ANNEX Q (OPERATIONS, PHYSICAL SECURITY AND FORCE PROTECTION) to LOGCAP CONTINGENCY SUPPORT PLAN

REFERENCES. See ANNEX N, Appendix 4.

TIME ZONE USED THROUGHOUT THE PLAN. Iraq.

TASK ORGANIZATION. See ANNEX A.

1. SITUATION. See Base PLAN.

a. General. BRS Security operates under the premise of threat avoidance through early detection, early warning, proper planning and education. This philosophy has been very successful for BRS as evidenced by the company experiencing no deaths or significant incidents due to hostile actions in the Balkans for approximately seven years of operations, or during LOGCAP I and III. This success is due to a multi-layered security approach that consists of identifying the threats to our personnel and operations, developing plans to accomplish the mission without overexposure to the threats, educating our employees to the threats and vulnerabilities, and by providing employee training to mitigate the threats. This proactive approach to security has proven successful in numerous operations and will continue be successful during future deployments. The purpose of this Security Annex is to establish procedures that will assure safe and secure sites, thus assuring successful mission accomplishment. As the project becomes more defined and in-country conditions change, this plan will be updated as needed.

1) General Security Tasks.

(a) The protection of employees, including subcontractors, from acts of terrorism, criminal activity, protection from the former warring faction/s and the protection U.S. Government property that will be entrusted to BRS.

(b) Implement a badge system to control access to LOGCAP EVENT facilities.

(c) Implement control measures, which detect and deter pilferage.

(d) Provide guard posts, roving patrols and access control.

(e) Observe local laws as well as our own security policies and procedures including the U.S. Army's General Order #1 as directed.

(f) Work in close coordination with U.S. and Allied Military Police counterparts and host nation law enforcement.

(g) Security department employees shall meet all security force assessment and selection qualification standards.

(h) Prepare special orders for each guard post and roving patrol.

(i) In the event an armed force (subcontractor) is required, training and the rules of engagement for employment of deadly force shall be reviewed and agreed to with the prime contractor.

(j) Unexploded ordnance (UXO), landmines, antipersonnel mines and other types of munitions shall be cleared by the client's Explosive Ordnance Detachment (EOD), or if the client is unavailable, BRS shall contact a qualified subcontractor for the puupose of clearing (making safe) a given device.

b. Unfriendly Situation. Within the EVENT area there are groups that may pose a significant danger to the BRS project and its employees. It is vital to protect BRS employees and operations from the following threats: kidnapping, assassination, civil unrest, sabotage and espionage. Additionally, BRS employees will face constant threat of exposure to mines, booby-traps and unexploded ordinance (UXO). The type and level of threat may vary from site to site. Security measures shall be implemented to meet the assessed threat level at each separate location. Implementation and/or changing of security policy, procedures or directives shall be accomplished through close coordination with Project Management and the client.

c. Friendly Situation. This Annex addresses the security aspects of the BRS Oil Production Restoration Team. BRS will establish base camps for which security must provide protection. In some cases, BRS may be collocated with client elements and therefore will utilize the client's capability to provide physical and force protection for BRS base camps. In other cases, BRS may establish base camps in isolated locations separated from friendly forces. BRS CSP personnel are considered members of the EVENT FORCE and, as such, depend heavily on the U.S. military to provide a response force to suppress adversaries that might otherwise overpower our isolated base camp protective forces.

d. Assumptions.

1) The unemployment rate for local nationals is very high in the EVENT area.

2) Unemployed local nationals (including a large number of ex-military personnel) pose a significant threat to BRS operations and personnel.

3) The client provides all force protection for BRS personnel, equipment and facilities until such time BRS obtains a subcontractor (as directed by the client) to provide armed guard services.

4) Applicant screening of potential Host Country National (HCN) and Third Country National (TCN) employees shall be accomplished by the client. BRS will assume screening responsibilities as directed by the client.

5) BRS personnel always reside overnight inside a protected base camp.

6) The BRS Security Manager is a member of the EVENT FORCE Anti-Terrorism/Force Protection Working Group.

2. MISSION. See Base PLAN.

3. EXECUTION. See Base PLAN.

a. Concept of the Operation. BRS, on order of the Procuring Contract Officer (PCO), provides unarmed physical security services and armed Anti-Terrorism/Force Protection (AT/FP) services to protect a Contract Force of up to 5,000 personnel in the EVENT area, dispersed to a number of isolated sites.

1) BRS will plan, deploy, repair and hand-off operations In Accordance With (IAW) instructions given by the PCO. This natural progression will be conducted in four Phases. Once the client gives BRS the approval to deploy, BRS Security will participate in the advance team to determine the security and force protection requirements. Deployment begins in Phase II and continues to be refined and capabilities developed throughout the remaining phases.

2) BRS plans to immediately establish a logistical base to support operations. As the support capability is established in country, BRS will establish forward camps/sites to support the mission. These sites will be stand-alone and in some cases, may be collocated with military units. In all cases, the BRS sites will be self-sustaining without undue security support requirements placed on the military. Where armed security is required on a 24/7 basis, BRS will subcontract with an international security company to provide armed guards at the BRS base camps and designated worksites as required.

3) Due to the limited capability to defend ourselves from large numbers of organized and armed adversaries, BRS will depend on the U.S. Military to provide a Quick Response Force (QRF) to respond to crisis situations that exceed the BRS armed guard capabilities to the BRS camps and worksites.

b. BRS Camp Locations:

1) Camp #1, located at the North Rumailah Oil Field will be the main logistical base which will process personnel, supplies, and equipment to accomplish the mission throughout Iraq. This site will be staffed by American Citizens and a limited number of local national personnel for administrative, labor, and security responsibilities. All HCN and TCN personnel will have a direct supervisor who is an American Citizen.

2) Camp #2, located at South Rumailah Oil Field will be an operational camp with specialized teams of expatriates directly performing the restoration mission within a designated operational area. All engineering, logistical and security services will be provided by American Citizens and a small staff of HCN or TCN employees.

3) Camp #3, located at Al Fawl Oil Terminal will be an operational camp with specialized teams of EXPATS directly performing the restoration mission within a designated operational area. All engineering, logistical and security services will be provided by American Citizens and a small staff of HCNs or TCNs.

4) Camp #4, located at Kirkuk Oil Field will be an operational camp with specialized teams of EXPATS directly performing the restoration mission within a designated operational area. All engineering, logistical and security services will be provided by American Citizens and a small staff of HCNs or TCNs.

5) Camp #5, located along the Iraq-Turkey Pipeline will be an operational camp with specialized teams of expatriates directly performing the restoration mission within a designated operational

area. All engineering, logistical and security services will be provided by American Citizens and a small staff of Host Country Nationals (HCN).

c. **Security Tasks Duties & Responsibilities:**

1) BRS will provide a 24/7 full range of security and force protection services including, but not limited to; physical security, access control, and static and roving security guards, supervision and training for BRS unarmed security guards.

2) BRS will require that the subcontractor provide appropriate training for their armed guards.

3) BRS will provide the logistical support including vehicles, equipment, supplies, personnel, administration, and security management required to establish and maintain a physical security program.

4) BRS will provide its own security for installations, storage locations, Ammunition Supply Points, and Customs Sterile Areas not controlled by the CENTCOM. BRS will depend on this to provide quick response forces (QRF) when the threat exceeds BRS capabilities.

5) BRS will establish and maintain the installation physical security programs IAW AR 190-13, The Army Physical Security Program, FM 19-30, Physical Security, and BRS SOPs.

6) BRS will assign responsibility to provide oversight of the sub-contracted armed guard forces to the BRS Project Manager's Security Management Office. The guiding principles for employing the Armed Guards are based on the threat and perceived vulnerabilities.

7) The BRS Security Manager will coordinate support and operational actions with the CENTCOM J2/S2/PMO/Counter Intelligence/CID and their appropriate staffs, and if required, with the Embassy RSO and Host Nation security personnel.

8) Physical security will be both passive and active, and with the primary focus on preventive measures.

9) The BRS Security Manager will focus on the protection of personnel, work sites/facilities, and GFE/GFP. The physical security procedures will address all aspects of unauthorized access, vandalism, pilferage, larceny, sabotage, arson, damage from natural causes, and abuse. The BRS Security Manager will coordinate with the J-2, G-2 or S-2 staff, as appropriate, concerning the possible threat of terrorist/criminal activity and other force protection risks.

10) BRS physical security activities will be proactive. Action will be taken to increase threat vigilance, and ensure visibility of the Guard Force. Preventive and passive measures, use of identification badges, restricted access, locking of facilities, key control, identification of vulnerable areas of entry and exit, and continuing review of fence/barricade locations will be taken, as appropriate, to eliminate potential security shortfalls. BRS will augment preventive and passive measures with active measures.

11) BRS Guard Force Supervisors and other designated personnel will stress the importance of security by frequent inspections and by taking immediate corrective action to address physical security deficiencies. Repeated or intentional violations of physical security procedures will be cause for immediate termination of employment.

12) BRS security guard techniques will range from physical presence and limiting access to facilities through actual use of force as applicable based on specific command ROE. The use of force will be limited to the minimum required to prevent bodily harm or damage to or loss of facilities or equipment. Deadly force will only be used when the life of a guard or another person is in danger, but always in accordance with ROE.

13) BRS will maintain internal safeguards of equipment and supplies through strict adherence to supply accountability and proper inventory procedures.

14) BRS Guard Force personnel, when required by the Delivery Order, will control access to designated installations, base camps, storage facilities, customs holding areas and material storage areas. The BRS Security Manager will establish identification passes, as required by the task order, and in accordance with AR 190-13, AR-640-3, or local directives. Access points for each BRS secured facility will be controlled by the BRS Security or designated Guard Force personnel. Access control will be accomplished through search of vehicles, personnel, and containers prior to entry into the facilities. Guard Force personnel will also be prepared to escort visitors in restricted areas.

15) The BRS Security Manager and the Guard Force Supervisor at each location will be responsible to ensure all BRS subcontracted security personnel receive appropriate training for the tasks to be performed.

d. Tasks to BRS Elements.

1) Specific tasks to BRS elements are dependent on the directions contained in the Notice to Proceed (NTP) received from the PCO. See Paragraph 4 of this Appendix. Regional and Area Commander-specific plans should address these tasks in a detailed fashion. In general terms, the following applies:

a) At NTP, the BRS will establish a 24-hour Iraq Operations Center to serve as the nerve center for all activities and to communicate with the BRS Advance Team. The Advance Team will deploy within 72 hours of NTP. The Advance Team Leader will serve as the initial on-site EVENT Project Manager and will establish contact with CENTCOM senior Army Commander.

b) During Phase III, BRS will be tasked to provide full operational support capability. Early in the Maturation Phase, a permanent on-site Iraq Manager may replace the Advance Team Leader and qualified managers and supervisors may replace the Advance Team if they do not remain as the permanent party.

c) Phase IV, Redeployment, is the final Phase of the mission. BRS elements will be tasked to assist in the redeployment, transfer, redistribution, or disposal of supplies and equipment; and remove or turnover facilities.

e. Planning Factors.

1) Number, size, and location of designated sites.

2) Host Nation laws, Rules of Engagement (ROE), Task Force directives.

3) Nature of conflict and scenario threat range.

f. Protection Program Planning:

1) Proper Protection Program Planning is essential to the success of this project. Protection Planning is a key factor in BRS' proven success in high threat environments. Identifying the threats and determining where our vulnerabilities allow BRS to take mitigating actions reducing or eliminating the threats.

2) The Security Manager is responsible to conduct security planning with the intent of developing a security program that adequately protects employees, government and BRS property.

3) All employees are fully aware of the need to anticipate possible hostile actions and plan to reduce their effects. Employees are trained to recognize possible hostile actions directed against BRS operations, facilities and its employees. All employees are required to report any such suspicions to the Security Manager who will evaluate the information and consider information from all sources to determine a proper course of action.

4) The Security Manager will cultivate information sources within the community to help determine the local population mood and to gain advance warning of any planned activities to be directed against CENTCOM, BRS operations or its' employees. This informal effort allows BRS security personnel to anticipate and avoid hostile actions directed against BRS and its' employees, thus avoiding causalities and property damage.

5) The following threat, risk and vulnerability analysis will answer the questions of who, what, where and how. With this information, the security manager will design a security program focused on the most important security issues, allow for cost-effective solutions to security weaknesses and develop an aggressive security posture that is proactive anticipating future threats rather than reacting to those that have already occured.

a) Threat and Risk Assessments:

(1) Initial informal Threat and Risk Assessments are conducted by the security manager and staff to determine valid threats and identify the risks associated with those threats. As the CENTCOM threat analysis products become available, BRS security will compare and modify, where appropriate, the BRS identified threats.

(2) Analysis answers the questions of who, what and identifies the affect of the threats on operations.

b) Vulnerability Assessments:

(1) Once BRS security knows the threats and associated risks, it will then identify BRS vulnerabilities to those threats. This process allows BRS to focus limited resources on areas needing the most security attention. This costs-effective approach to security assures management and the customer that dollars spent on security are used wisely and obtains the most "bang for the buck."

(2) This analysis answers the questions of where and how.

g. **Site Protection:**

1) Perimeter Security:

a) Perimeter security is one of the most important security functions that must be established while operating in a hostile or semi-hostile environment. BRS security managers and engineers have been very innovative in designing barriers to protect camp perimeters.

b) Shown below are barriers tied together to form a solid perimeter that will withstand heavy vehicle attempts to penetrate the perimeter.

The above vehicle gate was designed by a BRS engineer that resulted in approximately $10K in costs savings per gate over commercial models, without a reduction in effectiveness. These gates are in use in Macedonia at Camp Able Sentry (CAS) and at two BRS facilities in Hungary.

c) BRS builds perimeters that fully meet customer requirements and expectations. The normal perimeter consists of double fences topped with razor wire, lights and guard towers to afford 24/7 observation by the protective force and HESCO barriers or T-walls to prevent heavy vehicles and personnel from entering the site. The HESCO

also provides a barrier to prevent adversaries from throwing explosive charges and/or shooting RPG-7 like weapons into the site

d) BRS recognizes that a barrier must be monitored with weapons to be effective If the threat is high and a probability of an attack by adversaries exists, BRS will subcontract an armed security force to provide perimeter observation and protection.

Below is a typical perimeter BRS built for the US Army in Bosnia.

2) Access Controls:

a) Camp access must be controlled at the gate and at the perimeter of each facility with a combination sensitive/high cost items and BRS security personnel This is accomplished by the strategic placement of guards and use of established procedures that allow authorized personnel access while denying access to others

b) Access controls are developed in layers so that should any one system fail, other systems will still provide protection This layered approach to security starts at the perimeter, continues with the internal guards and procedures and is fully supported by the activities individuals take to avoid becoming a victim of criminal activities The overriding factor is to have good security planning that is proactive to hostile actions

3) Locks & Keys:

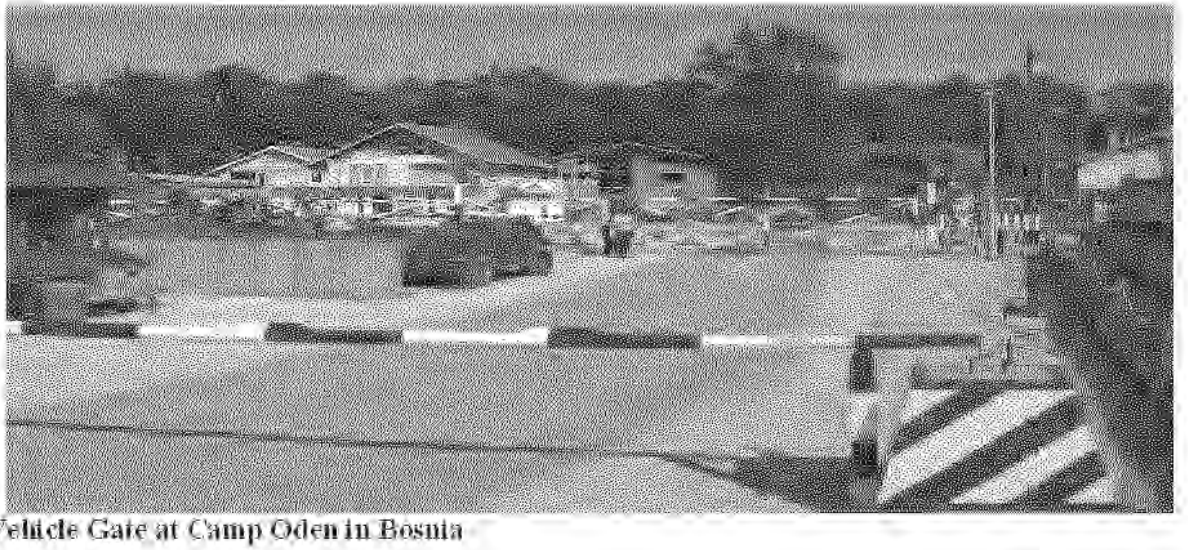
(a) Locks and keys or combination locks are used extensively for items determined not to be sensitive, classified or high value. Each section leader determines the required level of protection and is responsible to assure that these items are secured at the end of each shift. Security maintains a list of locks and a duplicate key or combination locked in a safe in the security office.

(b) The lock and key program tracks the locks and as they become unnecessary, reissues them to other personnel for property protection. These locks and keys/combinations are accounted for by each departing employee.

4) Gate Control:

(a) Gates protecting the interior of the site from vehicle and personnel assaults must be substantial. The policies and procedures must allow the guards to control access for vehicles as well as personnel. Picture identification cards are provided for each employee and authorized subcontractor, including local national personnel. The card stock is strictly controlled and employees are responsible for their issued badge. When 10 percent of the badges are lost or stolen, all employees will be issued a new badge with a new design to preclude the old design from being modified and possibly used to gain entry into the site. This will be discussed in more detail below in the section titled "Identification System."

(b) The pictures below show detail of the gates and the substantial aspects that assure adversary vehicles will not penetrate the vehicle gate.



Main Vehicle Gate at Camp Oden in Bosnia

Main Vehicle Gate at BRS Site in Kumanovo, Macedonia

Detail of Main Vehicle Gate at BRS Site in Kumanovo, Macedonia

5) Visitor Access:

Visitor access will be limited to those having a legitimate need for access (official business only). HCN or TCN visitors must have an appointment with a BRS employee and be approved by the expatriate supervisor. Other visitors can present themselves at the gate and the guard will notify the person being visited that the individual is at the gate. The BRS employee being requested and his/her expatriate supervisor will determine if the individual has a legitimate need for access.

6) Subcontractor Access:

(a) BRS subcontractors will identify employees that will work on the contract and of those, identify which will require access to the BRS site. Only those employees identified by the subcontractor as working on the contract and requiring access will be allowed onto the BRS site.

(b) Subcontractor badges will be issued with an expiration date that coincides with the contract termination date. The contract will require that all badges issued to subcontractors will be collected and turned into BRS security at the end of the contract or for each employee that is no longer working on the contract.

7) Personnel Searches:

(a) Personnel Searches are standard at each BRS facility. Each employee and visitor is searched upon entering the facility. These searches focus on preventing weapons, explosives and other prohibited articles from being introduced onto the BRS site. Normally searches are conducted by portable metal detectors. When it becomes necessary to hand search an individual they are searched by "like gender" guard personnel. Women are directed to a private area where the search is conducted.

(b) Anyone found attempting to bring a weapon, explosive or other prohibited article onto the site is immediately identified to CENTCOM, released from employment (if a BRS employee) and barred from site access. Visitors attempting to bring such items on site will be permanently barred from site access and CENTCOM notified.

8) Vehicle Searches:

(a) All vehicle searches focus on preventing weapons and other prohibited items from being introduced onto the BRS site. Exit searches focus on preventing theft of BRS and/or EVENT FORCE equipment, supplies, or materials.

(b) All non-CENTCOM vehicles will be searched each time they enter and leave a BRS site. CENTCOM vehicles and equipment operated by local nationals will be searched on each entry and exit. The only exception to this search policy is CENTCOM vehicles operated by U.S. Military Personnel. These vehicles will be included in the random search just as the BRS vehicles operated by BRS expatriate personnel.

9) Prohibited Articles:

(a) Prohibited Articles will not be allowed on a BRS Site at any time. The exception is the U.S. Military who may bring weapons on the BRS site, but must be cleared before entering the site.

(b) The BRS guard force may secure prohibited items until the security manager or coordinator can take possession.

(b) The BRS expatriate security manager and/or coordinator may hold and secure prohibited items pending final disposition.

(c) Below is a list of prohibited items that will not be brought onto the BRS site.

- Firearms
- Explosives
- Knives (any size)
- Tape Recorders
- Radios
- Tools (personal of any type)
- Personal Cell Phones
- Transceivers (any type)
- Scanners (any type)
- Any other electronic device
- Any item that could be used as a weapon or listening device

Any deliberate effort to bring the above items onto the site will result in the items being confiscated and not returned to the individual.

h. Security Identification System:

1) BRS issues all its employees a picture ID that identifies them as our employees. This ID is worn at all times and in plain sight when the employee is on duty. Should the EVENT FORCE provide other identification, emblems, or patches, these will also be worn at all times and in plain sight while accessing EVENT FORCE facilities. These emblems and patches will be returned to the BRS Security Manager upon an employee's contract termination.

2) Admittance of persons on EVENT FORCE controlled facilities require they be on official business and have positive identification.

3) BRS Security processes, issues, and controls permanent identification passes for BRS personnel and subcontractors.

4) BRS badges will be replaced with a new badge containing a new format when 10 percent of the issued badges have been lost or at the end of five years, whichever occurs first.

5) The BRS badge will be of a format design approved by the EVENT FORCE and will reflect the clearance level and category of the individual.

6) All badges will be numbered for accountability and reflect the BRS department in which the individual is assigned.

7) BRS security badges are U.S. Government property and accountable items. Badges will be returned to BRS Security when employees terminate employment.

8) When a subcontractor's employee terminates employment, the subcontractor will collect the BRS badge and returned it to BRS Security.

9) When the subcontract is terminated, the subcontractor is responsible to collect all badges and return to BRS Security before the contract will be considered complete.

10) Subcontractor badges will have an expiration date placed on them reflecting the end date of the contract.

11) All employees, subcontractors and visitors will display their security identification badge at all times while on BRS or CENTCOM property or leased facilities. This badge must be displayed on the front of the body and above the waist.

12) If a significant change in facial appearance takes place, a new photograph will be requested by the individual, supervisor, security official, access control personnel, or protective force personnel.

13) Protective Force personnel are authorized to confiscate faded, worn, damaged or badges that no longer reflect the actual appearance of the individual.

14) Managers will retrieve passes from employees who are suspended from work and deliver them to the Security Coordinator.

15) employees entering CENCOM facilities, who have forgotten or lost their identification pass or badge, may be provided a short term (one day) pass or badge by the protective force at the manned access point where the employee is attempting access. This is only after the protective force verifies employment and clearance level by checking with BRS Security and the individual has provided another form of picture identification, such as a Drivers License, Military ID, or Passport.

16) Employees will immediately notify security personnel at the nearest access control point and BRS Security when a pass or badge is discovered missing.

17) Personnel issued security identification badges must protect and maintain their security badges in good condition.

18) Security badges will not be used for "Ice Scrapers." Such use and repeated replacement will result in the employees' manager being notified of the abuse.

19) Security will notify the System Administrators when they become knowledgeable of a card being lost.

20) Card System Administrators will delete the card access for lost cards upon notification by BRS Security.

21) Employees who have lost a security identification badge will report to the BRS security and request a replacement.

22) Employees will be required to fill out a lost badge report for tracking/trending.

i. Personnel Protection:

1) It is essential for mission accomplishment that BRS personnel be protected from the threats and other hazards in the operational area. The anticipated hostile environment will dictate that BRS personnel remain overnight inside a protected base camp and be afforded lodging and food.

2) Medical services will be provided for those BRS employees that contact local medical problems. Medical treatment will be provided for stress related to long family separations. These essential services assure a mentally and physically healthy workforce to accomplish the mission.

a) Threats to BRS Personnel: BRS security has identified the following security related threats as valid for the Iraq operational area and there presence could impact mission accomplishment. No priority has been established for the identified threats; therefore, a threat analysis must be conducted immediately upon notification of deployment.

(1) Unexploded Ordinance is the most likely threat to the BRS personnel. There are a number of different types of unexploded ordinance that we expect to encounter in the Iraq operational area. The most common item expected to encounter is the Eastern Block Mine. There are a number of these ranging from antipersonnel to antitank mines and they vary in weight from a few ounces to over twenty pounds. BRS employees will be taught to expect to encounter these threats and to never touch or attempt to move a suspected mine.

(2) There will likely be **unexploded bombs** that have not been located by Explosive Ordinance Disposal (EOD) personnel. These bombs appear oblong weighing from a few hundred to thousands of pounds. These are likely to be of Western manufacture and will be olive green in color with black or yellow writing. These unexploded bombs will make a small crater on entry and often reemerge from the ground from 3 to 10 meters from the entry point. This is a very dangerous situation because this leaves the detonator pointed up and they are fully armed. The least vibration or impact with the bomb could set it off. BRS employees will also be instructed to not touch or attempt to move any of these items.

(3)Unexploded Artillery and Mortar shells are likely to be discovered by BRS personnel as they perform their mission. These could be of Eastern Block or Western manufacture. These are also oblong and will weight from ten to one hundred pounds. Again they could be slightly below the surface in a ten meter radius from the entry point. They are not as likely to resurface as the bomb because of their angle of impact and that they are spinning to form a gyro effect, which tends to maintain a straight trajectory.

(4) Booby-traps are very likely to be found by BRS personnel as they are performing their work. These come in many sizes, shapes and are initiated by a wide variety of devices. Normally they are made to look innocent by disguising them to look like something else or hiding them so the victim will inadvertently set them off by some seemingly innocent action. The most common initiator is the trip-wire. However, they can be initiated by pulling or releasing a taunt wire, applying pressure or releasing pressure. Releasing pressure is the most devious because normally something of value is placed on top of the release device and it activates when the victim removes the item of value.

(5) Assassinations are likely to occur with BRS employees because of our association with the CENTCOM. Military trained local nationals may see his/her only recourse to continue fighting is to become a terrorist and conduct assassinations on CENTCOM. This group of personnel would most likely have some marksmanship and possible some explosives training. They could assassinate by long distance shooting or setting booby-traps or command detonated mines. Weapons and explosives will be readily available in country and pose no problem for a local national to acquire.

(6) Kidnapping is also a likely occurence. To capitalize on the political mileage gained by publicly kidnapping and demanding ransom for an American would continue to meet most terrorist objectives, especially when there is no intent to release the individual. These types of actions can often have an affect on the American People that far outweighs the logical or expected outcome. The perception of an unbeaten organization would certainly prove beneficial to some local nationals.

(7) Assaults on BRS personnel are likely should the individuals be in unsafe areas alone. Most assaults occur on lone individuals who are in areas that are known to support this type of activity. Because of the sensitivity of BRS employees supporting the customer, this could be used to show other local nationals that the U.S. is not "all powerful." There are a number of possible motivating factors that would initiate an Assault. BRS personnel must be conscious of these and always act in a mature and prudent manner.

(b) Employee Protective Measures:

(1) Most BRS protective measures demand common sense and prudence to avoid becoming a victim.

(2) BRS personnel should travel in pairs when interfacing with local nationals in their areas, homes, or restaurants.

(3) When at work sites and traveling between, always be conscious of your surroundings and never touch or attempt to move objects that may be unexploded ordinance or booby-traps.

(4) Always be alert to personnel approaching you and attempt to determine early on, if they are armed.

(5) Watch the local nationals, especially the children, as their actions may indicate when something is about to happen.

(6) If you see indicators of unlawful activity or are uncomfortable in an area, restaurant, or just walking on the street, then get out of the area as quickly as possible.

(7) Don't set patterns. It is much more difficult to target someone moving in a random manner than someone who follows a pattern.

(8) Report any suspicious activity to the BRS Security Manager. He will have a way to check out the situation and alert the authorities of the possible unlawful activity.

(c) Employee Security Training Requirements:

(1) Each BRS employee will receive extensive indoctrination training before deployment to the operational area. This training will include local customs, what support/help can be expected from local authorities and any identified adversary groups operating in the area and their MOs.

(2) Each BRS employee will be given an annual security education and awareness class and OPSEC class. These subjects are identified in more detail below.

(3) Employees will be trained in security procedures and responsibilities. This training will vary from site to site depending on the site layout, threats, and the specific security requirements for each site.

i. Personnel Security:

1) Pre-employment Investigations:

a) BRS will prescreen potential employees for this contract before submitting them for a security clearance.

b) BRS will not submit their clearance packets until their pre-employment screening has been successfully passed.

c) To the extent possible, BRS will anticipate attrition of cleared personnel in advance, and submit clearance requests to CENTCOM for the anticipated replacement.

2) For all Sensitive Positions, managers will:

a) Assure that the potential employee is a U.S. Citizen. Acceptable documentation is a U.S. Birth Certificate, U.S. Passport or Naturalization Certificate.

b) For sensitive positions, BRS reviews the employee records to ensure the potential employee meets BRS employment standards. The basic standards are; U.S. Citizen and no derogatory or un-adjudicated information discovered from the pre-employment screening.

c) Advise and submit the request packet to employment services of potential employees who are selected for employment that will require a pre-employment background investigation.

d) Submit the personal biographical information to Personnel Security and request a pre-employment investigation be conducted. This process is to assure the highest possibility of the individual being able to obtain a security access authorization if hired.

e) Once the favorable pre-employment investigation is returned and the potential employee is approved for employment by the Security Department, the hiring manager will assure the employee submits his/her clearance packet to security for processing.

(1) The clearance packet will consist of the following:

(a) Form 4311
(b) SF-86
(c) FBI Fingerprint Card

(d) Fair Credit Reporting Act Release Form

(2) Not Recommended for Hire Guidelines:

(a) The determination of hire will be based solely upon the circumstances and records of each applicant`s case. The following conditions would generally result in a "Not Recommended For Hire" determination:

(b) The applicant cannot prove eligibility for hire, either by proving U.S. Citizenship or by providing other acceptable documentation as required by Immigration and Naturalization Laws.

(c) The applicant is currently on parole or probation for a felony.

(d) The applicant`s tests confirmed "positive" on the pre-employment Urinalysis Drug Screen or refuses to submit to same.

(e) The applicant has refused to take the polygraph as required under the contract.

(f) The applicant deliberately omits or misrepresents material facts in the employment application, Security Supplement, Questionnaire for Sensitive Positions, or other related documents.

(g) The "deliberate omission of material facts" is the apparent willful misrepresentation of facts to secure employment. This includes, but is not limited to, the following:

- The omission of one or more convictions of criminal law offenses.
- The omission or misrepresentation of the type of discharge received from the military service.
- The omission or misrepresentation of facts regarding the reason for leaving a previous employer.
- The omission of aliases or other names used over a period of time.
- The omission or rearrangement of employment history or residence addresses.
- The misrepresentation or falsification of statements concerning their level of education, training, or work experience.
- Illicit drug use or excessive use of alcohol.
- Issues that raise questions concerning the applicant`s loyalty.
- Mental Illness or Condition currently under treatment or previously received treatment for a mental condition which causes or may cause a significant defect in judgment and/or reliability.

j. Subcontractor Procedures:

1) BRS subcontracts will include the requirement to meet all BRS and CENTCOM security requirements and to follow all security policies and procedures.

2) Failure by the subcontract company management and/or its' employees to follow or to deliberately disregard those policies and procedures will be grounds to terminate the contract. Based on the situation, individual subcontract employees may be denied further access to BRS and CENTCOM facilities.

3) For subcontractors to receive a BRS subcontract badge, the BRS contracting officer must submit the names of the subcontractor who will require a badge for access to the BRS site. Only those personnel who require access to perform their mission will be issued a badge and afforded access.

4) The subcontractor employees will only use the issued badges to access BRS and CENTCOM sites in relation to their official duties outlined in the subcontract. Access will not be attempted for other reasons such as marketing their company or skills.

5) The subcontract will require that when a subcontractor employee terminates employee or is reassigned to other work, the subcontractor management is responsible to collect and return the employees badge to the BRS Security Manager. This will include any badges issued the subcontractor by the customer.

6) The subcontractor must return all badges, both those issued by BRS and the client to the BRS security manager at the termination of the contract, before the terms of the contract will be considered fulfilled.

7) BRS contracts will assure that all the above terms and conditions are appropriately reflected in each subcontract issued to perform work under this contract.

k. Reporting Marital Status and/or Name Changes:

1) Any employee becoming married or for other reasons have a name change, must report this marital status and/or name change to the security manager. In most cases name changes are because of the change in marital status, but some are for other reasons and must also be reported.

2) Marital status is normally accepted as a legal commitment between two people. However, this legal commitment can be establish between two people by way of "common law." This situation is known as a common-law marriage and in some states can be establish by couples of the same sex. These "same-sex" commitments must also be reported to the Security Manager. Same-sex marriages in and of themselves will not be grounds to deny a security clearance, but will be considered as other similar commitments between couples of different sex.

3) At all times when a name change occurs, the employee must report the change to security and receive a new security badge for facility access. Security records will be adjusted to show the new name.

l. Reinvestigation Program:

1) BRS Personnel Security will review each employee holding a security clearance every four years from the date of the last investigation to determine if they have a continuing need for a security clearance. For those that have a continuing need, the SF-86 form will be provided the employee early enough to allow the employee to provide personnel security with a completed SF-86 not later than four and one half years after the last investigation. This completed clearance request packet will be submitted for reinvestigation on or before the four and one half year point.

(a) Managers will:

(1) Justify to Personnel Security the need for continued clearance on this project.

(2) Allow each employee ample time during normal working hours to complete the reinvestigation forms.

(3) Ensure the employee completes and submits the required forms not later than 41/2 years from the date of the last investigation.

(b) Employees will:

(1) Legibly and completely fill out all forms in the reinvestigation packet.

(2) Contact Personnel Security to have the reinvestigation packet reviewed and fingerprints taken before four and one half years from the date of the last investigation has elapsed.

m. Reporting Procedures:

1) The BRS employees' manager will report to the security manager any contacts as described in NISPOM within two working days of his/her becoming knowledgeable of such event.

2) Breaches of BRS Policies, federal security rules or procedures, or participating in activities that raise doubt concerning an employee's loyalty or eligibility to continue holding a security clearance could result in the suspension or termination of the employee's clearance.

3) Individuals discovering what they suspect are wiretapping or eavesdropping devices or any illicit recording or transmitting device must immediately report the specifics to the Security Manager.

4) The individuals will not discuss the possible wiretapping or eavesdropping devices with anyone outside the Security Manager unless directed to do so by the U.S. Government CI representative.

a) Managers will report and consult with Personnel Security when an employee:

(1) Has been identified as having a potential drug or alcohol abuse problem.

(2) Is hospitalized or receives treatment for a mental illness that may cause a defect in judgment and/or reliability.

(3) Has been jailed.

(4) Becomes involved, or is suspected of becoming involved, in other wrong-doing.

b) Managers will counsel an employee regarding the:

(1) Need of the employee to inform Personnel Security in writing of any arrest and/or Court Judgment.

(2) Possible impact of an arrest/judgment on employment and/or clearance status.

(c) Managers will consider security clearance status by:

(1) Requesting a Management Information Sharing (MIS) meeting between the Personnel Security representative, and the individuals' manager. This MIS is only used in situations where the charge is not severe or as a beginning source of facts to help in deciding appropriate security clearance status.

(2) Withdrawing access to classified data or areas if charges are waiting final disposition.

(3) Advising the Personnel Security personnel when knowledgeable of a situation that warrant removal of a security clearance.

(4) Deciding security clearance status after trial and/or sentencing.

(c) Medical will:

(1) Notify Personnel Security when Medic Program Personnel identify an employee having an illness that may impair judgment or reliability.

(2) Relay details to Personnel Security when they become aware of drug abuse by an employee.

(3) Discuss with Personnel Security when employees are identified as having an alcohol problem.

(d) Employees and Subcontractor Personnel will:

(1) Report all arrests, charges (including those dismissed), or detention under federal, state, county, or municipal laws that occur during employment or during access to EVENT FORCE facilities or areas within five working days to Personnel Security except traffic violations with a fine of $250 or less.

(2) Notify his/her current manager and Personnel Security when arrested and/or convicted of a reportable offense.

(3) Surrender his/her identification pass and any government provided identifications, badges, or emblems when asked to do so by a security representative.

(4) Report to Security any knowledge or hint of possible fraud, abuse, or other form of wrong doing.

(5) Although employees and subcontractors have the option of reporting knowledge directly to the Inspector General or CID, we encourage employees to first the incident report to the BRS Security Manager, who will report it to CID.

(6) Report all change in marital status to Personnel Security.

(e) Testing for Illegal Drug and Alcohol Use:

Illegal use of drug or abuse of alcohol is not accepted in the BRS work environment. This illegal and abusive conduct is considered an indicator of poor judgment and grounds to terminate a security clearance. To assure that BRS meets its commitment of providing only the best and most trustworthy employees that exercise good judgment to work on this contract, each employee is subject to drug and alcohol testing.

(f) Testing for Cause:

(1) It is BRS policy that all employees will be free of the effects of illegal drugs and alcohol while performing their duties and responsibilities for the BRS and the customer. When a manager, supervisor, safety or security personnel suspect an employee of using illegal drugs or abusing alcohol they must request that the employee be tested for the suspected offense.

(2) Suspicion must be based on solid evidence of aberrant behavior or smelling alcohol on the breath of an employee. It is BRS policy that the operator of a motor vehicle or equipment involved in an accident be immediately tested for drug and/or alcohol abuse, regardless of fault in the accident.

(3) Employees found to have any illegal drug or alcohol in their system will be immediately terminated from employment.

(g) Random Testing:

(1) A random drug and alcohol testing program will be established. This program is administered by the security department and testing done by the medical department. These tests will be conducted during normal working hours for the employee and any employee found to have illegal drugs and/or alcohol in their system will be immediately terminated.

(2) The randomness is determined by a computer random number generator which is matched with the employee number. These employees will be identified by security and their names given to the medical department and the individual manager.

(3) The manager will escort the employee to medical and verify that the test was administered and witness the outcome of alcohol tests. He/she will witness that a urine sample was taken and that the "chain of custody" was followed by medical personnel. The urine sample will be sent to an independent laboratory for testing.

(4) Those tested personnel with positive results will be immediately terminated from employment.

n. Security Awareness and Training:

1) This program is a continuing, comprehensive effort to promote a high level of security awareness among employees and encourage employee compliance with security regulations and procedures.

2) Sponsor regulations and procedures applicable to BRS employees are taught as an integral part of the "Security Education and Awareness Program. Employees receive an initial class of instruction and annual refresher training each year thereafter.

3) BRS fully understands the need to meet customer requirements and communicated that need to all employees through our Security Education and Awareness Program. The Security Department conducted random audits of BRS activities to reinforce this need and assure that all applicable security requirements are met by all employees and subcontractors.

a) Managers Will:

(1) Provide a facility/area orientation for newly assigned employees immediately after they report for work.

(2) Assure that the newly assigned employee reports to the Security Education and Awareness Coordinator (SEAC) within two (2) days of being assigned and receives a briefing on access control, computer security, procedures for handling sensitive or classified information, etc.

(3) Ensure that employees attend the appropriate scheduled Annual Security Refresher Briefing.

(4) Provide ongoing security awareness activities for employees to augment the formal Security Education Program.

(5) Motivate employees to develop and maintain security awareness and good security habits.

(6) Inform employees in a timely manner of any changes to applicable Security Plans and Procedures.

(b) Employees Will:

Attend all required security briefings and orientations listed below:

- Initial Security Briefing
- Comprehensive Security Briefing when applicable
- Annual Security Refresher Briefing
- Foreign Travel Briefings when applicable
- Termination Briefing when applicable
- Maintain familiarity with BRS security requirements and policies.
- Maintain familiarity with applicable Security Plans and Procedures.

(c) Briefing, Re-briefing, and De-briefing Procedures:

(1) Many BRS employees will be required to have a security clearance access authorization briefing. It covers the requirements for handling, classifying, storing and transmitting classified information identified for inclusion in the above Security Education and Awareness Program.

(2) Compliance with these requirements and standards are mandatory for contractors working in a classified program.

(d) Initial Indoctrination: As soon as practicable after being approved for access to classified information, personnel will receive an initial security indoctrination briefing that includes:

(1) The need to protect classified information and the adverse effect on the National Security that could result from unauthorized disclosure will be taught.

(2) The administrative, personnel, physical and other procedural security requirements of BRS and the customer to include those requirements peculiar to specific duty assignments.

(3) Individual classification management responsibilities as set forth in appropriate directives and regulations to include classification/declassification and marking requirements.

(4) The definitions and criminal penalties for espionage, including harboring or concealing persons, gathering, transmitting, or losing defense information; gathering or delivering defense information to aid foreign governments; photographing and sketching defense installations; unauthorized disclosure of classified information.

(5) The administrative sanctions for violation or disregard for security procedures.

- A review of the techniques employed by foreign intelligence organizations in attempting to obtain National Security Information.

- Individual security responsibilities.

(e) Periodic Awareness Enhancement: Each BRS site will establish a continuing security awareness program that will provide frequent exposure of personnel to security awareness material. A continuing program may include live briefings, audiovisual presentations (e.g. video tapes, films, and slide/tape programs), printed material (e.g. posters, memorandums, pamphlets, fliers), or a combination thereof. It is essential that current information and materials be utilized. The program will include the basic elements as outlined below.

(f) Special Security Briefings/Debriefings will supplement the existing security awareness programs in the following situations:

(a) When an individual is designated as a courier.

(b) When high risk situations are present.

(c) When any other situation arises for which the Project Manager, Security Manager or designee determines that an increased level of protection is necessary.

(g) Access Authorization De-briefing:

(1) When a department/Agency has determined that access to classified information is no longer required, final instructions and guidelines will be provided to the individual. At a minimum these shall include:

(a) A requirement that the individual read appropriate sections of Titles 18 and 50, U.S.C., and that the intent and criminal sanctions of these laws relative to espionage and unauthorized disclosure be clarified.

(b) The continuing obligation, under the prepublication and other provisions of the nondisclosure agreement for classified information, never to divulge; publish; or reveal by writing, word, conduct, or otherwise, to any unauthorized persons any classified information, without the written consent of appropriate government officials.

(c) An acknowledgment that the individual will report without delay to the Federal Bureau of Investigation, or the government agency, any attempt by an unauthorized person to solicit National Security Information.

(d) A declaration that the individual no longer possesses any classified documents or material containing classified information.

(e) A reminder of the risks associated with foreign travel and foreign association.

o. **Operations Security:**

1) The OPSEC program is necessary to assure that the customer classified information is properly and appropriately protected. This program establishes policies and procedures to protect classified information by educating the employees and sensitizing the employees to possible methods adversaries use to gain information.

2) Not all efforts to gather information is from another Nation. Since the Soviet Breakup, most efforts to gather information is for economic reasons rather than political and are mostly conducted by corporations looking to increase their market share at the expense of their competitors.

3) Traditionally, BRS has focused the OPSEC program on collection efforts by other Nations for political purposes. We now have to include company proprietary information in the OPSEC program as well.

4) The formal BRS OPSEC program for this contract will be developed once BRS has entered the deployment phase. The individual elements that the program will cover are:

a) OPSEC Implementation Plan.

b) Development and Maintenance of Critical and Sensitive Information List (CSIL) and Essential Elements of Friendly Information List (EEFI)

c) Development of Adversarial Threat Statement:

d) Reporting/Tracking of Official Foreign Travel to Sensitive Countries:

e) Reporting/Tracking of Official Foreign Travel to Non-Sensitive Countries:

4. MATERIAL AND SERVICES.

a. **Supply.** Security personnel will require two sets of clothing, boots, and shirts per guard, daily rations and in the case of armed security guards, weapons and ammunition. Each armed guard should have one rifle with a basic load of ammunition and enough additional training ammunition on hand to conduct annual re-qualification training. One handgun should be issued to each supervisor with a basic load of ammunition and enough additional training ammunition on hand to conduct annual re-qualification training. Additionally, special items such as portable metal detectors for screening employees and visitors, flashlights, locks, vehicles (three per camp), transceivers, computers (three per camp), desks, chairs, and consumable supplies.

b. **Transportation and Movements.** Each camp requires a minimum of four vehicles. One, for the on-duty supervisor; one for emergency operations; response and posting of guards, one, for mobile patrols; and one, for administrative functions. Depending on the distance of required travel and physical layout of the camp, and areas of responsibility, the required number of vehicles may increase. (See Annex I for transportation details)

c. **Field Services.**

1) **Services provided to BRS.**

a) General. BRS will accomplish the following:

(1) Establish Liaison with local civil law enforcement agencies unless directed otherwise by the PCO/ACO.

(2) Maintain lost and found property by recording, processing, and returning property to owner(s), or properly disposing of unclaimed property.

(3) Monitor and assess installed alarms and intrusion detection systems.

(4) Conduct proactive anti-terrorism programs.

(5) Prepare and submit required incident reports.

(6) Rapidly respond to any incident reported to the security office or patrol by appropriate TF sources.

b) Physical Security Operations.

(1) Access Control. Provide access control for all BRS camps and facilities.

(a) Administer the BRS physical security program in accordance with AR 190-13, The Army Physical Security Program, and Appendix F, FM 19-30, Physical Security.

(b) Protect all personnel, Government and non-government property, material, and equipment located at the sites from unauthorized use, loss, theft, access,

espionage, sabotage, damage, and other incidents in accordance with Rules of Engagement (ROE).

(c) Control personnel and vehicle entry to and from designated entrances in the Rear Support Area and each Forward Support Area. Security will inspect deliveries and vehicles in accordance with BRS internal operating procedures. BRS will provide a corrective action report for all findings resulting from surveys, inspections. Corrective action reports will be provided to the PCO/ACO within seven days from the date of the survey or inspection. BRS will implement a badge and pass system to identify and control all military, civilian, BRS personnel and visitors to designated sites in accordance with AR 190-13, AR 640-3 and approved by the PCO/ACO. No more than ten (10) percent of issued badges will be compromised or lost without a badge and pass restart.

(d) Provide the PCO/ACO with complete identity data on each granted Limited Access Authority (LAA) to include the date LAA was granted, by whom, and expiration of the LAA.

(e) Ensure all LAAs are renewed in accordance with AR 380-67, paragraph 3-403.

(f) Protect all sensitive, controlled, and classified areas that include Category I and II munitions, and classified equipment and documents from theft, trespass, espionage, and sabotage in accordance with applicable ROE.

(g) Provide on-site supervision of the BRS Guard Force 24/7, to include inspection of each post, fixed and mobile.

(2) Communications. Installing, operating, and maintaining the security radio net Government Furnished Equipment (GFE). Installation and use of repeaters may be required to provide communications. The net will meet the following requirements:

(a) Consist of base stations, a repeater network as required, and a predetermined number of hand-held radios. Each station shall be capable of a minimum of 10 channel operations.

(b) Have one mobile radio in each patrol vehicle. The mobile radio will be able to communicate anywhere in sector, if applicable, and any other security mobile radio, hand-held or base station on the primary or alternate frequency.

(c) The secure base radio station(s) shall operate 24/7 for control of security Forces.

(d) Provide continuous two-way radio communications with sufficient range to communicate with all posts.

(e) Provide an alternate power source for two-way radios. Sufficient frequencies are required to ensure at a minimum one primary and one backup frequency.

(f) Provide hand-held radios with appropriate accessories, to include battery chargers, 100 percent spare batteries, belt clip carrying holsters, and - for 50 percent of the radios, detachable microphones, and ear pieces.

(g) Provide radios with locally reprogrammable channels. Each should be capable of a minimum of ten channels.

(h) Store, inventory, and account for the radios and accessories. BRS will issue radios to those individuals authorized in writing by the Government.

(i) Train all employees that use the radios to use standard radio procedures.

(j) **Roving Patrols.** BRS will patrol designated areas, including all parking lots, by motor vehicle, or on foot, as required to monitor any unauthorized entry or evidence of sabotage. While patrolling, BRS will check all designated gates, doors, and windows and visually check perimeter fences for damage or erosion and protective lighting systems. If gates or doors are found unlocked or windows open, BRS will notify the guard supervisor, who will contact the designated building custodian. The Guard Supervisor shall determine whether the patrol shall remain on site, and immediately notify the BRS Security Manager for that location. BRS will also perform other security-related activities necessary to meet the overall security requirements.

(k) Response to accidents and reports of crimes, to include First Aid (if required), protection of the crime scene, apprehension and detention of suspects, obtaining information from victims or witnesses, collection of evidence and processing of appropriate forms and reports. When necessary for off-installation investigations, functions will be performed in conjunction with Military Police.

(l) Investigate crimes affecting Government property.

(m) Complete formal reports on the results of investigations conducted.

(n) Collect, preserve, and safeguard evidence that may be used during courts-martial, civil courts, or board proceedings.

(o) Recover stolen property.

(p) Provide EVENT protective services, when directed by the PCO/ACO.

(3) Training.

(a) BRS will provide all guard service personnel the minimum training in the below listed areas prior to security post assignment:

- Mission and function of guard service operations. Purpose and duties of guard services.
- Post orders. Understand general and special orders provisions of the EVENT security process.
- Identification Badge System. Employee badge, visitor badge, and vehicle pass.

- Protection and transportation of sensitive equipment.
- Security guard authority to apprehend, detain and search.
- Rules of Engagement (ROE) as prescribed for specific locations by individual task orders issued under this contract.
- Radio procedures.
- Methods of detection of pilferage, sabotage, espionage and other criminal acts.
- Bomb threats, search methods, plans and evacuation of buildings.
- Civil disturbance and riot control. Protection of personnel and property.
- Contingency plans. Response to hostile situations, tactical response, and terrorist activities.
- Interpersonal communication skills.

(b) Refresher Training. Each security guard and supervisor will receive three hours of refresher training each month throughout the duration of the EVENT. Completion of training will be certified in writing by BRS after Government review.

d. Maintenance. Maintenance services required for guard service support. Minor and major maintenance (Level –10) will be performed by BRS guard service personnel on all assigned equipment in accordance with Army Regulations and manufacturer's instructions.

1) Initiate all work requests on a DD Form 2407/5504 to the Engineering Section for required repairs/replacements.

2) The principal security officer at each Forward Support Area and the Rear Support Area will maintain a Work Request Log. The log will include the request action, the time and date requested, the person making the request, a control number, and the date the work was satisfactorily completed.

e. Personnel. BRS will provide fully trained personnel for all guard service operations.

f. Uniforms. BRS security personnel will wear a distinctive uniform readily distinguishing them from other contractor and military personnel. Uniforms will be furnished by BRS.

g. Miscellaneous.

(1) Reports. BRS will maintain individual guard shift activity summaries and daily journals. BRS will prepare and submit full reports of incidents considered security breaches, violations of administrative regulations, or special instructions as set forth in Army EVENT General and Special Orders. Violations of AR 190-11, AR 190-13, AR 190-40, AR 190-50, and AR

190-51 shall be reported immediately to the guard supervisor and telephonically reported within one hour to the Government. Written reports shall be completed within 24 hours as designated in AR 190-40 for serious incident reporting. BRS employees will immediately report intrusion or threat of intrusion to installations to their supervisor.

(2) Safety.

(a) BRS will ensure all employees are thoroughly familiar with our Safety Program Plan and the operating procedures and safety precautions as stated in the Manufacturer's Instructions for each piece of equipment operated.

(b) Accident Reporting. A BRS Record of Injury will be prepared immediately upon occurrence of a job-connected injury and forwarded to the BRS Safety Officer.

(3) Quality Control. The BRS Security Manager will prepare a Delivery Order quality control checklist that will serve in consonance with BRS' Quality Control Plan.

5. **COMMAND AND SIGNAL.** See Base PLAN and ANNEX H

ACKNOWLEDGE

(b)(6)
BRS PGM, LOGCAP

OFFICIAL:
(b)(6) BRS D/PM

APPENDIX 1 (OPERATIONAL SECURITY) to ANNEX Q (PHYSICAL SECURITY) to LOGCAP CONTINGENCY SUPPORT PLAN

REFERENCES. See ANNEX N, Appendix 4.

TIME ZONE USED THROUGHOUT THE PLAN. Iraq

TASK ORGANIZATION. See ANNEX A.

1. **SITUATION.** See Base PLAN.

2. **MISSION.** See Base PLAN.

3. **EXECUTION.**

(a) Project General Manager's Intent: As a principle civilian contractor providing planning and operational support to our Nation's military, BRS has an innate responsibility to protect classified and unclassified information, thereby denying adversaries (or potential adversaries) its use in carrying out their plans for hostile actions against U.S. interests at home and abroad. Working hand-in-hand with PM LOGCAP, we will implement the OPSEC process for the BRS operations in Iraq, train all employees, and institute continual evaluation criteria to ensure our procedures remain effective and reasonable. We will look at ourselves through the enemy's eyes to determine how we need to adjust our behavior in denying critical information to adversaries. In doing so, our own operational effectiveness will be enhanced and our contributions to the success of any operation we support will be maximized.

(b) Concept of Operations. BRS operational planners will use the OPSEC process with the support of the Corporate Security Office and in close coordination with other company staff elements and supported military organizations. BRS, in conjunction with the CENTCOM and PM LOGCAP, will identify indicators that contribute to the loss of critical information and take action to deny or control the availability of those indicators to an adversary. OPSEC measures implemented will compliment physical, information, signals, computer, communications, electronic and other security measures to ensure a totally integrated security package. OPSEC is a continual requirement with changing parameters based on identified threats and locations. Each task order and/or support requirement under the LOGCAP contract will require evaluation and assessment of OPSEC requirements. BRS will utilize the OPSEC Process to determine how adversaries can be expected to derive critical information and to deny or control the availability of this information to them. The process consists of the following actions:

a. Identification of Critical Information.

While planning for the accomplishment of a task order, BRS will seek to identify the questions that we believe the adversary will ask about friendly intentions, capabilities, and activities. These questions are the essential elements of friendly information (EEFI). Critical information is a subset of EEFI. It is only that information that is vitally needed by an adversary. Identification of EEFI is important in that it will allow us to focus the remainder of the OPSEC process on protecting vital information rather than attempting to protect all information.

(1) Analysis of Threats.

BRS planners, with approval of CENTCOM, works with the intelligence and counterintelligence staffs of the supported units, seeking answers to the following questions.

(a) Who is the adversary? (Who has the intent and capability to take action against the planned operation or to pose a hostile threat of any kind?)

(b) What are the adversary's goals? (What does the adversary want to accomplish?)

(c) What is the adversary's strategy for opposing the planned operation?

(d) What critical information does the adversary already know about the operation or target? (What information is it too late to protect?)

(e) What are the adversary's intelligence collection capabilities? (Will require cooperation and support of PM LOGCAP and supported CINCs)

(2) Analysis of Vulnerabilities.

This step in the OPSEC Process requires an examination of each aspect of the planned operation to identify any indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. Vulnerabilities exist when the adversary is capable of collecting an OPSEC indicator, correctly analyzing it, and then taking action. BRS will work with supported units' intelligence and counterintelligence staffs to obtain answers to the following questions:

(a) What indicators (friendly actions and open source information) of critical information not known to the adversary will be created by the friendly activities that will result from the planned operation?

(b) What indicators can the adversary actually collect?

(c) What indicators will the adversary be able to use to the disadvantage of friendly forces? (Can the adversary analyze the information, make a decision, and take appropriate action in time to interfere with the planned operation?)

(3) Assessment of Risks.

(a) BRS will analyze the OPSEC vulnerabilities identified in the previous action and identify possible measures that can be taken for each of them.

(b) Specific OPSEC measures will be selected for execution based upon a risk assessment done by the PGM in coordination with PM LOGCAP. These measures will be used to prevent the adversary from detecting the indicator, provide an alternative analysis of an indicator, and attack the adversary's collection system.

(c) BRS, in close coordination with PM LOGCAP, will compare the estimated cost associated with implementing each possible OPSEC measure to the potential harmful effects on mission accomplishment resulting from an adversary's exploitation of a particular vulnerability. If the cost to mission effectiveness exceeds the harm that an adversary could inflict, then application of the measure may be inappropriate. Because the decision not to implement a particular OPSEC measure entails risk, this step requires military command involvement.

(4) Application of Appropriate OPSEC Measures.

(a) Implement measures approved in the previous action.

(b) Monitor adversary reaction to the measures implemented to determine effectiveness and coordinate feedback with the supported command.

(c) Adjust OPSEC measures as required.

4. SERVICE SUPPORT. See ANNEX I.

5. COMMAND AND SIGNAL. See Base PLAN and ANNEX A.

ACKNOWLEDGE:

(b)(6)
BRS PGM, LOGCAP

OFFICIAL:
(b)(6) BRS D/PGM