed identify, of an individual See GAO, *ELECTRONIC GOVERNMENT: Agencies Face Challenges in Implementing New Federal Employee Identification Standard* GAO-06-178 (Washington, D.C.: February 1, 2006)

contractors that support deployed forces to conduct comprehensive background screenings of employees and the steps installation commanders have taken to protect their troops. In our June 13, 2006, testimony before your committee on actions needed to improve the use of private security contractors in Iraq;[4] we provided you with preliminary information about the difficulties contractors and DOD encounter when conducting background screenings of contractor employees. This correspondence updates our preliminary observations and responds to your request concerning the process used to screen contractor employees.

To determine the ability of DOD and contractors that support deployed forces to conduct comprehensive background screenings of employees and the steps commanders have taken to protect their troops, we reviewed DOD, CENTCOM, MNF-I, and Multinational Corps-Iraq (MNC-I), polices including acquisition, force protection, base access, and biometric policies. We reviewed these policies to determine what, if any, background screening guidance and requirements were included in those documents as well as to determine who is responsible for installation safety and security.

We traveled to Iraq to meet with officials from MNF-I and, MNC-I as well as the garrison commander of a large logistics base to discuss issues related to background screenings, DOD's biometric screening program, and actions installation commanders take to reduce the risk posed by contractors. We also traveled to various locations within the United States where we met with representatives of 11 units most of whom had recently returned from Iraq and were available to meet with us. We met with them to gain an understanding of the military's role in conducting background screenings, their ability to conduct screenings on third country and host country nationals, the challenges they faced, the limitations of background screenings, and steps they took to mitigate the risks contractors pose. Additionally, we met with representatives of CENTCOM, the Under Secretary of Defense for Intelligence, and representatives of DOD's acquisition community.

We also interviewed officials from three background screening firms, one of whom served in an official capacity at a national background screening association, to obtain an understanding of the methods used by screeners and the challenges background screeners encounter when trying to screen foreign nationals. Our work focused on contractors who provide support to deployed forces in CENTCOM's area of operation and on those contractor employees who did not require security clearances.[5] [6] Enclosure I contains more detail on our scope and methodology. We

---

[4] GAO, *Rebuilding Iraq: Actions Still Needed to Improve the Use of Private Security Provides*, GAO-06-865T, (Washington, D.C.: June 13, 2006).

[5] DOD grants a security clearance to individuals needing access to classified information after conducting a personnel security investigation. DOD has established standards for these types of investigations which include examining a person's loyalty to the United States, financial situation, and criminal history. We have ongoing work looking at the process used by the government to conduct and grant security clearances for contractors, and as a result, we limited our work for this report to those employees not requiring a government issued clearance.

[6] Contractors who deploy with the forces are employees of system support and external support contractors and associated subcontractors who are specifically authorized in their contracts to deploy and provide support to U.S. military forces in contingency operations. A contingency operation is a military operation that is either designated by the Secretary of Defense as a contingency operation or becomes one as a matter of law.

conducted our review from August 2005 to August 2006 in accordance with generally accepted government auditing standards.

Results in Brief

DOD and contractors have difficulty conducting comprehensive background screening for U.S. and foreign nationals because of a lack of resources and inaccurate, missing, or inaccessible data. Because force protection officers, intelligence officers, and other officers have concerns about the comprehensiveness of background screenings and the risks contractors pose, installation commanders take steps to protect their troops. The information available to contractors that screen employees who live in the Unites States is limited to public information from county, state, or federal courts; state databases; or commercial databases, such as those that collect information on incarcerations. None of these types of searches guarantees a comprehensive background screening because these sources may not include all criminal data, among other things. Screening host nation and third country national employees can be difficult because of inaccurate or unavailable records in some countries. Also, officials from the background screening firms we spoke with told us that some foreign laws can restrict access to criminal records. Moreover, DOD's biometric screening programs are not as effective as they could be because the databases used to screen contractor employees include only limited international data, and some systems do not make all data accessible. Recognizing the limitations of data, military officials we interviewed who were responsible for security at installations in Iraq and elsewhere told us that they take steps to mitigate the risks contractors, particularly non-U.S. contractors, pose. For example, officials from most of the units we spoke with told us that contractor employees are routinely searched as they enter and leave the installation, while the majority of the units we spoke with told us that they interviewed some contractor employees before granting them access to the base.

DOD and the Department of Justice reviewed a draft of this report and neither agency disagreed with the contents of the report. Both agencies provided technical comments which we have incorporated into the report as appropriate.

Background

DOD guidance does not require that contracts contain clauses requiring contractors to conduct screenings of their employees' backgrounds However, Homeland Security Presidential Directive 12 (HSPD -12), which was issued in August 2004, and its implementing guidance, requires that the government develop standard forms of identification for all persons who need regular access to a federal facility, including U.S. military installations located overseas. Implementing guidance requires employees and contractors seeking access to federal facilities to undergo a National Agency check with written Inquiries (NACI) type background screening. [7] In January

[7]A NACI consists of searches of the Office of Personnel Management Security/Suitability Investigations Index, the Defense Clearance and Investigations Index, the Federal Bureau of Investigation Identification Division's name and fingerprint files, and other files or indexes when necessary. It also includes written inquiries and searches of records covering specific areas of an individual's background during the past 5 years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

2006, the Federal Acquisition Regulation (FAR) was amended to require that all contracts (including DOD contracts) contain a clause mandating compliance with HSPD-12.[8] In February 2006, we issued a report on issues related to implementing HSPD-12, which noted that doing a NACI on foreign nationals may be difficult because foreign nationals generally cannot have their identities verified through the standard NACI process.[9] In order to conduct a NACI, an individual must have lived in the United States long enough to have a traceable history which may not be the case for foreign nationals.

Some DOD contracts contain employee screening requirements; however, there are no DOD-wide standards or procedures for conducting these screenings when a contract requires background screenings. Furthermore, contracts do not provide guidance regarding the processes to be used or the depth of the investigations to be conducted, leaving the contractor to determine how to conduct the background screening. In addition, some contractors conduct background screenings as a result of company policy.[10] When background screenings are conducted, contractors generally use firms that specialize in conducting background screening.

Background Screenings of Contractor Employees May Not Be Comprehensive, but Military Officials Take Steps to Reduce the Risk.

Military commanders and other officers are aware that DOD and contractors have difficulties conducting comprehensive criminal background screenings and take steps to reduce the risk contractors may pose to U.S. forces and installations. When performing background screenings of contractor employees who live in the United States background screening firms use records, such as court records, which are available to the general public, or databases maintained by commercial or state entities. Using these resources does not ensure a comprehensive background screening for reasons such as incomplete data. Contractors may find it difficult to complete background screenings of their Iraqi and third country national employees because of a lack of reliable information. Another factor that can contribute to difficulties is foreign privacy laws that make some criminal information inaccessible, according to screening firm officials. Moreover, DOD's program to biometrically screen all Iraqis and most third country national contractor employees who seek access to U.S. installations is not as effective as it could be for a number of reasons, including the limited number of international and foreign databases available for screening. However, military officials we spoke with recognize the risk contractors pose to U.S. forces in part because of the numerous difficulties in screening employees, particularly those who do not live in the United States and have taken steps, such as requiring escorts for some contractor employees, to reduce the risk.

[8]Contracts awarded prior to October 27, 2005, must be amended to include the new FAR clause by October 2007.
[9]GAO-06-178
[10]Our survey of contractors that support deployed forces revealed that 3 firms that conducted background screenings did so because it was required by the contract while 21 firms conducted background screenings on their employees to satisfy internal company policies.

The Backgrounds and Identities of Contractor Employees May Be Unknown Because Important Data May Be Missing

Accurate information is not always available or accessible when contractors try to conduct criminal background investigations of U.S. nationals; third country nationals; and host country nationals, such as Iraqis. When screening firms conduct background investigations of those living in the United States, they generally use publicly available court records from the county, state, or federal level or search state criminal information repositories or commercial databases, such as those that collect information on incarcerations. However, none of these actions guarantees a comprehensive background check. For example, screening companies may not review federal court records if not directed to do so by the client. Moreover, background screening firms generally only check the records of the court that maintains the preponderance of criminal data and may miss some records maintained by specialized courts, such as domestic or family law courts. Furthermore, state repositories of information may not include all criminal data. For example, one official from a background screening firm explained that only some of the 88 counties in Ohio report crimes to the state repository. Similarly, the state of Illinois reported that in 2003 only 59 percent of the computerized criminal history records they audited had complete information. In addition, commercial databases may not provide a complete background investigation because the databases may not contain the most recent criminal data; certain criminal offenses may not be reported; and commercial databases do not have standards on how its data should be collected and validated.

Screening third country and host country nationals presents additional challenges according to background screeners to whom we have spoken. Officials from international background screening firms cited challenges in verifying criminal background information on foreign nationals for reasons such as the following.

- *Some contractors must rely on the applicant to provide all prior addresses.* Since some countries, such as India, have no national criminal database and maintain criminal data at the local level, persons doing the background screenings may miss crimes that were committed in locations within the country if the applicant did not reveal all previous addresses.
- *Some countries lack criminal records.* Officials from one firm we spoke with told us that they have encountered problems screening Iraqi nationals because the Iraqi police lack criminal records or criminal information.
- *Criminal records may be unreliable.* Some countries experience high levels of corruption. According to screening firm representatives we interviewed. Records could be destroyed, changed, or not acknowledged.
- *Some countries lack national identification numbers.* Without a national identification number the screener may not know if the person being screened was the person who committed the crimes cited in the court or police records.
- *Privacy laws limit access to data.* According to officials from background screening firms, some countries do not permit criminal background searches of their citizens or limit the type of information that can be released to a third party. In other countries, criminal information cannot be given to third parties and is only released to the applicant who can then determine whether to

release the information. According to screening company officials, there are often issues related to the authenticity of documents provided by applicants.

Information regarding those who pose a national security risk typically is not accessible to background screeners. For example, both the Federal Bureau of Investigation (FBI) and the International Criminal Police Organization (Interpol) gather information on terrorists and others who pose a national security risk, but this information is not available to commercial background screening firms. There are some online resources available but they may not provide reliable information. For example, some of the firms we spoke with told us they check the U.S. Treasury's Office of Foreign Asset Control's Specially Designated Nationals and Blocked Persons list, which consists of individuals designated as terrorists, narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. However, this type of search is limited because the primary identifier is an individual's name and aliases, thus making it difficult to know if the person being screened is the same person cited on the list.

As GAO reported in July 2005,[11] screening for human rights violators is problematic, and others we have spoken with agree that screening individuals for human rights abuses or convictions is very difficult. First, there is no unclassified U.S. government or international database of persons accused or convicted of human rights abuses. Second, crimes that might be considered human rights violations, such as homicides, are categorized by their designated criminal offense code. Third, those accused of human rights violations are difficult to track because individuals accused of such crimes can simply change their identities and their connection to human rights abuses would be lost.

The Effectiveness of DOD's Biometric Screening in Iraq Is Limited Because of Missing Data

DOD conducts biometric screening of most non-U.S. contractor employees needing access to installations in Iraq; however, the value of the screening process is limited because the databases used to screen applicants have little international biometric data. In March 2005, shortly after a dining facility bombing at a U.S. installation in Iraq killed 14 U.S. soldiers and wounded at least 50, the Deputy Secretary of Defense issued a policy requiring the biometric screening of most non -U.S. personnel seeking access to U.S. installations in Iraq. The goal of this policy is to improve force protection for U.S. and coalition forces in Iraq and provide positive identification of local and third country nationals accessing U.S. facilities. In July 2005 the Deputy Secretary of Defense issued an additional policy which requires that those seeking access to U.S. bases and installations in Iraq be fingerprinted, photographed, have their irises scanned, and be enrolled in one of two biometric systems DOD uses to gather the required biometric data. The two systems used by DOD are the Biometric Identification Systems for Access (BISA), a system specifically designed to facilitate base access, and the Biometric Automated Toolset (BAT), which was originally used in Iraq for purposes related to counterintelligence and detainee management and was later adapted for use as a base access control system.

[11] GAO, *Southeast Asia: Better Human Rights Reviews and Strategic Planning Needed for U.S. Assistance to Foreign Security Forces;* GAO-05-793 (Washington D.C.: July 29, 2005).

Biometric information from BISA and BAT is sent to the DOD's Biometric Fusion Center in West Virginia where it is merged with other biometric data collected in Iraq as well as other DOD biometric data to form the Automated Biometric Identification System (ABIS). The Biometric Fusion Center screens the applicant's data against the ABIS system as well as the FBI's Integrated Automated Fingerprint Identification System (IAFIS) database. The IAFIS database includes the fingerprint records of more than 51 million persons who have been arrested in the United States as well as information submitted by other agencies such as the Department of Homeland Security, the Department of State, and Interpol.[12]

While DOD's biometric screening process has successfully identified several persons seeking access to bases in Iraq who have criminal records in the United States, the lack of international biometric data limits its usefulness. According to an official from the FBI's Criminal Justice Information Services Division, the IAFIS database includes criminal fingerprint data from only a limited number of foreign countries because some countries are reluctant to share criminal history information and others do not have fingerprint repositories or do not collect fingerprints in a manner compatible with the FBI's system. In addition, although the IAFIS database includes fingerprint records submitted by Interpol, Interpol does not maintain a repository of all criminal offenses committed in the member countries. Instead, Interpol's criminal database is composed of wanted notices as well as some limited criminal histories. This information is submitted by the member countries, and is only retained for 5 years.

System Limitations Impact the Effectiveness of DOD's Biometric Screening

BISA and BAT both collect biometric data from a number of sources in Iraq, including contractor employees working at installations in Iraq; however, because of system shortcomings, installation commanders, who are responsible for making base access decisions in Iraq, may not have all the information necessary to make an informed decision when deciding who will have access to a U.S. installation.[13] As we noted earlier, biometric data from both BISA and BAT is sent to the Biometric Fusion Center where they are merged with other data to form the ABIS database. While data from BISA enters the ABIS database immediately, it takes, on average, 71 days for BAT biometric data to be merged into the ABIS database. As a result, any derogatory information entered into BAT in the weeks prior to a person applying for a BISA identification card might not be brought to the attention of the installation commander until after the applicant had been given access to the base. However, an official we spoke with in Iraq told us that eventually the installation commander receives this information and can revoke the employee's base access if necessary. Nevertheless, the employee may have been able to collect sensitive information or place the installation at risk during the interim.

[12]States voluntarily provide fingerprint records to the FBI for inclusion in the IAFIS database. According to FBI officials, not all persons arrested and convicted of crimes in the United States are included in the IAFIS database.

[13]The MNF-I base access policy states that installation commanders have the responsibility to make all base access decisions and makes the commanders responsible for adjudicating derogatory information found on individuals seeking base access.

Another limitation of BAT is its inability to easily determine those who pose a threat to U.S. forces from those who do not. BAT was used in Iraq as a detainee management system and was later adapted as a base access control system to improve force protection. Iraqis and others suspected of being insurgents are enrolled in BAT. In addition, Iraqis and many third country national contractor employees have also been enrolled in BAT. To distinguish detainees from contractor employees, BAT contains a text field that provides a description of why an individual was enrolled into the system. However, an official responsible for BAT told us that the text field is not a required field and data may not always be entered in the field. Officials we spoke with who have served in Iraq explained that the inability to determine why an individual was enrolled in BAT was frustrating because they could not identify those who had been enrolled as detainees from those who had been enrolled because they are contractor employees. Moreover, the descriptive text field is not included when BAT biometric data are sent to ABIS. As a result, the screening of persons enrolling in BISA who have previously been enrolled in BAT will result in a fingerprint match that must be adjudicated by the installation commander, which adds to the commander's workload unnecessarily.

Military Officials Responsible for Installation Security Recognize the Risk Contractors May Pose to their Installations but, Took Steps to Reduce the Risk

Force protection officers, military police, intelligence officers, and others from 10 of the 11 units we spoke with who served in Iraq as well as the installation commander of a large logistics base we visited in Iraq recognized the risk some contractor employees posed and took actions at their installations to minimize the risk.[14] Army officials from nine units and officers from the one U.S. Marine Corps unit we spoke with were aware of the shortcomings of the background screenings that were done by contractors or DOD. For example, several officers we spoke with told us that they believed BAT was ineffective as a screening tool because of the length of time it took to receive information from the database. Also, they noted that they did not have access to a server that contained all data collected in BAT, and thus did not have access to information collected at other installations. Moreover, one commander told us that he had concerns about whether contractors and subcontractors were screening their employees. When he asked a logistical support contractor's representative about the screening process and for screening documentation, the representative did not know if the company had conducted background screenings and could not produce any documentation of background screenings.

Given the inherent risk contractors may pose to military installations and the fact that DOD makes commanders responsible for the security of their installations, military commanders take a variety of actions to reduce that risk. Force protection officers and other military officials we spoke with who had served in Iraq described some of the steps that had been taken at their installations to reduce the risk posed by contractors. For example, host country and third country nationals were searched, prior to entering bases and installations, for contraband and other items that could jeopardize the safety of others, such as explosive materials, mobile telephones, and

[14] DOD's antiterrorism standards (DOD Instruction 2000.16) require that each unit have a designated antiterrorism officer who acts as the commander's advisor on force protection. See DOD Instruction 2000.16: DOD Antiterrorism Standards, June 14, 2001, standard E3.1.1.6 page 12.

cameras. Officials told us that employees were also searched when they left the base. If employees were found with prohibited items, they could be arrested, detained, and lose their jobs. In addition the military requires that many contractor employees, particularly host country and some third country nationals be escorted while on the base or installation. At other installations some contractor employees are required to undergo interviews with military or contractor personnel trained in human intelligence gathering. For example at one base we visited in Iraq, the installation commander required that all third country nationals from selected countries in Southwest and Central Asia be interviewed. This was in addition to the MNF-I requirement that employees who come from countries on the State Department's list of State Sponsors of Terrorism be interviewed. Also, contractor employees must display badges at all times. These badges allow or restrict an employee's access to certain areas of the installation, such as the dining facility. Finally, an official noted that he did not let host country or third country nationals from other installations have access to his installation due to concerns with security and knowing how or if the employees had been screened.

Agency Comments

DOD and the Department of Justice provided technical comments on a draft of this report. Those comments were incorporated where appropriate. Neither agency disagreed with the contents of the report.

– – – – –

We are sending copies of this report to the appropriate congressional committees and the Secretary of Defense. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

Please contact me at (202) 512-8365 or solisw@gao.gov if you or your staff have any questions concerning this report. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

Sincerely yours,

William M. Solis, Director
Defense Capabilities and Management
Enclosures-II

Scope and Methodology

Our objective was to determine the ability of the Department of Defense (DOD) and contractors that support deployed forces to conduct comprehensive background screenings of employees and the steps commanders have taken to protect their troops. To meet this objective we took several steps.

First, we met with DOD and service acquisition officials to obtain an understanding of both the extent to which background screening provisions are included in contracts as well as to learn the screening practices of their contractors. We also met with 12 U.S. and foreign contractors that provide support to deployed forces in Southwest Asia to gain an understanding of what types of background screenings are required in their contracts with DOD and the methods they use to screen their employees. We selected these contractors based upon a convenience sample, where the selection of contractors from the population was based on their availability. The contractors reflected a wide range of services provided to deployed forces. For example, we met with contractors who maintain weapons systems such as the Army's Stryker vehicle; contractors that provide base operations support, such as food and housings; and contractors that provide technical services such, as linguists or security. The contractors represented both prime contractors and subcontractors. Additionally, we met with officials from three U.S. background screening firms, two of which had international affiliates, that conduct screenings both in the United States and internationally to discover what screening practices, methods, and standards are used in the United States and other countries as well as the challenges faced in performing background screenings of U.S. nationals, third country nationals, and host country nationals. The screening firms were selected because they conducted background screenings for contractors with which we met. We also met an official from the National Association of Professional Background Screeners to obtain an industrywide perspective on methods used by screeners and challenges background screeners encounter when trying to screen foreign nationals.

To get a better understanding of the biometric screening programs being used in Iraq, we traveled to Iraq to meet with officials responsible for the biometric data systems to learn how the collection of biometric data is used to screen contractor employees and the compatibility between the systems. We also met with officials from the Biometrics Management Office and the Biometrics Fusion Center to obtain an understanding of the systems' limitations. In addition, we reviewed several DOD and Multinational Force-Iraq (MNF-I) policy documents dealing with base access and the biometric data systems.

To obtain a better understanding of the military's views and concerns regarding background screenings, we met with commanders from 11 units from 4 units (3 Army divisions and a Marine Expeditionary Force) who served in Iraq between 2003 and 2006 to discuss their ability to conduct background screenings of contractor employees who performed work at and had access to installations in Iraq. Specifically, we met with force protection officers, military police, intelligence officers, and others responsible for base operations and logistical support to gain an understanding of the military's role in conducting background screenings, their ability

to conduct screenings on third country and host country nationals, the challenges they faced, the limitations of background screenings, and steps they took to mitigate the risks contractors pose. These units were selected because, for the most part, they had recently returned from Iraq, and unit members had not moved to other locations. Additionally, we traveled to locations within Southwest Asia, including Iraq, to meet with commanders responsible for force protection at deployed locations to discuss the methods they use to conduct background screenings, actions taken to mitigate the risk, and their ability to protect their troops. We also reviewed DOD, U.S. Central Command's (CENTCOM) and MNF-I documents related to installation security and force protection.

In addition, we surveyed the contractor representatives from a random probability sample of 114 contracts providing combat support services with the principle place of performance in CENTCOM's area of responsibility originated or ongoing from the beginning of FY 2004 through May of 2005. Contracts through the end of FY2005 were included in the universe for three large contracting offices (Kuwait, Qatar, and Afghanistan), however, the majority of contracts included in the universe originated or were ongoing though May of 2005. The contracts were randomly selected from the universe of 560 contracts from the DD-350 database providing combat support services during the time period. We understood that achieving a survey response rate high enough to generalize to the population of DD-350 combat support services contracts would be difficult but acknowledged that gathering greater breadth of information through a random probability sample would be worthwhile. The questionnaire was developed with social science survey specialists in collaboration with GAO subject matter experts and was pretested with contractor representatives from 4 firms. The web based survey was administered between the dates of May 3, 2006 and July 14, 2006. We sent one follow-up e-mail message to all nonrespondents after the questionnaire had been online for 2 weeks. We then contacted remaining non-respondents by telephone after 5 weeks and sent a final email follow-up message after 9 weeks. We obtained responses from 35 contractor representatives for a response rate of 31.58 percent. The survey responses offer information from 36 contracts with 35 contracting firms providing combat support services and are not representative of the universe of all contracts in the CENTCOM area of responsibility. We include information obtained from selected survey questions to supplement information we obtained through site visits. The information from the following questions was used in this report:

[After being asked to indicate the nationalities of people hired by your firm to perform this contract] If you indicated "Nationals from other third countries" in the previous question, please describe the nationalities of these employees hired by your firm to perform this contract.

Why does your firm perform these checks for this contract? (Check all that apply.)

Required as part of the contract
Required as part of company standard policy
Other reasons
Don't know

Our work focused on contractors who provide support to deployed forces in CENTCOM area of operation and on individuals who did not require security clearances. We conducted our review from August 2005 to August 2006 in accordance with generally accepted government auditing standards.

We visited or contacted the following organizations during our review:

The Department of Defense:

- Office of the Under Secretary of Defense, Intelligence, the Pentagon
- Office of Assistant Secretary of Defense, Acquisition, Technology and Logistics, the Pentagon
- US Central Command, Tampa, Florida
- Defense Contract Management Agency, Alexandria, Virginia; Atlanta, Georgia; Houston, Texas; Baghdad, Iraq
- Personnel Security Research Center, Monterey, California
- Defense Manpower Data Center, Arlington, Virginia
- Multinational Force-Iraq, Deputy Chief of Staff Resources and Sustainment
- Multinational Force-Iraq, Deputy Chief of Staff Intelligence
- Multinational Force-Iraq, Deputy Chief of Staff Strategic Operations/Force Protection
- Multinational Corps-Iraq, Operations Directorate/ Antiterrorism/Force Protection Office

Department of the Army:

- Deputy Assistant Secretary of the Army—Policies and Procurement, Arlington, Virginia
- Coalition Forces Land Component Command, Camp Arifjan, Kuwait
- Stryker Brigade, Fort Lewis, Washington
  - Stryker Brigade: 3rd Brigade, 2nd Infantry Division, Fort Lewis, Washington
  - Stryker Brigade: 1st Brigade, 25th Infantry Division, Fort Lewis, Washington
  - Task Force Olympia, Fort Lewis, Washington
  - 593rd Corps Support Group, Fort Lewis, Washington
- Army Materiel Command, Fort Belvoir, Virginia
  - Army Field Support Command, Rock Island, Illinois

    - Army Field Support Battalion—Southwest Asia, Camp Arifjan, Kuwait
- 3rd Infantry Division, Fort Stewart, Georgia
    - Division Staff, Fort Stewart, Georgia
    - 26th Field Support Battalion, Fort Stewart, Georgia
    - 2nd Brigade Combat Team, Fort Stewart, Georgia
    - 703rd Field Support Battalion Fort Stewart, Georgia
    - Division Support Brigade, Fort Stewart, Georgia
    - 87th Combat Support Battalion, Fort Stewart, Georgia
- 3Rd Corps Support Command, Balad Iraq
- Camp Anaconda Garrison Command, Balad Iraq
- US Army Intelligence and Security Command, Fort Belvoir, Virginia
- US Army Central Command (rear), Fort McPherson, Georgia
- US Army Central Command (forward), Camp Arifjan, Kuwait
- Army Contracting Agency, Fort Lewis, Washington; Fort McPherson, Georgia
- Area Support Group-Kuwait Provost Marshall Office, Camp Arifjan, Kuwait
- Biometrics Management Office, Arlington, Virginia
- Biometrics Fusion Center, Clarksburg, West Virginia
- Biometrics Fusion Center (Forward), Camp Victory, Iraq

Department of the Navy

- 1st Marine Expeditionary Force, Camp Pendleton, California

Other Government Agencies:

- Department of Justice, Washington, DC
    - FBI, Washington, DC
        - Criminal Justice Information Services Division, Clarksburg, West Virginia
- Department of State
    - Bureau of Diplomatic Security, Arlington, Virginia
    - US Embassy Kuwait, Kuwait City, Kuwait

- US National Central Bureau of International Criminal Police Organization (INTERPOL), Washington, DC

Background Screening Firms:

- First Advantage, St. Petersburg, Florida
- First Advantage International, Bangalore, India
- Kroll Background America, Westminster, Maryland
- Kroll Background International, Nashville, Tennessee

- Background Information Services, Inc., Cleveland, Ohio
- National Association of Professional Background Screeners, Cleveland, Ohio

Contractors:

- Kellogg, Brown and Root, Camp Arifjan, Kuwait; Houston, Texas; Dubai, United Arab Emirates
- Triple Canopy Inc., Herndon, Virginia
- L3/Titan, Reston, Virginia
- CACI International, Arlington, Virginia
- Risk Management Solutions, Panama City, Florida
- Ahmadah General Trading & Contracting Co., Camp Arifjan, Kuwait
- British Link Kuwait, Camp Arifjan, Kuwait
- Tamimi Global Co., Camp Arifjan, Kuwait
- Kuwait & Gulf Link Transport Co., Camp Arifjan, Kuwait
- IAP World Services, Camp Arifjan, Kuwait
- ITT Industries, Camp Arifjan, Kuwait
- Prime Projects International, Dubai, United Arab Emirates

GAO Contact and Staff Acknowledgements

GAO contact

William M. Solis, (202) 512-8365 or solisw@gao.gov

Acknowledgements

In addition to the contact named above, major contributors to this report were David A. Schmitt, Assistant Director; Carole F. Coffey, Assistant Director; Vincent Balloon, Grace Coleman, Jennifer Cooper, Laura Czohara Wesley Johnson, Kenneth E. Patton, and James A. Reynolds.

(350732)

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 "Subscribe to 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, D.C. 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, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548