



Office of Inspector General

November 29, 2010

MEMORANDUM

TO: USAID/Iraq Mission Director, Alex Dickie

FROM: Director, Office of Inspector General/Iraq, Lloyd J. Miller /s/

SUBJECT: Survey of Security Incidents Reported by Private Security Contractors of USAID/Iraq's Contractors and Grantees (Report Number E-267-11-001-S)

This memorandum transmits our final report on the subject survey. We have carefully considered your comments on the draft report and included your response, without attachments, in Appendix II of the report.

The survey is not an audit. The report contains five recommendations to USAID/Iraq to assist in improving oversight of their private security service subcontractors.

On the basis of information provided by the mission in its response to the draft report, we consider that both a management decision and final action have been taken on Recommendations 2 and 4. Management decisions on Recommendations 1 and 3 can be reached once USAID/Iraq and the Office of Inspector General/Iraq agree on a firm plan of action, with target dates, for completing the implementation of the two recommendations. We added a new Recommendation 5 subsequent to the mission providing its response to the draft report, and consequently this recommendation does not have a management decision. Please provide written notice within 30 days of any actions planned or taken to implement these recommendations.

I want to express my appreciation for the cooperation and courtesies extended to my staff during the survey.

CONTENTS

- Background** 1
- Survey Findings** 4
 - Partners Reported 94 Security Incidents 5
 - Reporting of Security Incidents to USAID/Iraq Was Incomplete 6
 - Records of Security Incidents Were Incomplete 8
 - USAID/Iraq Agreement or Contracting Officer’s Technical
Representatives Were Not Aware of Responsibilities 9
 - Embassy Baghdad Has Not Issued Instructions in Accordance With
Regulation Implementing Statutory Requirements 10
- Evaluation of Management Comments** 12
- Appendix I—Scope and Methodology** 13
- Appendix II—Management Comments** 16
- Appendix III—List of 94 Serious Security Incidents** 20
- Appendix IV—Key Statutory Requirements in Sections 862 and 864 of the
National Defense Authorization Act for Fiscal Year 2008, as Amended** 23
- Appendix V—Interim Final Rule, 32 CFR Part 159** 29

BACKGROUND

Private security contractors (PSCs) operating in Iraq provide security services that include the protection of individuals, life support, office facilities, and nonmilitary transport movements. USAID/Iraq does not maintain any direct contracts with PSCs; security services were procured by the mission's implementing partners (contractors and grantees), who have primary oversight responsibilities for their security providers. Nevertheless, in managing its contracts and grant agreements, USAID/Iraq has some degree of oversight for private security activities. In addition, Section 862 of the National Defense Authorization Act for FY 2008 (NDAA FY 2008)¹ establishes a statutory scheme for oversight of all PSCs in areas of combat operations, specifically including Iraq and Afghanistan, through required regulations in subsection (a) and mandatory insertion of contract provisions in subsection (b). Section 862(a) requires that the Secretary of Defense promulgate regulations on the selection, training, equipping, and conduct of PSC personnel that meet specified requirements. Under Section 862(a)(2)(D), these regulations must establish a process under which contractors are required to report all incidents in which:

- A weapon is discharged by personnel performing private security functions in an area of combat operations.
- Personnel performing private security functions in an area of combat operations are killed or injured.
- Persons are killed or injured, or property is destroyed, as a result of conduct by contractor personnel.
- A weapon is discharged against personnel performing private security functions in an area of combat operations or personnel performing such functions believe a weapon was so discharged.
- Active, nonlethal countermeasures (other than the discharge of a weapon) are employed by the personnel performing private security functions in an area of combat operations in response to a perceived immediate threat to such personnel.

To meet the requirements of NDAA FY 2008 Section 862(a), the Secretary of Defense promulgated Interim Final Rule 32 CFR 159² on July 17, 2009, about a year after the deadline for the regulation set by NDAA FY 2008 Section 862(a). Prior to the July 2009 effective date for the Interim Final Rule, in May 2008 the U.S. Embassy in Baghdad (Embassy Baghdad) issued policy directives to armed PSCs that addressed some of the concerns of NDAA FY 2008. Although the Embassy Baghdad policy directives required serious incident reporting, it did not require PSC reporting of the specific incidents required to be reported by NDAA FY 2008 Section 862(a)(2)(D), as shown above. In March 2009, the Combatant Commander of the Multi-National Force-Iraq (MNF-I) updated its guidance to private security companies. These directives required PSCs to report serious security incidents. Specifically, the May 2008 Embassy Baghdad policy directives provided PSCs with rules, regulations, and requirements for operating in Iraq that were consistent with a December 2007 memorandum of agreement

¹ See Appendix IV for the key statutory requirements in Sections 862 and 864 of the National Defense Authorization Act for FY 2008, as amended.

² See Appendix V for Interim Final Rule (32 CFR 159).

between the Department of Defense (DOD) and the Department of State (DOS). The policy directives required all PSCs to coordinate their private security detail movements with the Embassy's Regional Security Office's (RSO) Tactical Operations Center and the Contractor Operations Cell of the Multi-National Corps-Iraq. In addition, the policy directives required PSCs to immediately activate their transponder alert system when a serious security incident occurs and to establish two-way communication with the Contractor Operations Cell.

The policy directives also required PSCs to provide verbal or email notification of any serious security incident to the RSO Tactical Operations Center and to the Contractor Operations Cell as soon as practical, but not later than 1 hour after the incident. In addition, PSCs must submit an initial formal incident report in writing within 4 hours of the incident. Finally, a follow-up comprehensive written report of the events surrounding the incident must be provided within 96 hours, unless otherwise directed by the RSO.

From July 1, 2007, to June 30, 2009, USAID/Iraq maintained a portfolio of contracts and grants with 12 implementing partners, who held 17 subcontracts for private security services in Iraq.³ According to information provided by USAID/Iraq's implementing partners, these 17 subcontracts for security services incurred cumulative expenditures of \$483 million⁴ as of December 31, 2009. USAID/Iraq reported that the implementing partners incurred expenditures of \$2.1 billion over the same period. The information provided by the implementing partners and USAID/Iraq shows that security services accounted for approximately 23 percent of the implementing partners' total costs.

In 2009, the Office of Inspector General/Iraq conducted an audit to determine whether USAID/Iraq's implementing partners were providing adequate oversight of their private security service subcontractors in Iraq.⁵ The audit included two recommendations, in which we advised USAID/Iraq to require its implementing partners (1) to establish procedures to monitor the reporting of serious security incidents⁶ to ensure that such incidents are properly reported and (2) to notify USAID/Iraq of all serious security incidents by including the mission in the reporting of these incidents.

The purpose of this survey was (1) to determine the number of serious security incidents that occurred between July 1, 2007, and June 30, 2009, and (2) to follow up on the effectiveness of the mission's and implementing partners' actions in implementing our March 2009 audit report recommendations.

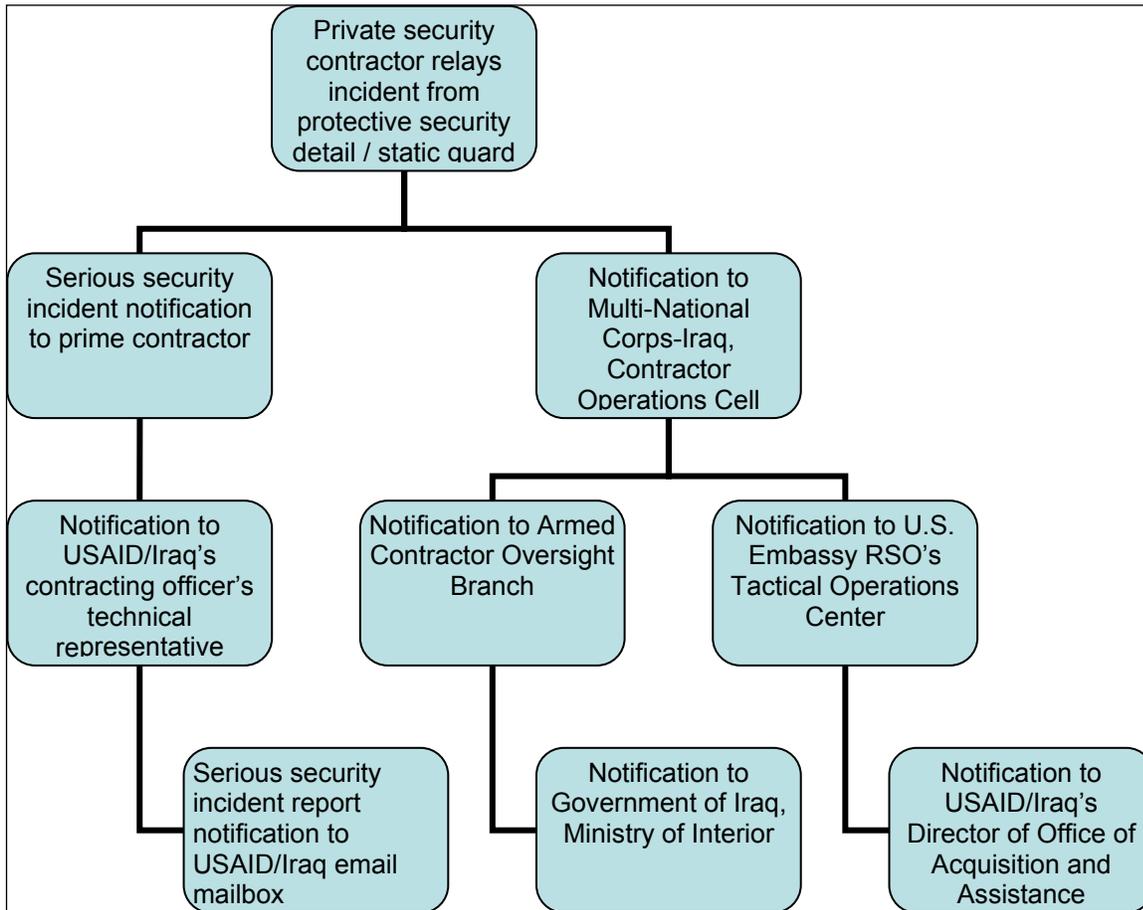
³ During this period, some USAID/Iraq contractors and grant recipients had more than one contract but only one subcontractor for security services, some contracts expired during the period and new contracts were issued, and one USAID recipient provided its own security services.

⁴ We did not verify these expenditure totals.

⁵ "Audit of USAID/Iraq's Oversight of Private Security Contractors in Iraq," Audit Report No. E-267-09-002-P, March 4, 2009.

⁶ According to DOS and DOD policy directives, the term "serious security incident" involves the use of deadly force, discharge of a weapon, an incident resulting in death, serious injury, or significant property damage (even if a weapon is not involved), or other serious consequences. PSCs shall report serious incidents they observe, suspect, or participate in, including aggressive personal behavior, road rage, criminal acts, traffic accidents, and any incident believed to have possible strategic or operational impact. NDAA FY 2008 and Interim Final Rule 32 CFR 159 simply refer to these as "incidents".

Security Incident Reporting Process⁷



⁷ The security incident reporting process in the diagram is based on the Embassy Baghdad May 2008 policy directive, the Combatant Commander's March 2009 guidance, and USAID guidance to its implementing partners. We also verified these steps with the Coordinator for Armed Contractor Oversight in the Embassy Baghdad Regional Security Office.

SURVEY FINDINGS

USAID/Iraq's implementing partners did not establish procedures to monitor reporting of serious security incidents and did not consistently report incidents as required by our two prior audit recommendations. Moreover, Embassy Baghdad has not issued instructions to incorporate the statutory and regulatory requirements for PSC oversight described in the background section of this report. However, USAID/Iraq has implemented numerous actions (1) to implement our two prior audit recommendations from March 2009 and (2) to provide oversight and direction of the use of private security contractors (PSCs) by its contractors and grantees. Nevertheless, contractor and subcontractor implementation has not been fully effective. USAID/Iraq actions include the following.

- Issued on March 15, 2009, a formal mission notice⁸ to all contractors and grantees specifying procedures for the reporting of security incidents by PSCs.
- Amended all 16 active direct awards to contractors and grantees to include a new provision for serious security incident reporting requirements.
- Set up on March 16, 2009, a central email account as a repository of all serious security incident reports received from implementing partners.
- Added new requirements to the official designation letter for contracting officer's technical representatives (COTRs), such as receiving and reviewing serious security incident reports, using the incident report as a monitoring tool, and seeking clarification from implementing partners on possible program impact.
- Ensured that all PSCs for USAID implementing partners have been registered with the Ministry of Interior of the Government of Iraq.
- Cochaired the Baghdad Joint Incident Review Board with DOD and DOS. The board's purpose is to conduct joint reviews of incidents involving PSCs, identify trends, and serve as a forum for exchanging information and coordinating efforts.
- Participated with DOD and DOS in the RSO-sponsored Armed Contractors Working Group, whose purpose is to review common security issues and lessons learned.
- Attended and gave presentations at quarterly conferences organized by DOD and DOS for Iraq PSCs.

Our March 2009 audit report recommended that USAID/Iraq require its implementing partners (1) to establish procedures to monitor the reporting of serious security incidents and (2) to notify the mission of all serious security incidents. Despite USAID's efforts, Recommendation 1 has not been implemented by implementing partners, and Recommendation 2 has not been consistently implemented. None of USAID/Iraq's implementing partners have established documented internal procedures to monitor the reporting of security incidents to ensure that such incidents are properly reported. In general, the implementing partners perceived that the amendments to their contract or grant agreement with USAID/Iraq had fulfilled the requirement to establish procedures. Nevertheless, contractor and subcontract implementation of USAID/Iraq's guidance has not been fully effective. The weaknesses include:

⁸ Mission Notice 09-03-001.

- Incomplete reporting of security incidents to USAID and the Contractor Operations Cell of the Multi-National Force-Iraq.
- Incomplete records of security incidents by implementing partners.

In addition to issues with contractor and subcontractor implementation, and despite clear guidance, the majority of USAID/Iraq’s own COTRs were not aware of their responsibilities. In addition, the Embassy Baghdad May 2008 policy directive, which is still in use, does outline conditions for reporting but does not explicitly require PSC reporting of the specific incidents required to be reported by NDAA FY 2008 or 32 CFR 159. Below is our discussion of these issues, along with a description of the 94 documented serious security incidents that occurred over the 2 years from July 1, 2007, to June 30, 2009.

Partners Reported 94 Security Incidents

During the 2 years from July 1, 2007, to June 30, 2009, 94 serious security incidents were documented and reported by USAID/Iraq implementing partners and their PSCs. As summarized in Table 1, two implementing partners (Research Triangle Institute and International Relief and Development) accounted for 72 (74 percent) of the 94 serious incident reports. Security services for the 12 USAID/Iraq prime contractors and grantees were provided through 6 private security subcontractors and 1 cooperative agreement recipient.⁹ Appendix III provides details of the 94 security incident reports.

Table 1. Security Incident Reports From July 1, 2007, to June 30, 2009

USAID/Iraq Implementer	Private Security Contractor	Number of Serious Security Incident Reports
Cooperative Housing Foundation	Unity Resources Group	2
International Foundation for Electoral Systems	Garda World	0
Research Triangle Institute	Armor Group/Unity Resources Group	43
BearingPoint	Garda World	1
Development Alternatives	Garda World	1
International Business and Technical Consultants	Garda World	0
Louis Berger Group	SallyPort	8
Management Systems International	SallyPort	7
AECOM International Development	SallyPort	1
International Relief and Development	Sabre	29
Relief International	Triple Canopy	2
ACDI-VOCA	No security contractor; security is self-provided	0
Total		94

⁹ Some private security companies provided services to more than one USAID implementing partner, and one USAID/Iraq implementer, ACDI-VOCA, provided its own security protection.

As shown in Table 2, of the 94 security incident reports, the more significant categories were 23 incidents involving improvised explosive devices,¹⁰ rockets, or missile attacks; 28 incidents involving a weapon discharge; and 19 incidents involving vehicles or traffic access denied by the Iraqi police.

Table 2. Security Incident Reports by Incident Type

USAID/Iraq Implementer	Improvised Explosive Device or Rockets or Missile Attacks	Weapon Discharge	Flare Shot	Negligent, Accidental, or Malfunction Discharge	Traffic Accident or Access Denial	Armed Robbery or Theft	Off-Duty Injury, Abduction, Threat
Cooperative Housing Foundation	2	0	0	0	0	0	0
International Foundation for Electoral Systems	0	0	0	0	0	0	0
Research Triangle Institute	5	17	6	6	7	1	1
BearingPoint	1	0	0	0	0	0	0
Development Alternatives	0	0	0	0	0	0	1
International Business & Technical Consultants	0	0	0	0	0	0	0
Louis Berger Group	0	5	1	0	1	0	1
Management Systems International	4	0	0	0	2	0	1
AECOM International Development	0	0	0	0	1	0	0
International Relief and Development	9	6	0	4	8	2	0
Relief International	2	0	0	0	0	0	0
ACDI-VOCA	0	0	0	0	0	0	0
Total	23	28	7	10	19	3	4

Reporting of Security Incidents to USAID/Iraq Was Incomplete

In response to our March 2009 “Audit of USAID/Iraq’s Oversight of Private Security Contractors in Iraq,” USAID/Iraq issued a formal mission notice to all contractors and grantees specifying procedures for the reporting of security incidents by PSCs. These procedures required contractors and grantees (1) to establish procedures and to monitor the serious incident reporting by their PSCs and (2) to inform the mission of any and all serious security incidents. In addition, the mission amended all direct awards to contractors and grantees to include a new provision for “serious incident reporting requirements.” These reporting requirements stated that PSCs must:

- Provide notification, verbally or by email, of any serious incident to the RSO Tactical Operation Center and to the Contractor Operations Cell not later than 1 hour after the incident.

¹⁰ The term “improvised explosive device” (IED) includes vehicle-borne IED, vehicle-carried IED, victim-detonated IED, and remote-controlled IED. The difference between “vehicle borne” and “vehicle carried” is that a “vehicle borne” IED is generally suicidal, whereas a “vehicle carried” IED is generally not suicidal.

- Submit an initial formal incident report in writing within 4 hours to the prime contractor/recipient, USAID/Iraq, the RSO Tactical Operation Center, and the Contractor Operations Cell.
- Provide a follow-up comprehensive written report of events within 96 hours to the prime contractor/recipient, the RSO Tactical Operation Center, and USAID/Iraq.

In addition, in May 2008, Embassy Baghdad issued policy directives to armed PSCs and, in March 2009, the Multi-National Force-Iraq (MNF-I) issued guidance to PSCs. These directives require serious incident reporting, as described in the USAID/Iraq mission notice.

During the period April to June 2009,¹¹ PSCs did not always report serious security incidents to USAID/Iraq. For example, records at implementing partners and their PSCs showed nine security incidents reported. Records at the Contractor Operations Cell and the Armed Contractor Oversight Branch showed 11 security incidents, and records at the USAID/Iraq mailbox showed 7 incidents. However, each source should show the same number of reported incidents. Table 3 provides the number of security incident reports from each source for the 3-month period following the issuance of new mission guidance in March 2009.

Table 3. Security Incident Reports, April 1–June 30, 2009

USAID/Iraq Implementer Partners	Reports at Private Security Contractors	Reports at Contractor Operations Cell or Armed Contractors Oversight Branch	Reports at USAID/Iraq Mailbox
Cooperative Housing Foundation	0	1	0
International Foundation for Electoral Systems	0	0	0
Research Triangle Institute	3	2	2
BearingPoint/Deloitte	0	0	0
Development Alternatives	1	1	0
International Business and Technical Consultants	0	0	0
Louis Berger	0	0	0
AECOM	0	0	0
Management Systems International	1	1	1
International Relief and Development	4	6	4
Relief International	0	0	0
ACDI-VOCA	0	0	0
Total	9	11	7

¹¹ We reviewed these 3 months because the period was subsequent to the March 2009 USAID/Iraq mission notice to all the contractors and grantees specifying procedures for the reporting of security incidents by PSCs.

In a more recent example in February 2010, one private security contractor reported six security incidents in its monthly threat report to USAID/Iraq. However, during the same interval, only two incidents were reported to USAID/Iraq's mailbox.

The disparity in reporting happened for two reasons. First, almost all of USAID/Iraq's implementing partners relied on their PSCs to report and maintain records of their security incidents. Only one partner had custody of its security incident reports and was able to provide records of them. Second, implementing partner staffs do not always understand reporting procedures. For example, one implementing partner stated that he sends security incident reports only to the RSO Tactical Operations Center and thought the RSO had the responsibility to forward the reports to USAID/Iraq. In another case, a security incident involving the negligent discharge of a weapon was not reported to USAID/Iraq. A USAID COTR learned of the incident when the Embassy's RSO asked about it. USAID/Iraq ultimately obtained a copy of the incident report only after the COTR had requested it. As noted earlier, none of USAID/Iraq's implementing partners had established documented internal procedures to monitor the reporting of security incidents to ensure that such incidents are properly reported.

Implementing partners did not always provide sufficient oversight of their PSCs with respect to incident reporting. This lack of monitoring led to reporting deficiencies and missing security incident reports. Because of USAID/Iraq's ineffective implementation of our March 2009 recommendations, we are restating our original recommendation and adding a requirement for the mission to verify implementing partners' actions.

Recommendation 1. We recommend that USAID/Iraq require its implementing partners to establish procedures to monitor the reporting of security incidents to ensure that such incidents are properly reported in accordance with Embassy and USAID guidance and verify that each implementing partner has completed this corrective action.

Recommendation 2. We recommend that USAID/Iraq provide training for the implementing partners to coordinate and reinforce roles and responsibilities and to address control weaknesses in security incident reporting requirements.

Records of Security Incidents Were Incomplete

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* states that internal controls and all transactions and other significant events need to be clearly documented and that the documentation should be readily available for examination.¹² A serious security incident qualifies as a significant event.

In response to our March 2009 audit, USAID/Iraq noted that in addition to GAO standards, its new procedures will require the partners at a minimum to (1) ensure that they receive a copy of all serious security incident reports issued by their PSC; (2) maintain detailed records (e.g., copies of incident reports) documenting all reported incidents to facilitate monitoring; (3) review applicable procedural guidance to gain a clear understanding of the current prescribed procedures for reporting serious security incidents; and (4) regularly review their PSC's actual reporting procedures to ensure that they are consistent with those current and prescribed by the U.S. Embassy. USAID/Iraq's March 2009 mission notice and the award amendments stipulate that the prime contractor/recipient must ensure that all records are maintained on file.

¹² GAO/AIMD-00-21.3.1 (November 1999), page 15

None of USAID/Iraq's implementing partners were able to fully account for all serious security incident reports. Of 10 implementing partners, one (Research Triangle Institute) had security incident reports on file. However, even this implementer had only incomplete records. For instance, from July 1, 2007, to June 30, 2009, this implementer had 39 security incident reports on file, while its PSC had 21 security incident reports on file for the same period.

The implementing partners were not able to account for all security incident reports because they had been relying on the PSCs to report and track the reports. Implementing partners felt that since they were colocated with the PSCs, maintaining separate recordkeeping of security incident reports would amount to duplicated efforts. However, implementing partners had no controls in place to ensure that all security incident reports were accurately accounted for and safeguarded. Furthermore, because implementing partners lacked complete records of security incidents, they were not in a position to detect inaccuracies and inconsistencies associated with the reports.

The prime contractors are responsible for ensuring that all subawardees are familiar with relevant rules and regulations and comply with them. Complete and reliable reporting and recordkeeping of security incidents is needed to ensure that security risks are promptly addressed and that coordination of information with other U.S. Government agencies is not hindered. Moreover, jurisdiction of private security contractors has been turned over to the Iraqi Government. Therefore, it is critical that implementing partners and their PSCs adhere to policies, procedures, and requirements.

***Recommendation 3.** We recommend that USAID/Iraq require its implementing partners to establish and maintain records of reported serious security incidents and verify that each implementing partner has completed this corrective action.*

USAID/Iraq Agreement or Contracting Officer's Technical Representatives Were Not Aware of Responsibilities

USAID's Automated Directives System 302 and 303 require that the agreement or contracting officer's technical representative (AOTR or COTR) should monitor, review, and verify reports and deliverables. In addition, according to their designation letter, the AOTR or COTR serves as the mission's point person for receiving and reviewing the serious incident reports. Further duties include:

- Using the serious security incident report as a monitoring tool and seeking clarifications from the implementing partner on any impact an incident may have on the implementation of the program.
- Alerting the contracting or agreement officer if the incident has potential cost or scope limitations.
- Forwarding a copy of the serious security incident report and any perceived impact to the USAID/Iraq mailbox designated for these reports.

However, some COTRs stated that they had not been provided guidance about their oversight responsibilities or their roles and responsibilities regarding security incident reporting procedures. In addition, some COTRs did not understand that one of their responsibilities was

to submit security incident reports that they received from the implementing partners or PSCs to the USAID/Iraq mailbox.

The USAID/Iraq special mailbox for security incident reports is monitored by the deputy mission director and the executive officer. However, if these technical representatives are not fulfilling their duties as designated, the mailbox will not have a complete record of incidents for consideration by mission management.

Recommendation 4. *We recommend that USAID/Iraq develop and provide training for its agreement/contracting officer's technical representatives for their roles in receiving, reviewing, and forwarding serious security incident reports to the designated USAID/Iraq mailbox and other required security incident responsibilities.*

Embassy Baghdad Has Not Issued Instructions in Accordance With Regulation Implementing Statutory Requirements

As discussed in the background section, the statutory scheme under NDAA FY 2008 Section 862(a) for oversight of all PSCs in combat operation areas is implemented by Interim Final Rule 32 CFR 159, promulgated in July 2009 by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics¹³. Under 32 CFR 159.4(c), the Chief of Mission for Iraq is responsible for issuing implementing instructions for non-DOD PSCs and their personnel consistent with the standards set forth by the geographic Combatant Commander, and has the option to instruct non-DOD PSCs and their personnel to follow the guidance and procedures developed by the Geographic Combatant Commander and/or Subordinate Commander. However, Embassy Baghdad has not issued instructions in accordance with 32 CFR 159.4(c) and its May 2008 policy directive does not incorporate the statutory requirements for PSC security incident reporting implemented by 32 CFR 159.

The Embassy Baghdad May 2008 policy directive, which is still in use, does outline conditions for reporting including small arms fire, improvised explosive devices, indirect fire, PSC weapons discharges, traffic accidents, rules for use of force incidents, and graduated force response incidents. Nevertheless, the policy directive does not explicitly require PSC reporting of the specific incidents required to be reported by NDAA FY 2008 Section 862(a)(2)(D) or 32 CFR 159.6(a)(1)(v)¹⁴. According to officials, the Embassy does plan to update the policy, but the update was not intended to incorporate statutory and regulatory requirements.

¹³ According to officials within the DOD's Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, all US government private security contractors in Iraq are covered by Interim Final Rule 32 CFR 159. The Department of State, DOD, and USAID are operating with the understanding that both Iraq and Afghanistan are designated areas of combat operations for the purposes of this provision. DOD and the Department of State are currently planning the transition to the Department of State as the lead agency in Iraq. When that happens, for the purposes of this provision, Iraq will no longer be considered an area of combat operations. The policy and guidance for the management of PSCs operating in Iraq after the transition are currently being developed. However, the officials do not believe that there will be a significant change in requirements for the management and oversight of PSCs.

¹⁴ The categories of security incidents under NDAA FY 2008 and 32 CFR 159 are essentially the same. 32 CFR 159 splits the statute's category, "persons are killed or injured, or property is destroyed, as a result of conduct by contractor personnel", into two categories: (1) persons are killed or injured and (2) property is destroyed.

As earlier noted, reported security incidents from July 2007 to June 2009 identified 94 security incidents. 65 of these 94 security incidents were among the incidents required to be reported by NDAA FY 2008 Section 862(a)(2)(D) or 32 CFR 159.6(a)(1)(v). Table 4 distinguishes the 94 security incident reports according to these conditions, including an “other” category for reports that did not specifically align with the statute’s conditions.

Table 4. Security Incident Reports by Statutory Conditions

National Defense Authorization Act for Fiscal Year 2008 Conditions for Reporting Security Incidents	Number of Security Incidents Reported¹⁵
A weapon is discharged by personnel performing private security functions in an area of combat operations.	35
Personnel performing private security functions in an area of combat operations are killed or injured.	13
Persons are killed or injured, or property is destroyed, as a result of conduct by contractor personnel.	8 ¹⁶
A weapon is discharged against personnel performing private security functions in an area of combat operations or personnel performing such functions believe a weapon was so discharged.	15
Active, nonlethal countermeasures (other than the discharge of a weapon) are employed by the personnel performing private security functions in an area of combat operations in response to a perceived immediate threat to such personnel.	22
Other types of security incidents reported.	29
Total	122

In order to align PSC security incident reporting with statutory and regulatory requirements, the audit is making the following recommendation.

Recommendation 5. *We recommend that USAID/Iraq request Embassy Baghdad to issue instructions for private security contractors and their personnel in accordance with Interim Final Rule 32 CFR 159.4(c).*

¹⁵ In some cases, the 94 security incident reports covered more than one condition as outlined in NDAA FY 2008, for a total of 122 conditions.

¹⁶ The 8 security incident reports from the column “persons are killed or injured, or property is destroyed, as a result of conduct by contractor personnel” include 3 reports of persons injured, 1 report of a person killed (pedestrian killed in collision with security convoy), 3 reports of property destroyed, and 1 report of both persons injured and property destroyed.

EVALUATION OF MANAGEMENT COMMENTS

The mission agreed with the four recommendations in the draft report and described actions planned and taken to address each of the recommendations.

In regard to recommendations 1 and 3, the mission revised the language of the “Serious Incident Reporting” (SIR) clause to be included in all mission award documents. Although it was a positive response to the recommendation, revising the clause language does not address all the elements of the recommendations—specifically, the need to verify that each implementing partner has completed corrective actions. Page 9 of the report states that, due to ineffective implementation of our March 2009 recommendations, we are restating our original recommendation and adding a requirement for the mission to verify implementing partners’ actions. In our opinion, such verification is essential. Furthermore, the mission response does not address when the language revisions will be incorporated into mission award documents. Management decisions for Recommendations 1 and 3 can be made when the mission submits an action plan, with target dates for completion, for implementing the recommendations including verification of implementing partners’ actions.

In regard to recommendation 2, the mission stated that they will use the quarterly partner meetings as the forum to provide information and guidance on the implementation of the requirements contained in the SIR clause set forth in the mission’s response to Recommendation 1. The management comments from the mission did not state a target date for completion of the training, however, subsequently, the mission provided additional documentation to support that the quarterly partner meetings were used as a forum to provide information and guidance on the implementation of the requirements. As a result, Recommendation 2 has a management decision and final action.

In regard to recommendation 4, the mission included a specific section on the handling of review, reporting, and distribution of the serious incident reports in its AOTR/COTR designation letters, and in July 2010, the mission added a mandatory briefing with the Office of Acquisition and Assistance to the mission’s check-in process for COTR/AOTRs. The briefing includes a detailed review of the SIR reporting procedures and their delegated responsibilities. We consider that a management decision has been made and final action taken for Recommendation 4.

In regard to recommendation 5, we added a new recommendation subsequent to the mission providing its response to the draft report, and consequently this recommendation does not have a management decision.

SCOPE AND METHODOLOGY

Scope

The purpose of this survey was (1) to determine the number of serious security incidents that occurred between July 1, 2007, and June 30, 2009, and (2) to follow up on the effectiveness of the mission's and implementing partners' actions in implementing the audit recommendations from our "Audit of USAID/Iraq's Oversight of Private Security Contractors in Iraq," issued March 4, 2009. This survey reviewed all incident reports from all 12 prime contractors and 6 private security subcontractors that were active during any part of the period from July 1, 2007, to June 30, 2009. According to information provided by USAID/Iraq's implementing partners, the 17 subcontracts for security services during this period incurred expenditures of \$483 million¹⁷ as of December 31, 2009, from inception of each subcontract.

We examined significant internal controls at USAID/Iraq, the implementing partners, and the private security contractors (PSCs). For USAID/Iraq, we examined:

- The March 2009 guidance to implementing partners.
- The mailbox established to receive security incident reports.
- Contracts and grant agreements (including amendments) with implementing partners to identify security requirements.

For the implementing partners, in addition to the controls listed above, we examined:

- Subcontracts and subawards with PSCs.
- Sample security incident reports from time of occurrence and filing of first report, interim, and final report.
- Records of all security incident reports for accuracy and completeness.
- Internal written procedures to monitor and supervise PSCs.
- Sample monthly or weekly reports to USAID/Iraq Office of Acquisition and Assistance.

For the PSCs, in addition to the controls and records listed above, we examined:

- Logs and records of incidents reported from July 1, 2007, to June 30, 2009.
- Monthly threat reports to USAID/Iraq Office of Acquisition and Assistance.
- Rules and regulations for protective security detail and protective security specialists.
- Task order schedule and statement of work.

¹⁷ We did not verify these expenditure totals.

Survey fieldwork was performed from September 23, 2009, to March 30, 2010, at the USAID/Iraq Mission and the in-country offices of eight prime contractors and their eight associated private security subcontractors whose offices were located in Baghdad, Iraq. Four of these offices were in the Red Zone, and four were in the International Zone. We also collected information from two additional implementing partners at the USAID/Iraq offices outside of Baghdad, and we collected information through electronic correspondence from two implementing partners whose contracts had expired and no longer had a presence in-country.

Methodology

To determine the number of serious security incidents from July 1, 2007, to June 30, 2009, we took the following actions:

- Interviewed USAID/Iraq Office of Acquisition and Assistance staff and contracting officer's technical representatives (COTRs).
- Identified all PSCs used by USAID/Iraq's prime contractors and grantees for the period under review.
- Visited and interviewed all active implementing partners and the PSCs.
- Obtained records of serious security incident reports from the implementing partners, the PSCs, the Armed Contractor Oversight Branch, the Contractor Operations Cell of the Multi-National Corps-Iraq, and USAID/Iraq's mailbox; we then compared the data.
- Reviewed PSCs' monthly threat reports.
- Reviewed all serious security incident reports for accuracy, completeness, and compliance with rules and regulations.
- Compared records received from each reporting entity to determine whether all serious security incident reports were reported to the appropriate authorities.
- Performed a walk-through of the PSCs' operations, including observation of protective security detail dispatch movements and surveillance monitoring.
- Reviewed Department of Defense, Department of State, and USAID regulations and guidance on private security services in Iraq.

We also followed up on two prior audit recommendations, in which we had advised USAID/Iraq to require its implementing partners (1) to establish procedures to monitor the reporting of serious security incidents and (2) to notify the mission of all serious security incidents. In addition to the actions described above, our assessment included whether the prime contractors and their private security subcontractors had established controls, had communicated all the serious security incident reports to USAID/Iraq management, and were using sample security incident reports consistent with data requirements established in policy directives. We also obtained an understanding of the guidance on security incident reporting requirements by reviewing the following rules and regulations:

- Policy Directives for Armed Private Security Contractors in Iraq, U.S. Embassy in Baghdad, Iraq, May 2008.

- “Overarching FRAGO for Requirements, Communications, Procedures, Responsibilities for Control, Coordination, Management, and Oversight of Armed Contractors/DoD Civilians and Private Security Companies,” Fragmentary Order 09-109, Multi-National Force-Iraq, February–March 2009 updates.¹⁸
- USAID/Iraq Mission Notice, “Private Security Contractors—Incident Reporting,” No. 09-03-001, March 15, 2009.
- USAID/Iraq’s AOTR and COTR designations.
- USAID Automated Directives System, Chapters 302 and 303.
- Key Statutory Requirements in Sections 862 and 864 of the National Defense Authorization Act for Fiscal Year 2008, as amended
- 32 CFR Part 159 Private Security Contractors Operating in Contingency Operations.

¹⁸ Fragmentary Order 09-109, March 2009, replaced earlier orders. MNF-I FRAGO 09-109 is a revision of prior PSC guidance that was required in the National Defense Authorization Acts of Fiscal Years 2008 and 2009 and was committed to in earlier interagency agreements. The FRAGO is intended to apply equally to DOD and DOS PSCs by virtue of the memorandum of agreement signed by the Departments on December 5, 2007.

MANAGEMENT COMMENTS



August 29, 2010

MEMORANDUM
UNCLASSIFIED

TO: Lloyd Miller, Office of the Inspector General/Iraq

FROM: Alex Dickie, Mission Director /s/

SUBJECT: Management Comments in Response to Draft Survey of Security Incidents Reported by Private Security Contractors of USAID/ Iraq's Contractors and Grantees (Report Number E-267-10-00X-S)

On July 29, 2010, the Office of the Inspector General/Iraq (OIG/Iraq) transmitted its draft Survey of Security Incidents Reported by Private Security Contractors of USAID/ Iraq's Contractors and Grantees (Report Number E-267-10-00X-S) (Tab A). The draft report contains four recommendations:

Recommendation 1. We recommend that USAID/Iraq require its implementing partners to establish procedures to monitor the reporting of security incidents to ensure that such incidents are properly reported in accordance with Embassy and USAID guidance and verify that each implementing partner has completed this corrective action.

Recommendation 2. We recommend that USAID/Iraq provide training for the implementing partners to coordinate and reinforce roles and responsibilities and to address control weaknesses in security incident reporting requirements.

Recommendation 3. We recommend that USAID/Iraq require its implementing partners to establish and maintain records of reported serious security incidents and verify that each implementing partner has completed this corrective action.

Recommendation 4. We recommend that USAID/Iraq develop and provide training for its agreement/contracting officer's technical representatives for their roles in receiving, reviewing, and forwarding serious security incident reports to the designated USAID/Iraq mailbox and other associated security incident responsibilities.

Management Comments in Response to Recommendations 1 & 3:

The Mission concurs with Recommendations 1 and 3, and in response to the OIG's previous audit concerning management of contracts and grants such that implementing partners provided adequate oversight of Private Security Contractors (PSC), USAID issued Mission Notice 09-03-001 dated March 15, 2009 (Tab B) establishing procedures for the reporting of incidents by PSCs.

Among these procedures was the establishment of a special requirement on the reporting of Serious Incidents (SI) included via administrative modification in all Mission awards.

To facilitate more efficient and effective implementation of the procedures for monitoring the reporting of serious incidents and maintaining records of the Serious Incident Reports (SIR), USAID has revised the language of the SIR clause as reproduced verbatim below and will include it in all Mission award documents.

H.XX SERIOUS INCIDENT REPORTING

Definitions:

Private Security Contractor (PSC): A private company, and or its personnel that provides physical protection to or security for persons, places, buildings, facilities, supplies, or means of transportation.

Contractors Operations Cell (CONOC): United States Forces-Iraq (USF-I) operated coordination center for all PSCs supporting/protecting USG funded operations in Iraq, and all follow-on entities performing the same function.

Protective Security Specialist (PSS): An individual performing static or mobile security functions on a personnel protective security detail assignment, as authorized by contract.

Protective Security Detail (PSD): A team of PSS personnel that provides physical protective services for the movement of protected persons and/or property.

Static Guards: An individual who is providing security at facilities and/or check-points.

Serious Incident (SI): An incident involving the use of deadly force, the discharge of a weapon (other than in training or into a clearing barrel) by a PSS or against a PSS, use of non-lethal countermeasures by a PSS, and/or an incident that resulted in death, serious injury, significant property damage (even if a weapon is not involved), or other serious consequences.

Serious Incident Report (SIR): A comprehensive, formal written report of the events surrounding a SI. This report will document the SI based upon the notification and initial written incident report provided to the CONOC and any follow-up investigation.

Reporting Requirements:

The following reporting requirements apply to all PSCs (including static guards). The Prime contractor shall establish policies and procedures to ensure that:

- (1) All PSD movements shall be coordinated through the United States Forces – Iraq (USF-I) Contractor Operations Cell (CONOC), or any successor entity.
- (2) The Prime contractor's PSCs provide *notification*, either verbal or in writing via email, of any serious incident to the CONOC and the Prime – as soon as practical, but not later than one hour after the incident. This notification must provide as many details about the incident, as possible. PSCs must submit an *initial written incident report* within 4 hours of the incident to the CONOC and the Prime. The initial written report shall include the name of the company, where the incident occurred, the time when the incident occurred, a brief description of the events leading up to the incident, and a point of contact for the company.
- (3) As soon as practical after the Prime is aware of a serious incident, but not later than one hour after receiving the initial verbal or written report from the PSC or PSD, the Prime shall inform the cognizant Contracting Officer's Technical Representative (COTR) or Agreement Officer's Technical Representative (AOTR) of the incident verbally followed by a confirming email to both. The Prime will send the PSC's initial written incident report to the COTR or AOTR immediately upon receipt by the Prime.
- (4) The Prime shall verify in the contract file that the initial (1 hour) notification and the initial written incident report (4 hour) are appropriately disseminated to the CONOC (as specified above) and sent to the COTR or AOTR as specified above.
- (5) The SIR shall be provided with confirmed receipt to the CONOC and COTR or AOTR within 96 hours. All further follow-up reports produced by the PSC will likewise be submitted as soon as received with confirmed receipt to the CONOC and to the COTR or AOTR.
- (6) The SIRs received are reviewed by the Prime to determine whether they reveal any special vulnerability or other conditions that require adjustment in project implementation or other implications for the security of personnel and/or property. All vulnerabilities identified shall be discussed with USAID and the PSC. This process shall be documented in the contract file of the Prime and copied to the COTR or AOTR.
- (7) All SIRs and associated documentation shall be maintained by the Prime in the contract file for the life of the project. The prime shall also produce and maintain as a separate comprehensive document a complete, accurate and up to date inventory of all SIRs during the life of the project. The Prime shall make this file available to U.S. Government investigators and/or auditors upon request.
- (8) All incident reports will generally be reviewed by the Regional Security Office

(RSO) and a follow-up investigation will be conducted by the RSO Force Investigations Unit (FIU) if required. The FIU will notify the prime, either directly or through the COTR, AOTR or the Contracting/Agreement Officer, of their need to conduct a full investigation as soon as that determination is made.

(9) All sub-awardees are familiar with and comply with this provision (H.XX), all relevant Chief of Mission and US Military policies, rules and requirements, all additional USAID requirements and applicable Iraqi law.

Based upon the foregoing, USAID/Iraq requests OIG/Iraq's concurrence that final action has been taken on Recommendations 1 & 3.

Management Comments in Response to Recommendation 2:

The Mission concurs with Recommendation 2. The Mission will use the quarterly partner meetings as the forum to provide information and guidance on the implementation of the requirements contained in the "Serious Incident Reporting" clause set forth above. The meetings will also be used to review the procedures for maintaining and reporting SIs and to identify partner security concerns in order to discuss ways to counter vulnerabilities that may be shared by more than one partner. Additionally, this will serve a compliance monitoring function by verifying that partners are keeping SIR records in the manner prescribed, that communication between the PSCs, CONOC, PRIME and COTR/AOTR has been conducted as prescribed, and that each partner has taken corrective action as appropriate.

Based upon the foregoing, USAID/Iraq requests OIG/Iraq's concurrence that final action has been taken on Recommendation 2.

Management Comments in Response to Recommendation 4:

The Mission concurs with Recommendation 4. Mission Notice 09-03-001 establishes the responsibilities of COTR/AOTRs regarding receiving, reviewing and forwarding SIRs to the designated USAID/Iraq mailbox. Furthermore, the COTR/AOTR Designation Letters issued by the Contracting Officer for each of the Mission's awards include a specific section on how COTRs/AOTRs are to handle review, reporting and distribution of SIRs, which mirrors the procedures established in the Mission Notice. By signing the Designation Letter, the COTRs/AOTRs acknowledge and take responsibility for following those procedures. As an additional measure to reinforce COTR/AOTR knowledge, in July 2010, USAID/Iraq added a mandatory briefing with OAA to the Mission's check-in process for COTR/AOTRs. This briefing includes detailed review of the SIR reporting procedure and a reminder of their delegated responsibilities in that regard.

Based upon the foregoing, USAID/Iraq requests OIG/Iraq's concurrence that final action has been taken on Recommendation 4.

List of 94 Serious Security Incidents				
No.	Date of Incident	Contractor/ Subcontractor	Description of Incident	Injury or Damage
1	7/30/2007	Research Triangle Institute-Unity Resources Group (RTI-URG)	Flare shots	No
2	8/5/2007	RTI-URG	Weapon discharge	Yes
3	8/6/2007	RTI-URG	Warning shot	No
4	8/7/2007	RTI-URG	Weapon discharge	No
5	8/7/2007	RTI-URG	Indirect-fire attack	No
6	8/13/2007	RTI-URG	Accidental discharge	Yes
7	8/31/2007	RTI-URG	Theft of weapon	No
8	9/7/2007	RTI-URG	Weapon discharge	No
9	9/8/2007	RTI-URG	Vehicle hijacking	No
10	9/9/2007	RTI-URG	Weapon discharge	Yes
11	9/14/2007	RTI-URG	Vehicle accident	No
12	9/24/2007	RTI-URG	Warning shots	No
13	10/9/2007	RTI-URG	Weapon discharge	Yes
14	11/13/2007	RTI-URG	Improvised explosive device	No
15	11/17/2007	RTI-URG	Improvised explosive device	No
16	11/29/2007	RTI-URG	Negligent discharge	No
17	12/23/2007	RTI-URG	Warning shots	No
18	12/27/2007	RTI-URG	Warning shot	No
19	1/7/2008	RTI-URG	Vehicle accident	No
20	1/16/2008	RTI-URG	Vehicle accident	No
21	1/29/2008	RTI-URG	Warning shot	No
22	1/29/2008	RTI-URG	Warning shot	No
23	1/31/2008	RTI-URG	Warning shots	No
24	2/13/2008	RTI-URG	Flare and warning shots	No
25	2/16/2008	RTI-URG	Warning shot	No
26	2/29/2008	RTI-URG	Collision with parked car	No
27	3/17/2008	RTI-URG	Warning shots	No
28	3/24/2008	RTI-URG	Warning Shots	No
29	3/27/2008	RTI-URG	Improvised explosive device	Yes
30	3/28/2008	RTI-URG	Gunfight exchange	Unknown
31	4/10/2008	RTI-URG	Warning shot	No
32	4/12/2008	RTI-URG	Nonbattle off-duty injury	Yes
33	5/20/2008	RTI-URG	Flare shots	No
34	6/10/2008	RTI-URG	Stray bullet	No
35	9/12/2008	RTI-URG	Negligent discharge	No
36	12/11/2008	RTI-URG	Accidental discharge	No
37	1/3/2008	RTI-URG	Flare shot	No
38	10/2/2008	RTI-URG	Flare shots	No
39	10/6/2008	RTI-URG	Traffic accident	No
40	12/1/2008	RTI-URG	Traffic accident	No

List of 94 Serious Security Incidents				
No.	Date of Incident	Contractor/ Subcontractor	Description of Incident	Injury or Damage
41	4/16/2009	Research Triangle Institute-Armor Group	Warning shot	No
42	5/14/2009	Research Triangle Institute-Armor Group	Explosive formed projectile attack	Yes
43	6/14/2009	Research Triangle Institute-Armor Group	Disabling shot	No
44	7/16/2007	International Relief Development-Sabre International Security (IRD-Sabre)	Celebrative shooting spree	No
45	11/14/2007	IRD-Sabre	Gunfight exchange	Yes
46	12/9/2007	IRD-Sabre	Weapon discharge	No
47	12/16/2007	IRD/Sabre	Victim-detonated improvised explosive device	Yes
48	2/19/2008	IRD-Sabre	Rocket-missile attack	No
49	3/8/2008	IRD-Sabre	Negligent discharge	Yes
50	3/19/2008	IRD-Sabre	Negligent discharge	Yes
51	3/24/2008	IRD-Sabre	Rollover accident	Yes
52	4/15/2008	IRD-Sabre	Vehicle-borne improvised explosive device	Unknown
53	6/30/2008	IRD-Sabre	Armed robbery	No
54	8/6/2008	IRD-Sabre	Vehicle accident	Yes
55	10/7/2008	IRD-Sabre	Armed robbery	Yes
56	10/8/2008	IRD-Sabre	Victim-detonated improvised explosive device	Yes
57	10/20/2008	IRD-Sabre	Malfunctioning weapon discharge	No
58	11/3/2008	IRD-Sabre	Improvised explosive device	No
59	11/23/2008	IRD-Sabre	Improvised explosive device	No
60	12/12/2008	IRD-Sabre	Stray-projectile injury	Yes
61	1/14/2009	IRD-Sabre	Small-arms fire	No
62	1/17/2009	IRD-Sabre	Unexploded ordnance under car	No
63	1/29/2009	IRD-Sabre	Small-arms-fire exchange	Yes
64	2/5/2009	IRD-Sabre	Small-arms fire	No
65	2/10/2009	IRD-Sabre	Vehicle accident	No
66	2/27/2009	IRD-Sabre	Vehicle accident	Yes
67	3/9/2009	IRD-Sabre	Indirect-fire attack	No
68	3/19/2009	IRD-Sabre	Collision with pedestrian	Yes
69	4/3/2009	IRD-Sabre	Traffic accident	No
70	5/25/2009	IRD-Sabre	Weapon discharge	No
71	6/10/2009	IRD-Sabre	Iraqi Army traffic control incident	No
72	6/10/2009	IRD-Sabre	Traffic incident	Yes
73	9/28/2007	Louis Berger Group-SallyPort Global Services (LBG-SallyPort)	Guard abduction	No
74	11/12/2007	LBG-SallyPort	Warning shot	No
75	11/27/2007	LBG-SallyPort	Assassination	Yes
76	12/30/2007	LBG-SallyPort	Warning shots	No

List of 94 Serious Security Incidents				
No.	Date of Incident	Contractor/ Subcontractor	Description of Incident	Injury or Damage
77	2/14/2008	LBG-SallyPort	Warning shots	No
78	4/16/2008	Louis Berger Group-SallyPort Global Services (LBG-SallyPort)	Warning shot	No
79	7/20/2008	LBG-SallyPort	Collision accident	No
80	8/3/2008	LBG-SallyPort	Flare shot	No
81	7/25/2007	Management Systems International-SallyPort Global Services (MSI-SallyPort)	Vehicle-borne improvised explosive device	Yes
82	9/16/2007	MSI-SallyPort	Vehicle-borne improvised explosive device	No
83	9/27/2007	MSI-SallyPort	Guard abduction	No
84	3/16/2008	MSI-SallyPort	Vehicle-borne improvised explosive device	No
85	8/27/2008	MSI-SallyPort	Collision accident	Yes
86	9/22/2008	MSI-SallyPort	Collision accident	No
87	4/20/2009	MSI-SallyPort	Improvised explosive device	No
88	2/3/2009	Cooperative Housing Foundation-Unity Resources Group	Improvised explosive device attack	Yes
89	3/11/2009	Cooperative Housing Foundation-Unity Resources Group	Improvised explosive device attack	No
90	3/3/2009	Relief International-Triple Canopy	Improvised explosive device	Yes
91	4/5/2009	Relief International-Triple Canopy	Improvised explosive device	Yes
92	3/19/2009	AECOM International Development-SallyPort	Iraqi Army traffic control incident	No
93	5/4/2008	BearingPoint-Garda World	Rocket attack	Yes
94	6/23/2009	Development Alternatives International-Garda World	Death threat	No

Key Statutory Requirements in Sections 862 and 864 of the National Defense Authorization Act for Fiscal Year 2008, as Amended

Sec. 862. Contractors performing private security functions in areas of combat operations.¹

(a) Regulations on contractors performing private security functions.--

(1) In general.—Not later than 120 days after the date of the enactment of this Act [Jan. 28, 2008], the Secretary of Defense, in coordination with the Secretary of State, shall prescribe regulations on the selection, training, equipping, and conduct of personnel performing private security functions under a covered contract in an area of combat operations.

(2) Elements.—The regulations prescribed under subsection (a) shall, at a minimum, establish—

(A) a process for registering, processing, accounting for, and keeping appropriate records of personnel performing private security functions in an area of combat operations;

(B) a process for authorizing and accounting for weapons to be carried by, or available to be used by, personnel performing private security functions in an area of combat operations;

(C) a process for the registration and identification of armored vehicles, helicopters, and other military vehicles operated by contractors performing private security functions in an area of combat operations;

(D) A process under which contractors are required to report all incidents, and persons other than contractors are permitted to report incidents, in which—

(i) a weapon is discharged by personnel performing private security functions in an area of combat operations;

(ii) personnel performing private security functions in an area of combat operations are killed or injured;

¹ Public Law 110-181, div. A, title VIII, subtitle F, §§ 862 and 864, Jan. 28, 2008, 122 Stat. 254-259; as amended by Public Law 110-417, div. A, title VIII, §§ 853, 854(a), (d), Oct. 14, 2008, 122 Stat. 4544; and Public Law 111-84, div. A, title VIII, § 813(a) to (c), Oct. 28, 2009, 123 Stat. 2406. Codified at 10 U.S.C. 2302 note.

(iii) persons are killed or injured, or property is destroyed, as a result of conduct by contractor personnel;

(iv) a weapon is discharged against personnel performing private security functions in an area of combat operations or personnel performing such functions believe a weapon was so discharged; or

(v) active, non-lethal countermeasures (other than the discharge of a weapon) are employed by the personnel performing private security functions in an area of combat operations in response to a perceived immediate threat to such personnel;

(E) A process for the independent review and, if practicable, investigation of—

(i) incidents reported pursuant to subparagraph (D); and

(ii) incidents of alleged misconduct by personnel performing private security functions in an area of combat operations;

(F) requirements for qualification, training, screening (including, if practicable, through background checks), and security for personnel performing private security functions in an area of combat operations;

(G) Guidance to the commanders of the combatant commands on the issuance of—

(i) orders, directives, and instructions to contractors performing private security functions relating to equipment, force protection, security, health, safety, or relations and interaction with locals;

(ii) predeployment training requirements for personnel performing private security functions in an area of combat operations, addressing the requirements of this section, resources and assistance available to contractor personnel, country information and cultural training, and guidance on working with host country nationals and military; and

(iii) rules on the use of force for personnel performing private security functions in an area of combat operations;

(H) a process by which a commander of a combatant command may request an action described in subsection (b)(3); and

(I) a process by which the training requirements referred to in subparagraph (G)(ii) shall be implemented.

(3) Availability of orders, directives, and instructions.—The regulations prescribed under subsection (a) shall include mechanisms to ensure the provision and availability of the orders, directives, and instructions referred to in paragraph (2)(G)(i) to contractors referred to in that paragraph, including through the maintenance of a single location (including an Internet website, to the extent consistent with security considerations) at or through which such contractors may access such orders, directives, and instructions.

(b) Contract clause on contractors performing private security functions.—

(1) Requirement under FAR.—Not later than 180 days after the date of the enactment of this Act [Jan. 28, 2008], the Federal Acquisition Regulation issued in accordance with section 25 of the Office of Federal Procurement Policy Act (41 U.S.C. 421) shall be revised to require the insertion into each covered contract (or, in the case of a task order, the contract under which the task order is issued) of a contract clause addressing the selection, training, equipping, and conduct of personnel performing private security functions under such contract.

(2) Clause requirement.—The contract clause required by paragraph (1) shall require, at a minimum, that the contractor concerned shall—

(A) Comply with regulations prescribed under subsection (a) [of this note], including any revisions or updates to such regulations, and follow the procedures established in such regulations for—

(i) registering, processing, accounting for, and keeping appropriate records of personnel performing private security functions in an area of combat operations;

(ii) authorizing and accounting of weapons to be carried by, or available to be used by, personnel performing private security functions in an area of combat operations;

(iii) registration and identification of armored vehicles, helicopters, and other military vehicles operated by contractors and subcontractors performing private security functions in an area of combat operations; and

(iv) The reporting of incidents in which—

(I) a weapon is discharged by personnel performing private security functions in an area of combat operations;

(II) personnel performing private security functions in an area of combat operations are killed or injured; or

(III) persons are killed or injured, or property is destroyed, as a result of conduct by contractor personnel;

(B) Comply with and ensure that all personnel performing private security functions under such contract are briefed on and understand their obligation to act in accordance with—

(i) qualification, training, screening (including, if practicable, through background checks), and security requirements established by the Secretary of Defense for personnel performing private security functions in an area of combat operations;

(ii) applicable laws and regulations of the United States and the host country, and applicable treaties and international agreements, regarding the performance of the functions of the contractor;

(iii) orders, directives, and instructions issued by the applicable commander of a

combatant command relating to equipment, force protection, security, health, safety, or relations and interaction with locals; and

(iv) rules on the use of force issued by the applicable commander of a combatant command for personnel performing private security functions in an area of combat operations; and

(C) cooperate with any investigation conducted by the Department of Defense pursuant to subsection (a)(2)(E) by providing access to employees of the contractor and relevant information in the possession of the contractor regarding the incident concerned.

(3) Noncompliance of personnel with clause.—The contracting officer for a covered contract may direct the contractor, at its own expense, to remove or replace any personnel performing private security functions in an area of combat operations who violate or fail to comply with applicable requirements of the clause required by this subsection. If the violation or failure to comply is a gross violation or failure or is repeated, the contract may be terminated for default.

(4) Applicability.—The contract clause required by this subsection shall be included in all covered contracts awarded on or after the date that is 180 days after the date of the enactment of this Act [Jan. 28, 2008]. Federal agencies shall make best efforts to provide for the inclusion of the contract clause required by this subsection in covered contracts awarded before such date.

(5) Inspector General report on pilot program on imposition of fines for noncompliance of personnel with clause.—Not later than March 30, 2008, the Inspector General of the Department of Defense shall [...deleted for the purposes of this appendix]

(c) Areas of combat operations.—

(1) Designation.—The Secretary of Defense shall designate the areas constituting an area of combat operations for purposes of this section by not later than 120 days after the date of the enactment of this Act [Jan. 28, 2008].

(2) Particular areas.—Iraq and Afghanistan shall be included in the areas designated as an area of combat operations under paragraph (1).

(3) Additional areas.—The Secretary may designate any additional area as an area constituting an area of combat operations for purposes of this section if the Secretary determines that the presence or potential of combat operations in such area warrants designation of such area as an area of combat operations for purposes of this section.

(4) Modification or elimination of designation.—The Secretary may modify or cease the designation of an area under this subsection as an area of combat operations if the Secretary determines that combat operations are no longer ongoing in such area.

(d) Exception.—The requirements of this section shall not apply to contracts entered into by elements of the intelligence community in support of intelligence activities.

Sec. 864. Definitions and other general provisions.

(a) Definitions.—In this subtitle [this note]:

(1) Matters relating to contracting.—The term ‘matters relating to contracting’, with respect to contracts in Iraq and Afghanistan, means all matters relating to awarding, funding, managing, tracking, monitoring, and providing oversight to contracts and contractor personnel.

(2) Contract in Iraq or Afghanistan.—The term ‘contract in Iraq or Afghanistan’ means a contract with the Department of Defense, the Department of State, or the United States Agency for International Development, a subcontract at any tier issued under such a contract, a task order or delivery order at any tier issued under such a contract, a grant, or a cooperative agreement (including a contract, subcontract, task order, delivery order, grant, or cooperative agreement issued by another Government agency for the Department of Defense, the Department of State, or the United States Agency for International Development), if the contract, subcontract, task order, delivery order, grant, or cooperative agreement involves work performed in Iraq or Afghanistan for a period longer than 30 days.

(3) Covered contract.—The term ‘covered contract’ means—

(A) a contract of a Federal agency for the performance of services in an area of combat operations, as designated by the Secretary of Defense under subsection (c) of section 862 [of this note];

(B) a subcontract at any tier under such a contract;

(C) a task order or delivery order issued under such a contract or subcontract;

(D) a grant for the performance of services in an area of combat operations, as designated by the Secretary of Defense under subsection (c) of section 862 [of this note]; or

(E) a cooperative agreement for the performance of services in such an area of combat operations.

(4) Contractor.—The term ‘contractor’, with respect to a covered contract, means—

(A) in the case of a covered contract that is a contract, subcontract, task order, or delivery order, the contractor or subcontractor carrying out the covered contract;

(B) in the case of a covered contract that is a grant, the grantee; and

(C) in the case of a covered contract that is a cooperative agreement, the recipient.

(5) Contractor personnel.—The term ‘contractor personnel’ means any person performing work under contract for the Department of Defense, the Department of State, or the United States Agency for International Development, in Iraq or Afghanistan, including individuals and subcontractors at any tier.

(6) Private security functions.—The term ‘private security functions’ means activities engaged in by a contractor under a covered contract as follows:

(A) Guarding of personnel, facilities, or property of a Federal agency, the contractor or subcontractor, or a third party.

(B) Any other activity for which personnel are required to carry weapons in the performance of their duties.

(7) Relevant committees of Congress.—The term ‘relevant committees of Congress’ means each of the following committees:

(A) The Committees on Armed Services of the Senate and the House of Representatives.

(B) The Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Government Reform of the House of Representatives.

(C) The Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(D) For purposes of contracts relating to the National Foreign Intelligence Program, the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

(b) Classified information.—Nothing in this subtitle [this note] shall be interpreted to require the handling of classified information or information relating to intelligence sources and methods in a manner inconsistent with any law, regulation, executive order, or rule of the House of Representatives or of the Senate relating to the handling or protection of such information.”

Federal Register / Vol. 74, No. 136 / Friday, July 17, 2009 / Rules and Regulations (Interim Final Rule, 32 CFR Part 159)

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 159

[DOD–2008–OS–0125/RIN 0790–AI38]

Private Security Contractors (PSCs) Operating in Contingency Operations**AGENCY:** Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, DoD.**ACTION:** Interim final rule.

SUMMARY: This part establishes policy, assigns responsibilities and provides procedures for the regulation of the selection, accountability, training, equipping, and conduct of personnel performing private security functions under a covered contract during contingency operations. It also assigns responsibilities and establishes procedures for incident reporting, use of and accountability for equipment, rules for the use of force, and a process for administrative action or the removal, as appropriate, of PSCs and PSC personnel. For the Department of Defense, this IFR supplements DoD Instruction 3020.41, “Contractor Personnel Authorized to Accompany the U.S. Armed Forces,” which provides guidance for all DoD contractors operating in contingency operations.

This part is of critical importance. It is being published as an Interim Final Rule because there is insufficient policy and guidance regulating the actions of DoD and other governmental PSCs and their movements in the operational area. It will procedurally close existing gaps in the oversight of Private Security Contractors (PSCs), ensure compliance with laws and regulations pertaining to Inherently Governmental functions, and ensure proper performance by armed contractors. The expansion of troops in Afghanistan will result in a corresponding increase in the number of PSCs performing in that Area of Operations. This part is required to ensure implementation of necessary guidance for all U.S.G. PSCs across the CENTCOM area of responsibility. Further, the publication of this IFR is required to meet the mandate of Section 862 of the 2008 National Defense Authorization Act. The Congress has expressed continuing concern that regulations for the oversight of PSCs are not yet in place.

DATES: This rule is effective July 17, 2009. Comments must be received by August 31, 2009.

ADDRESSES: You may submit comments, identified by docket number and/or RIN

number and title, by any of the following methods:

- *Federal Rulemaking Portal:* [http:// www.regulations.gov](http://www.regulations.gov). Follow the instructions for submitting comments.
- *Mail:* Federal Docket Management System Office, 1160 Defense Pentagon, Washington, DC 20301–1160.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Jeffrey Taylor, (703) 692–3032.

SUPPLEMENTARY INFORMATION: This Interim Final Rule is required to meet the mandate of Section 862 of the FY 2008 National Defense Authorization Act. Section 862 of the 2008 NDAA lays out two requirements:

- (i) That the Secretary of Defense, in coordination with the Secretary of State shall prescribe regulations on the selection, training, equipping, and conduct of personnel performing private security functions under a covered contract in an area of combat operations; and
- (ii) That the FAR shall be revised to require the insertion into each covered contract of a contract clause addressing the selection, training, equipping, and conduct of personnel performing private security functions under such contract.

This Interim Final Rule meets requirement (i). There will be a separate and subsequent **Federal Register** action to meet requirement (ii) to update the FAR.

Executive Order 12866, “Regulatory Planning and Review”

It has been certified that 32 CFR part 159 does not:

- (1) Have an annual effect on the economy of \$100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities;
- (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency;
- (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or
- (4) Raise novel legal or policy issues arising out of legal mandates, the President’s priorities, or the principles set forth in this Executive Order.

Public Law 104–121, “Congressional Review Act” (5 U.S.C. 801)

It has been determined that 32 CFR part 159 is not a “major” rule under 5 U.S.C. 801, enacted by Public Law 104– 121, because it will not result in an annual effect on the economy of \$100 million or more; a major increase in costs or prices for consumers, individual industries, Federal, State, or local government agencies, or geographic regions; or significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of United States-based enterprises to compete with foreign-based enterprises in domestic and export markets.

Section 202, Public Law 104–4, “Unfunded Mandates Reform Act”

It has been certified that 32 CFR part 159 does not contain a Federal mandate that may result in expenditure by State, local and tribal governments, in aggregate, or by the private sector, of \$100 million or more in any one year.

Public Law 96–354, “Regulatory Flexibility Act” (5 U.S.C. 601)

It has been certified that 32 CFR part 159 is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities. This rule will apply only to a specific sector of defense industry and a limited number of small entities.

Public Law 96–511, “Paperwork Reduction Act” (44 U.S.C. Chapter 35)

It has been certified that 32 CFR part 159 does impose reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995. These requirements have been approved by OMB and assigned OMB Control Numbers 0704–0460, “Synchronized Predeployment and Operational Tracker (SPOT) System” and 0704–0461, “Qualification to Possess Firearms or Ammunition.”

Executive Order 13132, “Federalism”

It has been certified that 32 CFR part 159 does not have federalism implications, as set forth in Executive Order 13132. This rule does not have substantial direct effects on:

- (1) The States;
- (2) The relationship between the National Government and the States; or
- (3) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 159

Contracts, Security measures.

■ Accordingly 32 CFR Part 159 is added to read as follows:

PART 159—PRIVATE SECURITY CONTRACTORS OPERATING IN CONTINGENCY OPERATIONS

Sec.

159.1 Purpose.

159.2 Applicability and scope.

159.3 Definitions.

159.4 Policy.

159.5 Responsibilities.

159.6 Procedures.

Authority: Public Law 110–181; Pub. L. 110–417.

§ 159.1. Purpose.

This part establishes policy, assigns responsibilities and provides procedures for the regulation of the selection, accountability, training, equipping, and conduct of personnel performing private security functions under a covered contract. It also assigns responsibilities and establishes procedures for incident reporting, use of and accountability for equipment, rules for the use of force, and a process for administrative action or the removal, as appropriate, of PSCs and PSC personnel.

§ 159.2. Applicability and scope.

This part:

(a) Applies to:

(1) The Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to as the “DoD Components”).

(2) The Department of State and other Federal agencies insofar as it implements the requirements of section 862 of Public Law 110–181. Specifically, in areas of operations which require enhanced coordination of PSC and PSC personnel working for Government (U.S.G.) agencies, the Secretary of Defense may designate such areas as areas of combat operations for the limited purposes of this part. In such an instance, the standards established in accordance with this part would, in coordination with the Secretary of State, expand from covering only DoD PSCs and PSC personnel to cover all U.S.G.-funded PSCs and PSC personnel operating in the designated area.

(b) Prescribes policies applicable to all:

(1) DoD PSCs and PSC personnel performing private security functions during contingency operations outside the United States.

(2) USG-funded PSCs and PSC personnel performing private security functions in an area of combat operations, as designated by the Secretary of Defense.

§ 159.3. Definitions.

Unless otherwise noted, these terms and their definitions are for the purpose of this part.

Area of combat operations. An area of operations designated as such by the Secretary of Defense for the purpose of this part, when enhanced coordination of PSCs working for U.S.G. agencies is required.

Contingency operation. A military operation that is either designated by the Secretary of Defense as a contingency operation or becomes a contingency operation as a matter of law (10 U.S.C. 101(a)(13)). It is a military operation that: a. Is designated by the Secretary of Defense as an operation in which members of the Armed Forces are or may become involved in military actions, operations, or hostilities against an enemy of the United States or against an opposing force; or b. Is created by definition of law. Under 10 U.S.C. 101(a)(13)(B), a contingency operation exists if a military operation results in the (1) call-up to (or retention on) active duty of members of the uniformed Services under certain enumerated statutes (10 U.S.C. 688, 12301(a), 12302, 12304, 12305, 12406, or 331–335); and (2) the call-up to (or retention on) active duty of members of the uniformed Services under any other (non-enumerated) provision of law during war or national emergency declared by the President or Congress. These may include humanitarian or peacekeeping operations or other military operations or exercises.

Contractor. The contractor, subcontractor, grantee, or other party carrying out the covered contract.

Covered contract. A DoD contract for performance of services in an area of contingency operations or a contract of a non-DoD Federal agency for performance of services in an area of combat operations, as designated by the Secretary of Defense; A subcontract at any tier under such a contract; or

A task order or delivery order issued under such a contract or subcontract.

Also includes contracts or subcontracts funded under grants and sub-grants by a Federal agency for performance in an area of combat operations as designated by the Secretary of Defense. Excludes temporary arrangements entered into by non-DoD contractors or grantees for the performance of private security functions by individual indigenous personnel not affiliated with a local or expatriate security company. Such arrangements must still be in compliance with local law.

Private security functions. Activities engaged in by a contractor under a covered contract as follows:

(1) Guarding of personnel, facilities, designated sites, or property of a Federal agency, the contractor or subcontractor, or a third party.¹

(2) Any other activity for which personnel are required to carry weapons in the performance of their duties. For the DoD, DoDI Instruction 3020.41, "Contractor Personnel Authorized to Accompany the U.S. Armed Forces,"² prescribes policies related to personnel allowed to carry weapons for self defense.

PSC. During contingency operations "PSC" means a company employed by the DoD performing private security functions under a covered contract. In a designated area of combat operations, the term "PSC" expands to include all companies employed by U.S.G. agencies performing private security functions under a covered contract.

PSC personnel. Any individual performing private security functions under a covered contract.

§ 159.4. Policy.

(a) Consistent with the requirements of paragraph (a)(2) of section 862 of Public Law 110–181, the selection, training, equipping, and conduct of PSC personnel including the establishment of appropriate processes shall be coordinated between the DoD and the Department of State.

(b) Geographic Combatant Commanders will provide tailored PSC guidance and procedures for the operational environment in their Area of Responsibility (AOR) in accordance with this part, the Federal Acquisition Regulation (FAR)³ and the Defense Federal Acquisition Regulation Supplement (DFARS).⁴

(c) In a designated area of combat operations, the relevant Chief of Mission will be responsible for developing and issuing implementing instructions for non-DoD PSCs and their personnel consistent with the standards set forth by the geographic Combatant Commander in accordance with paragraph (b) of this section. The Chief of Mission has the option to instruct non DoD PSCs and their personnel to follow the guidance and procedures developed by the Geographic Combatant Commander and/or Subordinate Commander.

(d) The requirements of this part shall not apply to contracts entered into by elements of the intelligence community in support of intelligence activities.

§ 159.5. Responsibilities.

¹ Contractors performing private security functions are not authorized to perform inherently governmental functions. In this regard, they are limited to a defensive response to hostile acts or demonstrated hostile intent.

² Available at <http://www.dtic.mil/whs/directives/corres/pdf/302041p.pdf>.

³ Published in Title 48 of the Code of Federal Regulations.

⁴ Published in Title 48 of the Code of Federal Regulations.

(a) The Assistant Deputy Under Secretary of Defense for Program Support, under the authority, direction, and control of the Deputy Under Secretary of Defense for Logistics and Materiel Readiness, shall monitor the registering, processing, and accounting of PSC personnel in an area of contingency operations.

(b) The Director, Defense Procurement and Acquisition Policy, under the authority, direction, and control of the Deputy Under Secretary of Defense for Acquisition and Technology (DUSD(AT)), shall ensure that the DFARS and (in consultation with the other members of the FAR Council) the FAR provide appropriate guidance and contract clauses consistent with this part and paragraph (b) of section 862 of Public Law 110-181.

(c) The Director, Defense Business Transformation Agency, under the authority, direction, and control of the Deputy Chief Management Officer of the Department of Defense, through the DUSD(AT), shall ensure that information systems effectively support the accountability and visibility of contracts, contractors, and specified equipment associated with private security functions.

(d) The Chairman of the Joint Chiefs of Staff shall ensure that joint doctrine is consistent with the principles established by DoD Directive 3020.49 “Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution,”⁵ DoD Instruction 3020.41, “Contractor Personnel Authorized to Accompany the U.S. Armed Forces,” and this part.

(e) The geographic Combatant Commanders in whose AOR a contingency operation is occurring, and within which PSCs and PSC personnel perform under covered contracts, shall:

(1) Provide guidance and procedures, as necessary and consistent with the principles established by DoD Directive 3020.49, “Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution,” DoD Instruction 3020.41, “Contractor Personnel Authorized to Accompany the U.S. Armed Forces,”⁶ and this part, for the selection, training, accountability and equipping of such PSC personnel and the conduct of PSCs and PSC personnel within their AOR. Individual training and qualification standards shall meet, at a minimum, one of the Military Departments’ established standards. Within a geographic Combatant Command, Subordinate Commanders shall be responsible for developing and issuing implementing procedures as warranted by the situation, operation, and environment, in consultation with the relevant Chief of Mission in designated areas of combat operations.

(2) Through the Contracting Officer, ensure that PSC personnel acknowledge, through their PSC, their understanding and obligation to comply with the terms and conditions of their covered contracts.

(3) Issue written authorization to the PSC identifying individual PSC personnel who are authorized to be armed. Rules for the use of force, developed in accordance with Chairman of the Joint Chief of Staff Instruction 3121.01B, “Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces,”⁷ shall be included with the written authorization.

⁵ Available from <http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf>.

⁶ Available from <http://www.dtic.mil/whs/directives/corres/html/302041.htm>.

⁷ CJCSI 3121.01B provides guidance on the standing rules of engagement (SROE) and establishes standing rules for the use of force (SRUF) for DOD operations worldwide. This document is classified secret. CJCSI 3121.01B is available via Secure Internet Protocol Router Network at <http://js.smil.mil> If the requester is not an authorized user of the classified network, the requester should contact Joint Staff J-3 at 703-614-0425.

(4) Ensure that the procedures, orders, directives and instructions prescribed § 159.6(a) of this part are available through a single location (to include an Internet Web site, consistent with security considerations and requirements).

(f) The Heads of the DoD Components shall:

(1) Ensure that all private security-related requirement documents are in compliance with the procedures listed in § 159.6 of this part and the guidance and procedures issued by the geographic Combatant Command,

(2) Ensure private security-related contracts contain the appropriate clauses in accordance with the applicable FAR clause and include additional mission-specific requirements as appropriate.

§ 159.6. Procedures.

(a) *Standing Combatant Command Guidance and Procedures.* Each geographic Combatant Commander shall develop and publish guidance and procedures for PSCs and PSC personnel operating during a contingency operation within their AOR, consistent with applicable law; this part; applicable Military Department publications; and other applicable DoD issuances to include DoD Directive 3020.49, "Orchestrating, Synchronizing, and Integrating Program Management of Contingency Acquisition Planning and Its Operational Execution," DFARS, DoD Directive 2311.01E, "DoD Law of War Program,"⁸ DoD 5200.8-R, "Physical Security Program,"⁹ CJCSI 3121.01B, "Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces," and DoD Directive 5210.56, "Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties."¹⁰ The guidance and procedures shall:

(1) Contain, at a minimum, procedures to implement the following processes, and identify the organization responsible for managing these processes:

(i) Registering, processing, accounting for and keeping appropriate records of PSCs and PSC personnel in accordance with DoD Instruction 3020.41, "Contractor Personnel Authorized to Accompany the U.S. Armed Forces."

(ii) PSC verification that PSC personnel meet all the legal, training, and qualification requirements for authorization to carry a weapon in accordance with the terms and conditions of their contract and host country law. Weapons accountability procedures will be established and approved prior to the weapons authorization.

(iii) Arming of PSC personnel. Requests for permission to arm PSC personnel shall be reviewed on a case-by-case basis by the appropriate Staff Judge Advocate to the geographic Combatant Commander (or a designee) to ensure there is a legal basis for approval. The request will then be approved or denied by the geographic Combatant Commander or a specifically identified designee, no lower than the flag officer level. Requests to arm non-DOD PSC personnel shall be reviewed and approved in accordance with § 159.4(c) of this part. Requests for permission to arm PSC personnel shall include:

(A) A description of where PSC personnel will operate, the anticipated threat, and what property or personnel such personnel are intended to protect, if any.

⁸ Available at <http://www.dtic.mil/whs/directives/corres/html/231101.htm>.

⁹ Available at <http://www.dtic.mil/whs/directives/corres/pdf/520008r.pdf>.

¹⁰ Available at <http://www.dtic.mil/whs/directives/corres/html/521056.htm>.

(B) A description of how the movement of PSC personnel will be coordinated through areas of increased risk or planned or ongoing military operations, including how PSC personnel will be rapidly identified by members of the U.S. Armed Forces.

(C) A communication plan, to include a description of how relevant threat information will be shared between PSC personnel and U.S. military forces and how appropriate assistance will be provided to PSC personnel who become engaged in hostile situations. DoD contractors performing private security functions are only to be used in accordance with DoD Instruction 1100.22, "Guidance for Determining Workforce Mix,"¹¹ that is, they are limited to a defensive response to hostile acts or demonstrated hostile intent.

(D) Documentation of individual training covering weapons familiarization and qualification, rules for the use of force, limits on the use of force including whether defense of others is consistent with host nation Status of Forces Agreements or local law, the distinction between the rules of engagement applicable to military forces and the prescribed rules for the use of force that control the use of weapons by civilians, and the Law of Armed Conflict.

(E) Written acknowledgment by the PSC and its individual PSC personnel, after investigation of background of PSC personnel by the contractor, verifying such personnel are not prohibited under U.S. law to possess firearms.

(F) Written acknowledgment by the PSC and individual PSC personnel that:

(1) Potential civil and criminal liability exists under U.S. and local law or host nation Status of Forces Agreements for the use of weapons.¹²

(2) Proof of authorization to be armed must be carried by each PSC personnel.

(3) PSC personnel may possess only U.S.G.-issued and/or -approved weapons and ammunition for which they have been qualified according to paragraph (a)(1)(iii)(E) of this section.

(4) PSC personnel were briefed and understand limitations on the use of force.

(5) Authorization to possess weapons and ammunition may be revoked for non-compliance with established rules for the use of force.

(6) PSC personnel are prohibited from consuming alcoholic beverages or being under the influence of alcohol while armed.

(iv) Registration and identification in the Synchronized Predeployment and Operational Tracker (or its successor database) of armored vehicles, helicopters, and other vehicles operated by PSC personnel.

(v) Reporting alleged criminal activity or other incidents involving PSCs or PSC personnel by another company or any other person. All incidents involving the following shall be reported and documented:

(A) A weapon is discharged by an individual performing private security functions;

(B) An individual performing private security functions is killed or injured in the performance of their duties;

(C) A person other than an individual performing private security functions is killed or injured as a result of conduct by PSC personnel;

(D) Property is destroyed as a result of conduct by a PSC or PSC personnel;

(E) An individual performing private security functions has come under attack including in cases where a weapon is discharged against an individual performing private security

¹¹ Available at <http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf>.

¹² This requirement is specific to arming procedures. Such written acknowledgement should not be construed to limit civil and criminal liability to conduct arising from "the use of weapons." PSC personnel could be held criminally liable for any conduct that would constitute a federal offense (see MEJA, 18 USC 3261(a)).

functions or personnel performing such functions believe a weapon was so discharged;
or

(F) Active, non-lethal counter-measures (other than the discharge of a weapon) are employed by PSC personnel in response to a perceived immediate threat in an incident that could significantly affect U.S. objectives with regard to the military mission or international relations.

(vi) The independent review and, if practicable, investigation of incidents reported pursuant to paragraphs (a)(1)(v)(A) through (a)(1)(v)(F) of this section and incidents of alleged misconduct by PSC personnel.

(vii) Identification of ultimate criminal jurisdiction and investigative responsibilities, where conduct of U.S.G.-funded PSCs or PSC personnel are in question, in accordance with applicable laws to include a recognition of investigative jurisdiction and coordination for joint investigations (i.e., other U.S.G. agencies, host nation, or third country agencies), where the conduct of PSCs and PSC personnel is in question.

(viii) A mechanism by which a commander of a combatant command may request an action by which PSC personnel who are non-compliant with contract requirements are removed from the designated operational area.

(ix) Interagency coordination of administrative penalties or removal, as appropriate, of non-DoD PSC personnel who fail to comply with the terms and conditions of their contract, as is applicable to this part.

(x) Implementation of the training requirements contained below in paragraph (a)(2)(ii) of this section.

(2) Specifically cover:

(i) Matters relating to authorized equipment, force protection, security, health, safety, and relations and interaction with locals in accordance with DoD Instruction 3020.41, "Contractor Personnel Authorized to Accompany the U.S. Armed Forces."

(ii) Predeployment training requirements addressing, at a minimum, the identification of resources and assistance available to PSC personnel as well as country information and cultural training, and guidance on working with host country nationals and military personnel.

(iii) Rules for the use of force and graduated force procedures.

(iv) Requirements and procedures for direction, control and the maintenance of communications with regard to the movement and coordination of PSCs and PSC personnel, including specifying interoperability requirements. These include coordinating with the Chief of Mission, as necessary, private security operations outside secure bases and U.S. diplomatic properties to include movement control procedures for all contractors, including PSC personnel.

(b) *Availability of Guidance and Procedures.* The geographic Combatant Commander shall ensure the guidance and procedures prescribed in paragraph

(a) of this section are readily available and accessible by PSCs and their personnel (e.g., on a Web page and/or through contract terms), consistent with security considerations and requirements.

(c) *Subordinate Guidance and Procedures.* The Subordinate Commander, in consultation with the Chief of Mission, will issue guidance and procedures implementing the standing combatant command publications specified in paragraph (a) of this section, consistent with the situation and operating environment.

(d) *Consultation and Coordination.* The Chief of Mission and the geographic Combatant Commander/Subordinate Commander shall make every effort to consult and coordinate responses to common threats and common concerns related to oversight of the conduct of U.S.G.-funded PSC and their personnel. The Memorandum of Agreement between

the Department of Defense and Department of State on U.S.G. Private Security Contractors¹³ shall provide the framework for the development of guidance and procedures without regard to the specific locations identified therein.

Dated: July 14, 2009.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. E9-17059 Filed 7-16-09; 8:45 am]

BILLING CODE 5001-06-P

¹³ Available at http://www.acq.osd.mil/log/PS/p_vault.html.

U.S. Agency for International Development
Office of Inspector General
1300 Pennsylvania Avenue, NW
Washington, DC 20523
Tel.: 202-712-1150
Fax: 202-216-3047
www.usaid.gov/oig