# Integrating Antiterrorism and Operations Security Into the Contract Support Process

## *Desk Reference*

*October 2014*

*4th Edition*

Always Ready, Always Alert

*Because someone is depending on you*

*ATTP 4-10 (FM 3-100.21)

# OPERATIONAL CONTRACT SUPPORT TACTICS, TECHNIQUES, AND PROCEDURES

June 2011



Headquarters, Department of the Army

# Contents


Photo by Sgt. 1st Class John Queen

# Introduction

## Purpose of This Publication

To provide Army leaders and selected staff officers with supplemental implementation guidance to Army antiterrorism (AT) Standard 18 related to integrating AT and operations security (OPSEC) matters into contract support planning and execution.

## Overview

On 12 October 2000 the USS *Cole* was attacked in the Yemeni port of Aden. Although the act was not committed by a contractor, the gap in protection afforded as part of the contract was a major contributing factor. The gap in contract control fatally allowed access to the ship. The subsequent investigation of the incident highlighted that "contracting and AT/FP are inextricably linked." Although it happened to a U.S. Navy ship, the lessons learned in the port of Aden have broad implications across the Army. In fact, over the past decade, subsequent attacks on Army organizations and potential for others led to specific efforts designed to improve antiterrorism and protection associated with contracting. That attack led to the development of the first Desk Reference and "Contract Requirements Package Antiterrorism/Operations Security Review Cover Sheet."

The threat of terrorism has not diminished since the last publication of the Desk Reference in 2012. More significantly, ongoing and evolving events suggest terrorism will not just remain but become more menacing to U.S. Army equities around the world. We know from experience that terrorists use contracting as a vehicle to get inside organizations' defenses. Access to installations, facilities, and information offers vulnerabilities that terrorists can take advantage of. This demands a thoughtful and informed response as contracts are developed and executed.

Using the Cover Sheet and Desk Reference is not a check-the-block concept. It requires practical decisions by commanders of organizations that require contracts—that is, "requiring activities." This version of the Desk Reference and AT/OPSEC Cover Sheet provide commanders with possible contract language related to decisions about the use of the Common Access Card (CAC) and, where the CAC is not necessary, appropriate policy-driven language for non-CAC access.

Army requirements to prevent terrorist attacks through contracting are spelled out in Army antiterrorism policy. Every unit, at the battalion level and above, must apply the standards for protection through its assigned antiterrorism officer (ATO). The Desk Reference provides techniques that support implementation of policy standards. Use of the pamphlet can assist the ATO in the duty to coordinate the organization's staff input. Using the contract support process, it indicates the actions necessary at the various steps of contract development and execution.

The division of responsibilities in the contract support process demands that requiring activities develop the protection necessary for their contracts. This occurs in the statement of work. The ATO acts as the staff focal point for requiring activities in the coordination necessary to make this happen. It is not solely the ATO or OPSEC officer's responsibility to ensure that all necessary protective measures are embedded in the contract. It is the collective response of many staff functions that ensures implementation of the most likely preventative measures in contract development and execution.

An attack at the Washington Navy Yard in 2013 (see "AT Procedures in a Contract …" p. 5) serves as a reminder that entering the appropriate security language into the SOW and ultimately the contract does not end the process. The language must be continually evaluated to ensure that contractors have

adhered to the contract language. This requires coordination with the contracting officer's representative and response by appropriate members of the staff associated with the selected contract language. The Desk Reference provides guidance to integrate AT/OPSEC language into the contract support process. Not all examples or techniques will apply to each contract. But the contract support process remains consistent, as does the role of the ATO and OPSEC officers using the cover sheet as requiring activity coordinators. Resourceful and attentive application of the principles expressed in the Desk Reference can help close the contracting gap in AT protection.

## Remarks on This Revision

- Language supporting commander's decision for CAC credentialing
- Language for both CAC and non-CAC contractors
- Encouragement for ATO as coordinator of the requiring activity staff
- Emphasis of coordination between tenant activities and installation officials for installation access considerations for contractors

## Intent

- Ensure integration of necessary and appropriate security measures in statements of work
- Compel adherence to Army and DoD policy regarding access control and vetting personnel
- Promote continual checks to ensure compliance with contracted security standards and update personnel records
- Encourage commands to develop situational language for differing circumstances

## Target Audience

- Requiring activity leaders
- Requiring activity contract support planning and management staff*
- Requiring activity ATOs
- Requiring activity OPSEC officers
- Requiring activity staff officers (for example, physical security, industrial security, force health protection) as applicable
- Law enforcement officials with access to NCIC and other law enforcement databases
- Contracting organizations and officers
- Selected training and capabilities development organizations

## Authority

The use of a cover sheet formalizes integration of necessary security measures in the contract support process. It is mandated by the Deputy Assistant Secretary of the Army for Procurement Policy Alert and Army AT policy. The use of the Requirements Package Cover Sheet in Appendix A (or one similar) as outlined in Army AT policy and related contract language codified in Deputy Assistant Secretary of the

* The Army has approved the 3C Operational Contract Support Planning and Management additional skill identifier (3C ASI) and is documenting this ASI in all units brigade sized and above, as well as all logistics battalions throughout the Army. This ASI is awarded upon successful completion of the Army Logistics University's Operational Contract Support Course. In some Army organizations, a Department of the Army civilian staff officer will perform the 3C function without the formal 3C ASI.

Army for Procurement Policy Alert is strongly encouraged. The additional procedures found in this Desk Reference are provided as reference materials and guidance to assist requiring activities in integrating AT and OPSEC considerations into all contract support requirements packages.

## Applicability

These procedures apply to all Army organizations in the request and receipt of contracted supplies, services, and construction in Army operations and garrison activities worldwide. Specific AT/OPSEC-related contract language, when included in a contract, applies to the prime contractor and all subcontractors via standard flow-down procedures. This language also applies in joint operations where the Army is the lead contracting agency.

## How to Use This Desk Reference

This Desk Reference provides various products to educate and assist the target audience, especially the unit ATO and OPSEC officer, in integrating AT and OPSEC matters into the contract support process, from requirements definition to contract execution.

- **Part I. General Considerations.**

  This section provides general considerations in planning and executing contract support applicable to all Army leaders.

- **Part II. AT & OPSEC in the Contract Support Process.**

  This table provides a detailed sequential step-by-step process, including the staff officer lead for each step.

- **Part III. ATO/OPSEC Risk Analysis and Assessment Checklist.**

  The ATO is the focal point for all staff planning required to properly integrate necessary AT-related security measures into statements of work (SOWs). This checklist is intended to aid the requiring activity staff, primarily the ATO, in reviewing the SOW, draft quality assurance surveillance plan (QASP) (for service contracts), purchase description (for supply contracts), and evaluation factors (as necessary) for AT/OPSEC matters and in completing the mandatory AT/OPSEC requirements package cover sheet (see Appendix A).

- **Appendix A. AT/OPSEC Requirements Package Cover Sheet and Standard AT/OPSEC Contract Language.**

  This form and enclosed standard contract language are encouraged for use for all contract requests with the exception of those exempted IAW Section I of this form. This form is intended to capture the requiring activity intent to include, or not include, selected AT/OPSEC standard contract language and clauses in each requirements package. The decisions expressed on this form will then guide the supporting contracting officer in determining the appropriate AT/OPSEC language in the solicitation and subsequent contract award. The cover sheet at Appendix A is a template. Commanders may modify the cover sheet to meet their specific requirements.

- **Appendix B. Sample AT/OPSEC Quality Assurance Surveillance Plan Elements.**

  This appendix provides examples of AT/OPSEC–related QASP elements.

- **Appendix C. Sample AT/OPSEC Work Statement Language.**

  This appendix provides examples of contract-specific AT/OPSEC SOW language.

- **Appendix D. Glossary of Terms, Abbreviations, and Acronyms.**

  This appendix provides definitions and descriptions of key terms and a list of all established abbreviations and acronyms used in this Desk Reference.

- **Appendix E. Supporting References.**

  This appendix provides information on all references used in, or directly related to, this Desk Reference.

## BALANCING FORCE PROTECTION AND CONTRACTED MISSION REQUIREMENTS

In 2002, shortly after the USS *Cole* incident, a major U.S. ship repair required work at a port in the Mediterranean. In order to ensure adequate protection, the local American commander decided that force protection (FP) was critical in making the repairs. In support of that particular concept, the evaluation plan reflected FP as the most important factor in best-value analysis of prospective contracts. A contract was awarded to a company associated with a foreign navy and residing on a foreign naval base because it afforded the best possibility for security. This ensured formidable protection during repair operations. During contract performance the ship was well protected; however, the contractor was ineffective in completing the necessary repairs.

In subsequent repair operations FP was integrated into best-value analysis rather than identified as the most important factor. FP was assessed on a "pass-fail" scale (that is, technical acceptability). Only companies that demonstrated the acceptable FP criteria would go further in the competition. The primary goal of prospective contracting competition became more balanced to ensure successful repairs coupled with improved considerations for protecting the troops and the ship.

**Lessons Learned**

1. The balanced approach could assign force protection as a "pass-fail" factor. Only companies that pass the FP criteria go further in the competition.
2. Contracts should be evaluated on best-value analysis with balanced factors (past performance, skilled workforce, schedule compliance, like price, etc.). In that way the contract accomplishes the mission and a vendor is selected from among those with approved FP plans.
3. Bottom line: there are ways to give appropriate weight to FP measures while still meeting all the requiring activity's standards and contract performance objectives.

**AT Awareness in Contracting Considerations**

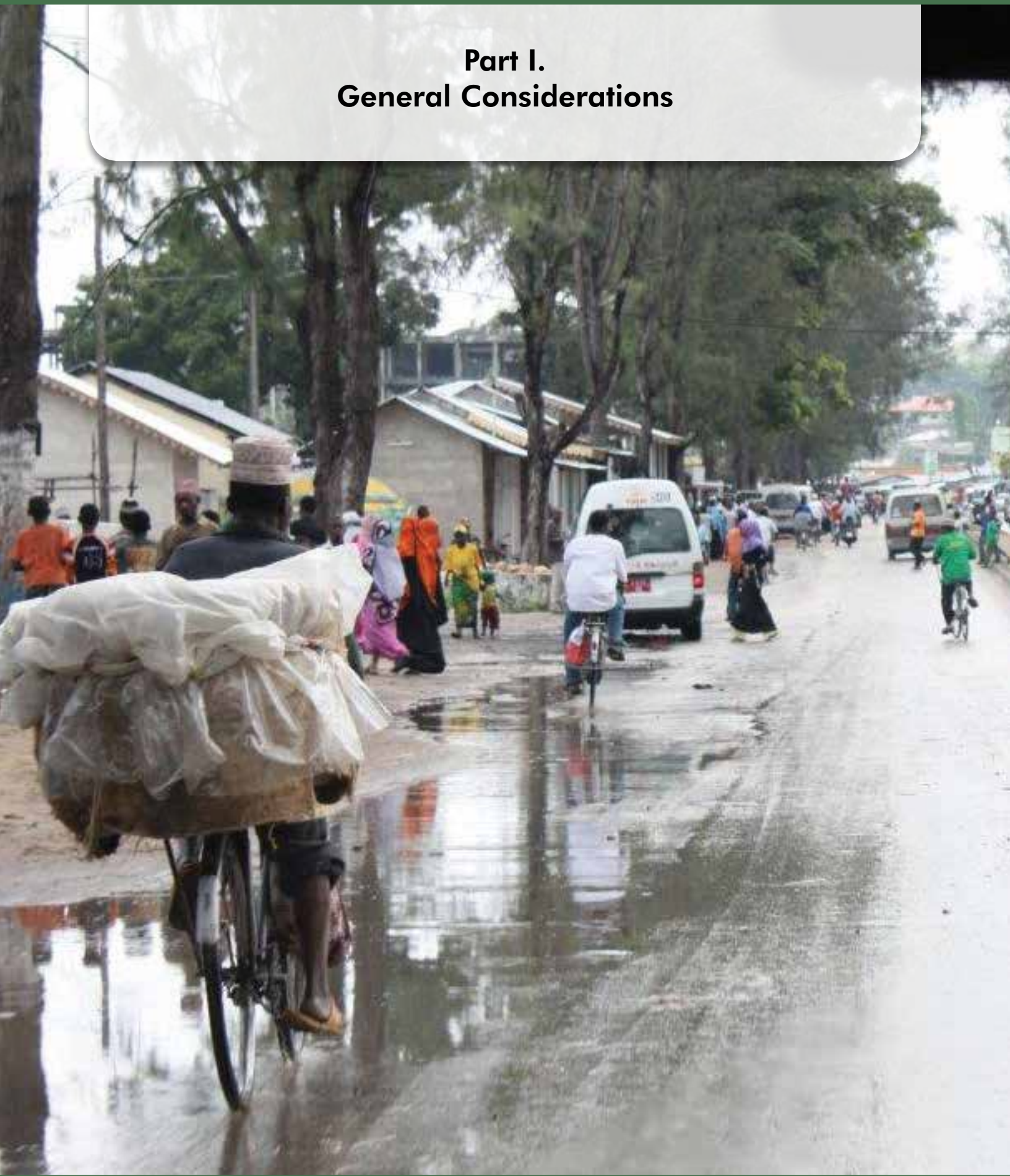
1. Illustrates the need for balance between mission and FP in contract development.
2. Suggests appropriate risk management in the initial planning.

**AT Procedures in a Contract, Properly Implemented and Tracked, Could Also Protect Against Some Criminal Attacks by Contractors***

On 16 September 2013 a lone shooter entered the Washington Navy Yard and proceeded to murder 12 civilian and contract employees, wounding four others. The attacker, Aaron Alexis, was not, in a strict sense, a terrorist, but he was a contracted worker, nor is there any certainty that pre-contract actions could have prevented his attack. However, there are at least two actions that, had they been implemented, might have changed the outcome. First, Alexis' actions might have been affected by different implementation of AT procedures in a contract. To be sure, he had the proper credentials allowing access to the Navy Yard, and the contractor had followed all procedures required by his contract. And yet, in retrospect, the background investigation required for employees on that contract did not include full inquiries into past arrests and warrants associated with the individuals. Had that been part of the investigation, Alexis' three previous arrests (2004, 2008, and 2010), two for firearms infractions and one for disorderly conduct, likely would have deterred any contract company from hiring him. Additionally, after Alexis was hired by the contractor company there were no checks (QASP) or reporting requirements during the execution of the contract to account for changes in character or subsequent criminal or bizarre behavior. Had there been a reporting requirement for changes in behavior, an admittedly strange episode with both installation and city police in August 2013 might have resulted in his release from the contract. There are no guarantees of success, but consciousness of the prospects should encourage rigorous review of people allowed access through contracts and encourage sustained reviews of contracts and contractors.

* For more detailed information on this incident, see "Washington Navy Yard Attack: 16 September 2013. The Challenge of an Active Shooter." This can be found on the Army Antiterrorism Enterprise Portal: https://west.esps.disa.mil/army/sites/APP/OPMG/OPS/antiterror/ATEP/default.aspx

# Part I.
# General Considerations



- Terrorists can attack anywhere, anytime—the threat is real.
- Contracted support, especially service and construction contracts, is vulnerable to terrorist exploitation, especially in foreign contingency operations.
- Requiring activities, contracting organizations, and contractors themselves all play a vital role in protection against terrorist acts.
- AT/OPSEC considerations must be taken into account when conducting both contract support pre-award and post-award tasks.
- Each contract has unique AT/OPSEC considerations. There is not one model that fits all contracts.
- Implementing AT/OPSEC measures requires a moderate degree of coordination and effort, so allow sufficient time to review and coordinate contract support request actions.
- The unit ATO is the lead integrator responsible to ensure that AT/OPSEC–related measures are considered in this process.
- The OPSEC officer and other security-related staff officers assist in this process.
- By embedding AT/OPSEC awareness throughout the contracting process, the Army as a community is better protected from terrorists.

*Special Note*

Recent terrorist and criminal attacks have generated more focused efforts aimed at improved access control. Army Directive 2014-05 (Policy and Implementation Procedures for Common Access Card Credentials and Installation Access for Uncleared Contractors) provides emphasis by direction and implication of the importance of effective access control procedures. Requiring activity ATO and associated law enforcement officials must ensure that all contracts contain the necessary access control procedures to prevent terrorists and/or criminals from exploiting vulnerabilities through contracting. This Desk Reference provides guidance that can assist requiring activity commanders and their staffs in doing just that.

## UNDOCUMENTED IMMIGRANTS USING CONTRACTS FOR ENTRY ONTO MILITARY BASES

On 4 July 2010, 25 construction workers were detained for using forged identification while trying to enter an Air Force Base in South Carolina. The news reports indicate that the detained workers were actually working construction on the base under a contract for the work. In actuality this has become a frequent occurrence. Since 2005 hundreds of undocumented workers have been involved with contracted work on military installations. In further investigations, some have even had criminal backgrounds and associations with gangs and possibly terrorist groups.

It is also true that instances such as these highlight the possibility of prospective terrorists using contract positions to survey or even attack Army installations.

**Lessons Learned**

1. Ensure contracts include the provisions that check for the possibility of and prevent undocumented workers for inclusion in contracted work related to Army missions.
2. In the QASP, include the checks that ensure only qualified personnel are performing the contract.

# Part II.
# AT & OPSEC in the Contract Support Process

| Phase | Step | Office of Primary Responsibility (OPR): Major Tasks |
|---|---|---|
| Initial Planning | 1. Determine initial requirements | • **Requiring activity commander and staff**<br>▪ In coordination with appropriate staff subject matter experts, determine support requirements based on the military decision-making process or another planning process<br>▪ Determine specific requirements that cannot be provided by organic or other noncommercial means<br>▪ Conduct an initial risk assessment to determine whether the commercial-sector support is appropriate<br>▪ Determine current and potential future threat assessment levels' effect on contract performance<br>▪ Develop an OPSEC critical information list<br>• **ATO, OPSEC and personnel who possess the 3C ASI**<br>▪ Integrate current AT/OPSEC and operational contract support and related HQDA and local command policy and procedures (for example, AR 525-13, ATTP 4-10, ALARACT messages 110/2011, Army Directive 2014-05) into routine staff planning |
| Requirements Development | 2. Develop requirements package | • **Requiring activity 3C staff officer, noncommissioned officer (NCO), or staff equivalent**<br>▪ Comply with applicable command guidance for requirements development<br>▪ Develop requirements package to include draft SOW or purchase description, draft QASP, and other documents as required by local policy or type of support required (for example, service or supply request)<br>▪ Obtain funding and approval for the requirements package<br>▪ Ensure nomination of properly trained and technically qualified contracting officer representatives (CORs)<br>▪ Consider including Contracting Specialist assistance when drafting the SOW—would potentially yield a better package submitted to a Contracting Officer |
| | 3. Perform AT/OPSEC–related risk analysis | • **Requiring activity 3C staff officer, NCO, or staff equivalent**<br>▪ Obtain proper unit or organization ATO review as required by HQDA and local command policy<br>▪ Work with appropriate staff to develop other support alternatives if risk of contract support is deemed unacceptable for this service<br>• **ATO**<br>▪ Review the draft SOW (for service contracts) and item description or product description in the purchase request (for supply contracts), QASP (for services contracts), and any evaluation factors to determine whether current protection measures, installation or facility access, contractor verification, and physical security and cyber security procedures are sufficient to mitigate identified AT risks<br>▪ Determine whether contract AT/OPSEC language or clauses are applicable and, if so, whether they are sufficient without additional SOW and QASP elements<br>▪ Coordinate a draft requirements package with other protection function staff members as appropriate for additional risk analysis<br>• **OPSEC officer**<br>▪ Ensure review of the requirements package for OPSEC matters by an OPSEC level II–certified individual |

| Phase | Step | Office of Primary Responsibility (OPR): Major Tasks |
|---|---|---|
| **Requirements Development** | 4. Finalize AT/OPSEC–related measures in the requirements package (or contract modification requests) and adjust installation or facility and contract service performance site security measures (as required) | • **Requiring activity 3C staff officer, NCO, or staff equivalent, the ATO, and as necessary other AT/protection staff**<br>▪ Include any work site–specific AT-related requirements in the SOW, QASP, and solicitation evaluation criteria as appropriate<br>▪ Stipulate applicability of the standard contract language or clause on the AT/OPSEC cover sheet<br>▪ Include DD Form 254 if the contract is classified or if the contractor will require access to classified information and/or systems<br>▪ Be prepared to appoint a trusted agent (TA) to approve contractor requests for Common Access Cards<br>• **ATO**<br>▪ Coordinate with appropriate staff or command to ensure that AT/OPSEC procedures are modified as necessary to mitigate any specific contract support–related AT risks<br>▪ At a minimum, ensure that the following matters are reviewed or considered: (1) personnel identification requirements are in the SOW, (2) reason for access is validated, (3) type of access and privileges are appropriate<br>• **OPSEC officer**<br>▪ Ensure that the final version of the requirements package is reviewed by an OPSEC level II–certified individual<br>▪ Sign the AT/OPSEC cover sheet<br>• **ATO**<br>▪ Review the final version of the requirements package to ensure recommended language is incorporated into the final SOW<br>▪ Sign the AT/OPSEC cover sheet<br>• **Requiring activity 3C staff officer, NCO, or staff equivalent**<br>▪ Ensure that the signed AT/OPSEC cover sheet is included in the requirements package<br>▪ Submit the requirements package to the appropriate contracting office |
| **Contract Solicitation and Award** | 5. Contract solicitation and award | • **Contracting officer**<br>▪ Ensure that the AT cover sheet is part of the requirements package<br>▪ Incorporate, if applicable, AT/OPSEC–related measures into the solicitation or contract via a standard contract or SOW-specific language<br>▪ Incorporate AT/OPSEC–related items in the QASP as appropriate<br>▪ Ensure that the solicitation or contracts provide information on or links to requirements for access to installations or facilities owned or leased by the Army and to other AT-related requirements<br>▪ Ensure that AT/OPSEC-related past performance is included in source selection as identified by the requiring activity<br>▪ Ensure that DD Form 254 is included if required<br>• **Requiring activity AT/OPSEC officers**<br>▪ Assist the contracting officer in determining appropriate source selection evaluation criteria and participate in the Source Selection Evaluation Board as a technical advisor on the AT/OPSEC evaluation factor<br>▪ Conduct background checks through the installation provost marshal office that vets contract employees using NCIC and terrorist screening databases (see background checks in glossary) |

| Phase | Step | Office of Primary Responsibility (OPR): Major Tasks |
|---|---|---|
| Contract Execution | 6. Execute contract and perform contract oversight | • **Contracting officer**<br>▪ Include major AT/OPSEC responsibilities in the COR appointment letter (as required)<br>▪ Notify the requiring activity of contract award; provide a copy of the contract; provide contract-specific orientation to the COR (as required)<br>• **Requiring activity trusted agent (TA)**<br>▪ Process contractor TASS requests per established TASS policy<br>• **ATO**<br>▪ Conduct post-award risk evaluation based on contract award and change to threat levels<br>▪ Notify the contracting officer through the requiring activity 3C staff (or designated individual) if there are any changes to AT-related procedures that may impact the supporting contractor<br>• **Contractor, requiring activity or supported unit, and continental United States replacement center**<br>▪ Validate contractor employee completion of AT/OPSEC pre-deployment and preparation for overseas travel training IAW the terms and conditions of the contract<br>• **Contracting officer via the COR**<br>▪ Ensure that the contractor has met AT/OPSEC training requirements before performance commences<br>▪ Document and report the quality of contractor AT/OPSEC performance<br>• **Requiring activity 3C officer, NCO, or staff equivalent**<br>▪ Notify the ATO(s) of the contract start and end dates<br>• **ATO/OPSEC officer**<br>▪ Advise the COR in assessing AT/OPSEC measures per QASP as determined necessary<br>• **ATO**<br>▪ Review AT measures as the local threat and force protection condition (FPCON) level changes; notify requiring activity 3C staff of same<br>• **Requiring activity 3C officer, NCO, or staff equivalent**<br>▪ Notify the contracting officer (via the COR) of any change to AT-related requirements and, when necessary, develop an appropriate request for contract modification and associated cost estimate<br>• **Contracting officer**<br>▪ Ensure that the contractor is provided with any changes to work site–specific or installation- or facility-wide security and protection procedures<br>▪ Initiate and execute appropriate contract modifications with the contractor, as necessary or as required by the requiring activity<br>▪ Ensure that AT-related performance is included in any consideration for contract renewal per approved acquisition policy guidance<br>• **COR, ATO, OPSEC officer, and contracting officer**<br>▪ Ensure that protection considerations are included in any incentive fee contracts (if applicable) |

# Part III.
# ATO/OPSEC Risk Analysis and Assessment Checklist

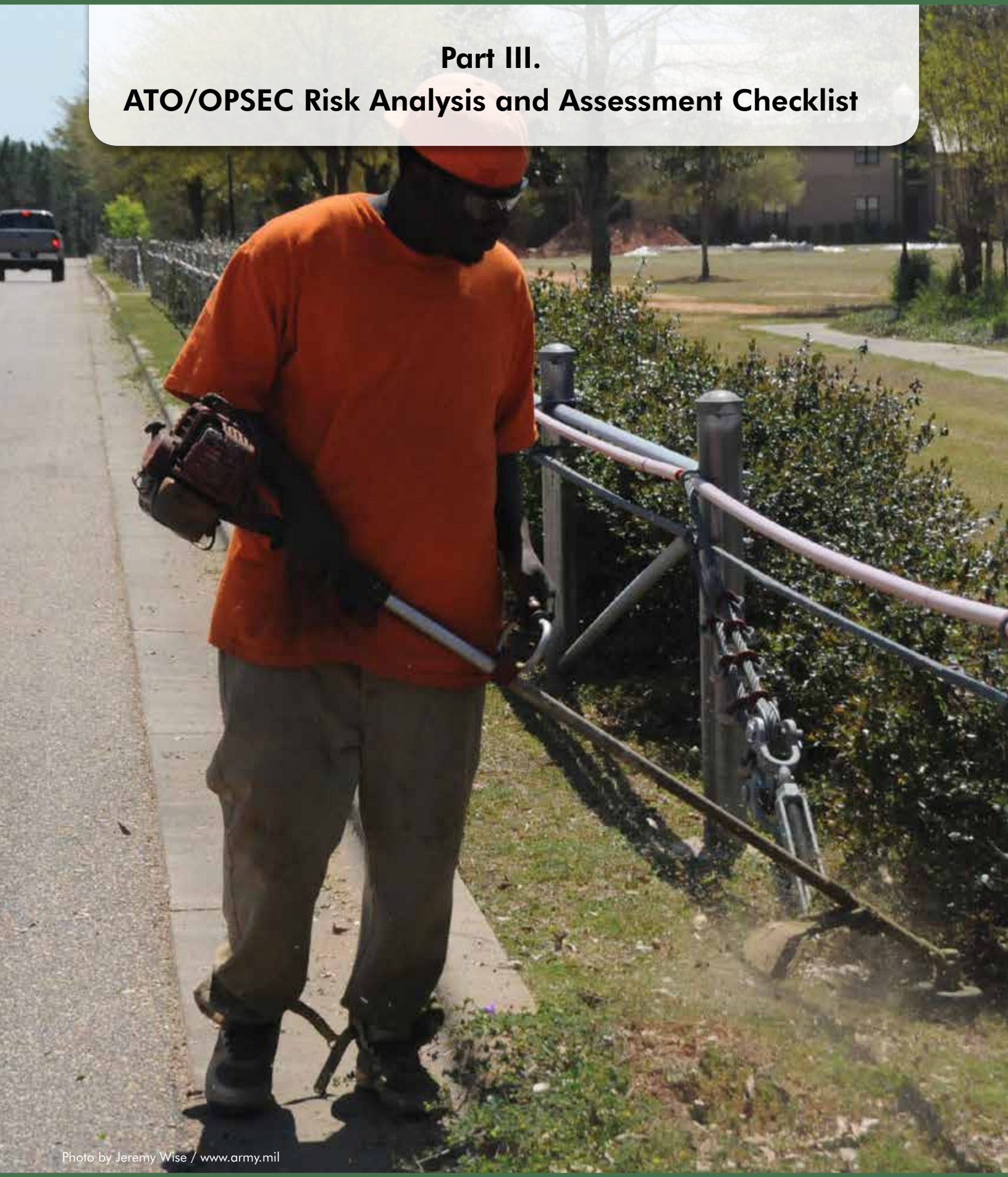


Photo by Jeremy Wise / www.army.mil

## Risk Assessment Process

### Threat Assessment Factors

- Is the contract request for a service, construction, or a supply? Note: It could be a combination of supply and service.
  - *Assessment of supply contract request:*
    - Could the commodity easily be tampered with? If yes, address special AT requirements in the product specification or item description.
  - *Assessment of service, construction, or supply contract request with delivery on a government-controlled installation, facility, or area:*
    - Will the contractor's area of performance be on a military installation or military-controlled area, or in proximity to military personnel while outside a military-controlled area?
    - Will contractor area of performance be in or on a facility that requires additional security measures such as security clearances, additional screening, or badging?
    - Have current and potential future threat levels' effect on contractor performance been considered?
    - Will contractor employees require access to military information systems?
    - Will contractor employees be handling or need access to classified and/or sensitive data?
    - Will contractor employees have frequent direct contact with government personnel?
    - What are the period of performance, working days, and hours?
- In consideration of the threat assessment of the area of performance, point of manufacture, and/or in-transit location(s):
  - *Does the threat assessment specifically consider the likelihood of the potential insider threat risk associated with granting contractor personnel access to the unit area, personnel, and equipment?*
  - *Does the threat assessment consider the likelihood of terrorist threats directed against contractor personnel providing goods and services?*
  - *Do local nationals (LNs) or third-country national contractor personnel in overseas locations go through a locally approved personnel verification process?*
  - *Is there a biometrics process in place to register LN and third-country national employees in overseas locations? (coordinate with legal office covering the HN; some nations have strict laws regarding biometric collection on LNs)*

### Criticality

A detailed review of potential vulnerability consequences that could result if contractor actions are not mitigated.

- Will the contract be performed at or near mission-critical facility or capability locations? If so, have AT/OPSEC procedures been put in place? Can the contractor gain unauthorized access to critical areas or locations?
- What unit or installation areas have or require controlled access?
- Is the contracted service mission critical? Would delay or loss of the contracted service have a critical impact on the mission?

- Is the contractor working with personnel, systems, or material that are of critical importance? Consider IT systems and networks, weapons systems, etc.
- What essential information can contractor personnel gain knowledge of in performance of their duties?
- Does the requirements package contain sensitive information?

### Vulnerability

A detailed review of the potential vulnerabilities associated with the contractor's performance of the specific task described in the SOW and evaluated through the QASP. Vulnerabilities are directly affected by the effectiveness of any existing security procedures or AT measures that are in place.

- Does the contractor require access to sensitive areas to perform duties?
- What potential vulnerabilities to forces, facilities, and supplies may we incur through this particular contract requirement?
- Will contractor personnel have access to hazardous materials (fuel, ammunition, medical waste, etc.)?
- Can these vulnerabilities be mitigated with specific contract and/or QASP language?
- What AT measures need to be added or modified to mitigate the vulnerabilities discussed above (for example, a supported unit requirement to provide armed escorts of LN contractor employees, more robust contract employee searches upon installation or facility entrance and egress)?

### Requirements Package Risk Evaluation

- What is the unmitigated or baseline risk (that is, before additional mitigation procedures are placed in the requirements package and/or AT measures are modified) of this contract request to the unit or mission, based on consideration of the threat, criticality, and vulnerability variables?
- Is there a need to modify or develop specific SOW, QASP, or AT/OPSEC evaluation factors and unit AT/OPSEC procedures?
- What is the residual risk (that is, after additional mitigation requirements are placed in the requirements package and/or AT measures and security procedures are modified) of this contract request to the unit or mission based on consideration of the threat, criticality, and vulnerability variables?

### Continuous Risk Evaluation

After contract award, ensure that the contracting office is informed (immediately through the appropriate COR) of any major threat level or AT/OPSEC procedure changes that may significantly impact the terms and conditions of the contract.

## PROTECTING THE CONTRACTING SOURCE

Early in Operation Iraqi Freedom, a brigade from the 101st Airborne Division was assigned a large area of operations near Tal Afar. The terrain the unit was required to cover and support exceeded the distribution capabilities of its ground transportation assets. Logistic officers supporting the brigade sought out and found a local business leader with a family-owned transportation company. He was positive towards U.S. aims for improving Iraq and willing to work with U.S. forces by providing various truck and bus services. After two months of ad hoc daily arrangements for services at the U.S. forces' compound entry point, the unit established a six-month contract to make the transportation support more regular. As the working relationship became more solid, the contractor and his employees also furnished insights into the effectiveness of U.S. information operations and the presence and activities of suspicious persons possibly affiliated with the insurgency. The arrangement worked exceptionally well, effectively supported counterinsurgency activities, and maintained peace and security—as long as the original unit that established the services was stationed in the area. Eventually, a smaller task force replaced the first unit that established the contract, and the security situation in the area began to deteriorate. Upon detecting this change in security posture, insurgents found the contractor and killed him. No doubt their intent was to degrade the U.S. forces' logistic posture and to send the message to other local vendors that doing business with the Americans was costly (Source: FM 3-24).

### Lessons Learned

Insurgents and terrorists are exceptionally adept at finding ways to attack gaps in logistics and support services. Inadequate or shifting U.S. security arrangements can provide openings for attacks against host-nation (HN) contractors and logistic providers. When insurgents attack people branded as traitors, there is an added terror and challenge to HN governance. When establishing logistic contracting arrangements with HN contractors in high-risk environments, U.S. logisticians and contracting officers must remember the grave risks people take by accepting contracting positions. Based on an operational assessment of the threat, vulnerability, and criticality, include sufficient security requirements in the contract to protect against loss of services/support or serious risk to contractors.

### AT Awareness in Contracting Considerations

If units do not address AT and security considerations, the use of contractor support to facilitate mission accomplishment may create vulnerabilities that terrorists can exploit. Units should understand that contractor personnel may represent soft targets for terrorists to attack, especially local/HN contractors who may not be accustomed to providing or able to provide their own security. Contracting with locals may provide valuable intelligence and promote coalition/HN relations. However, contracting with locals may also make them lucrative targets in non/semi-permissive environments. The degradation of contracted logistical support can be operationally significant, depending on the criticality of the support and timing of the service provided. Including security requirements in contracts can mitigate some risk. Repeated attacks against local contractors could cause U.S./coalition forces to establish additional security measures to protect contractors. Depending on the operational environment and resources available, the additional security may be at the expense of other mission-critical requirements and thus require the unit to balance support and security. If local contractors lack confidence in the ability of U.S./coalition military forces and law enforcement to provide a secure environment, not only will they be unlikely to provide the support, they may shift their support to the terrorists/extremists' cause.

# Appendix A.

## AT/OPSEC Requirements Package Cover Sheet and Standard AT/OPSEC Contract Language

Photo by Patrick N. Moes / US Army photo

## Contract Requirements Package Antiterrorism/Operations Security Review Cover Sheet

Requirements Package Title _____ Date _____

**Section I.**

**Purpose of cover sheet:** To document the review of the requirements package statement of work (SOW) quality assurance surveillance plan and any applicable source selection evaluation criteria for antiterrorism (AT) and other related protection matters, including AT, operations security (OPSEC), information assurance (IA)/cyber security, physical security, law enforcement, intelligence, and foreign disclosure.

**Army policy requirement:** A signed AT/OPSEC cover sheet must be included in all requirements packages except for supply contracts under the simplified acquisition level threshold, field ordering officer actions, and Government purchase card purchases. Command policy may require this form for supply contracts under the simplified acquisition level threshold.

**Mandatory review and signatures:** The organizational antiterrorism officer (ATO) must review each requirements package prior to submission to the supporting contracting activity, including coordination with other staff elements for review as appropriate per Section II below. If the requiring activity does not have an ATO, the first ATO in the chain of command will review the contract for considerations. An OPSEC officer review is also mandatory.

**Section II. Standard Contract Language Provision/Contract Clause Text Applicability and/or Additional SOW Language.** If standard contract or clause language found on page 2 (Section IV) of this form is sufficient to meet specific contract request requirements, check "Yes" in the block below and include this language in the SOW. If standard contractual text (provisions or clauses) or clause language does not apply, check "No." If the standard SOW language applies, but is not in and of itself sufficient, check "Yes" and "SOW" and include both the standard language and additional contract-specific language in the SOW. If standard contract text or clause language is not desired, but there is related contract-specific language in the SOW, check "No" and "SOW."

| | | | |
|---|---|---|---|
| 1. AT Level I training (general) | ☐ Yes | ☐ No | ☐ SOW |
| 2. Access and general protection policy and procedures | ☐ Yes | ☐ No | ☐ SOW |
| 2a. For contractor requiring Common Access Card (CAC) | ☐ Yes | ☐ No | ☐ SOW |
| 2b. For contractor not eligible for CAC, but requiring access to a DoD facility or installation | ☐ Yes | ☐ No | ☐ SOW |
| 3. AT awareness training for U.S.-based contractor personnel traveling overseas | ☐ Yes | ☐ No | ☐ SOW |
| 4. iWATCH training | ☐ Yes | ☐ No | ☐ SOW |
| 5. Army Training Certification Tracking System (ATCTS) registration for contractor employees who require access to Government information systems | ☐ Yes | ☐ No | ☐ SOW |
| 6. For contracts that require a formal OPSEC program | ☐ Yes | ☐ No | ☐ SOW |
| 7. Requirement for OPSEC training | ☐ Yes | ☐ No | ☐ SOW |
| 8. Information assurance/information technology training | ☐ Yes | ☐ No | ☐ SOW |
| 9. Information assurance/information technology certification | ☐ Yes | ☐ No | ☐ SOW |
| 10. Contractor Authorized to Accompany the Force clause | ☐ Yes | ☐ No | ☐ SOW |
| 11. Contract requiring performance or delivery in a foreign country | ☐ Yes | ☐ No | ☐ SOW |
| 12. Handling or access to classified information | ☐ Yes | ☐ No | ☐ SOW |
| 13. Threat Awareness Reporting Program | ☐ Yes | ☐ No | ☐ SOW |

**Section III. Remarks:**

**Antiterrorism Review Signature:** I am an ATO (Level II Certified) and have reviewed the requirements package and understand my responsibilities in accordance with Army Regulation 525-13, *Antiterrorism*.

Reviewer _____
Typed or printed name, rank or civilian grade

_____
Signature

Date _____

Phone number _____

**Operations Security Review Signature:** I am OPSEC Level II certified and have reviewed the requirements package, and it is in compliance with Army Regulation 530-1, *Operations Security*.

Reviewer _____
Typed or printed name, rank or civilian grade

_____
Signature

Date _____

Phone number _____

| Section IV. Standard Contract Language/Contract Clause Applicability and/or Additional SOW Language |
|---|
| **1. AT Level I training.** *This standard language is for contractor employees with an area of performance within an Army-controlled installation, facility, or area.* All contractor employees, including subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete AT Level I awareness training within XX calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee to the COR or to the contracting officer, if a COR is not assigned, within XX calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: http://jko.jten.mil. |
| **2. Access and general protection/security policy and procedures.** *This standard language is for contractor employees with an area of performance within an Army-controlled installation, facility, or area.* Contractor and all associated subcontractor employees shall provide all information required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office, Director of Emergency Services, or Security Office. Contractor workforce must comply with all personal identity verification requirements (CFR clause 52.204-9, Personal Identity Verification of Contract Personnel) as directed by DoD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes. |
| **2a. For contractors requiring CAC.** Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management. |
| **2b. For contractors that do not require CAC, but require access to a DoD facility or installation.** Contractor and all associated subcontractor employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (Army Directive 2014-05/AR 190-13); applicable installation, facility and area commander installation and facility access and local security policies and procedures (provided by Government representative); or, at OCONUS locations, in accordance with status-of-forces agreements and other theater regulations. |
| **3. AT Awareness Training for Contractor Personnel Traveling Overseas.** This standard language requires U.S.-based contractor employees and associated subcontractor employees to make available and to receive Government-provided area of responsibility (AOR)–specific AT awareness training as directed by AR 525-13. Specific AOR training content is directed by the combatant commander, with the unit ATO being the local point of contact. |
| **4. iWATCH Training.** ***This standard language is for contractor employees with an area of performance within an Army-controlled installation, facility, or area.*** The contractor and all associated subcontractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity ATO). This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within XX calendar days of contract award and within YY calendar days of new employees commencing performance, with the results reported to the COR NLT XX calendar days after contract award. |
| **5. Army Training Certification Tracking System (ATCTS) registration for contractor employees who require access to Government information systems.** All contractor employees with access to a Government info system must be registered in the ATCTS at commencement of services and must successfully complete the DoD Information Assurance Awareness prior to access to the information system and annually thereafter. |
| **6. For contracts that require a formal OPSEC program.** The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer. This plan will include a process to identify critical information, where it is located, who is responsible for it, how to protect it, and why it needs to be protected. The contractor shall implement OPSEC measures as ordered by the commander. In addition, the contractor shall have an identified certified Level II OPSEC coordinator per AR 530-1. |
| **7. For contracts that require OPSEC Training.** Per AR 530-1, *Operations Security*, the contractor employees must complete Level I OPSEC Awareness training. New employees must be trained within 30 calendar days of their reporting for duty and annually thereafter. |
| **8. For IA/IT training.** All contractor employees and associated subcontractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M, and AR 25-2 within six months of appointment to IA/IT functions. |
| **9. For IA/IT certification.** Per DoD 8570.01-M , DFARS 252.239.7001, and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award. |
| **10. For contractors authorized to accompany the force.** DFARS Clause 252.225-7040, *Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed Outside the United States*, shall be used in solicitations and contracts that authorize contractor personnel to accompany U.S. Armed Forces deployed outside the U.S. in contingency operations; humanitarian or peacekeeping operations; or other military operations or exercises, when designated by the combatant commander. The clause discusses the following AT/OPSEC-related topics: required compliance with laws and regulations, pre-deployment requirements, required training (per combatant command guidance), and personnel data required. |
| **11. For contracts requiring performance or delivery in a foreign country.** DFARS Clause 252.225-7043, *Antiterrorism/Force Protection for Defense Contractors Outside the US*, shall be used in solicitations and contracts that require performance or delivery in a foreign country. This clause applies to both contingencies and non-contingency support. The key AT requirement is for non-local national contractor personnel to comply with theater clearance requirements and allows the combatant commander to exercise oversight to ensure the contractor's compliance with combatant commander and subordinate task force commander policies and directives. |
| **12. For contracts that require handling or access to classified information.** Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information classified "Confidential," "Secret," or "Top Secret" and requires contractors to comply with (1) the Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); (2) any revisions to DoD 5220.22-M, notice of which has been furnished to the contractor. |
| **13. Threat Awareness Reporting Program.** For all contractors with security clearances. Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in 2-4b. |

## CONTRACTOR VERIFICATION PROCESS

**Background**

This vignette provides situational awareness and guidance regarding recent incidents which reveal potential security vulnerabilities on CONUS installations.

1. When a subcontractor employee attempted to gain access, a diligent access security guard noted discrepancies with his pass, which was determined to be a forgery. A subsequent review of all passes issued to the workers of the subcontractor resulted in the identification of 25 additional forged passes in the possession of workers who were also undocumented immigrants.
2. A subcontractor supervisor working for a building cleaning company was determined to be an undocumented immigrant after being apprehended on post for assault.
3. Two construction subcontractors attempted to access an installation using state identification cards. Security guards determined the identification cards were fraudulent. After the workers were questioned by installation law enforcement, they admitted that they were undocumented immigrants.

**Lessons Learned**

1. Commanders should review installation access control procedures and ensure that law enforcement, security forces, and supporting contracting offices are aware of the above incidents and take action to prevent unauthorized access.
2. Ensure access control programs comply with DoD Directive-Type Memorandum (DTM) 09-012 (8 Dec 09), Subject: "Interim Policy Guidance for DoD Physical Access Control," Attachment 3, physical security access control standards. Review all access control procedures to ensure that procedures are in place to proof and vet the claimed identity and to determine fitness for entry for all non-Federal government and non-DoD issued card holders. These personnel must also provide a valid purpose to enter when requesting access to installations.
3. Conduct regular inventories and account for all passes issued to contractors and subcontractors holding non–Federal government and non–DoD issued cards who are allowed access to the installation. Commanders may also direct their Provost Marshal/Director of Emergency Services to use the Centralized Operations Police Suite (COPS) Vehicle Registration System module or the Defense Biometric Identification System to produce temporary passes.
4. Incorporate features in locally produced passes and identification that decrease the likelihood of forgery, such as (1) Include a digital photograph of the holder; (2) include a unique identifier that enables quick visual authenticity determination such as an embossed seal or other similar method; (3) laminate or tamper proof the document. Conduct random validation checks of temporary installation passes to ensure authenticity.

**Notes for Commanders**

1. Commanders should ensure contracting office representation on the Antiterrorism Working Group. Commanders should review the integration procedures contained in Appendix 8, DTM 09-012, and ensure the requirements of AR 525-13 (Antiterrorism), Standard 18, are implemented.
2. Implement verification processes that demonstrate the trustworthiness of a defense contractor or subcontractor. This should be done by ensuring that contracts require background checks to meet installation access requirements.
3. Commanders should ensure that installation contracting offices review existing and all new service contracts to ensure those contracts that exceed the specified acquisition threshold and do not meet one of the exceptions specified in FAR 22.1803 include FAR Clause 52.222-54 (Employment Eligibility Verification). If compliance violations are suspected or identified, commanders should contact the contracting officer to explore remediation actions.

# Appendix B.
# Sample AT/OPSEC Quality Assurance Surveillance Plan Elements

Photo by Sgt. Melissa Shaw

| Sample—Quality Assurance Surveillance Antiterrorism/Operations Security Elements |
|---|
| **Contractor: Ajax Commercial** |
| **Contract Number: TCH345-987** |
| **Service or Supply Provided: Facility Maintenance** |
| **COR Name: CPT Houser** |
| **Date:** [XX]* |

| Standard Language / Specific PWS Requirement | Requirement | Method of Surveillance | Frequency | Performed by Whom? | Acceptable Quality Level | Was the Requirement Met? | Comments/ Remarks |
|---|---|---|---|---|---|---|---|
| iWATCH Training Standard Language | Has the contractor provided iWATCH training to all personnel within 30 calendar days of contract award? | Training report from the prime contractor | Periodic | COR in coordination with the requiring activity ATO | 90% | Yes | Report submitted on time, 97% of employees trained |
| Standard Installation or Facility Access Language | Has the contractor followed installation or facility access procedures? (contingency example) | Incident reporting | Once a month | COR in coordination with the installation or facility security office | No more than one incident per month | No | Three employees found to be carrying cell phones when searched at the gate |
| OPSEC SOP/ Plan | Has the contractor submitted the required OPSEC SOP/ Plan and does it meet minimum quality standards? | Submitted by the contractor | Within 90 calendar days of contract award | Received by the COR, evaluated by the supporting OPSEC officer | No | No | SOP/Plan submitted on time; the OPSEC Officer returned for more detail on counter-measures, incomplete linkage to current threat |
| Info Assurance Standard Clause | Are IA workforce personnel trained IAW DoD and Army policy? | Submitted by the contractor | Within 30 calendar days of contract award | Received by the COR, evaluated by the supporting OPSEC officer | 100% | Yes | All employee certifications complete and training records on file |
| Access to Classified Information | Is access to classified information and spaces restricted to properly cleared personnel? | Incident reporting | Once a month | COR in coordination with unit info security officer | 100% | Yes | No violations reported |

* [XX] are fields to be filled in when finalizing the QASP.

# Appendix C.
# Sample AT/OPSEC Work Statement Language

Photo by SSG Ashlee Lolkus

## Routine Examples

FAR clause 52.204-9 Personal Identity Verification of Contractor

Personnel----------

PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (JAN 2011)

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24 and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall account for all forms of Government-provided identification issued to the Contractor employees in connection with performance under this contract. The Contractor shall return such identification to the issuing agency at the earliest of any of the following, unless otherwise determined by the Government:

(1) When no longer needed for contract performance.

(2) Upon completion of the Contractor employee's employment.

(3) Upon contract completion or termination.

(c) The Contracting Officer may delay final payment under a contract if the

Contractor fails to comply with these requirements.

(d) The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts when the subcontractor's employees are required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system. It shall be the responsibility of the prime Contractor to return such identification to the issuing agency in accordance with the terms set forth in paragraph (b) of this section, unless otherwise approved in writing by the Contracting Officer.

(End of clause)

- **Contracts requiring access to Army-controlled installations or facilities.**
  - The company will have a law enforcement background check completed for all employees who will be entering Army-controlled installations or facilities. Documentation of these checks will be made available to the COR upon request.
  - The company will provide to the COR, seven days in advance of the event, names and Social Security numbers (or equivalent identification numbers for non-U.S. citizens) of all employees who will be entering Army-controlled installations or facilities.
  - The company will ensure that its employees entering Army-controlled installations or facilities have obtained access badges and passes in accordance with facility regulations and that these badges and passes are obtained in advance so as not to delay the accomplishment of contracted services.

- The company will return all issued U.S. Government Common Access Cards, installation badges, and/or access passes to the COR when the contract is completed or when a contractor employee no longer requires access to the installation or facility.

- **Employee escort for housecleaning services in secure areas.**
  - The contractor has complied with all personnel identity verification procedures. Employees must be accompanied by an authorized Government employee at all times while in Building [XXX].*

- **FPCON impact on work levels.**
  - During FPCONs Charlie and Delta, [XXX]* services are discontinued. [XXX]* services will resume when the FPCON level is reduced to level Bravo or lower.
  - This contract and its employees are considered mission essential. Therefore, all contractor employees are required to report for duty and remain on duty during declared emergencies and/or elevated FPCON levels unless otherwise directed by the contacting officer via the appropriate COR.

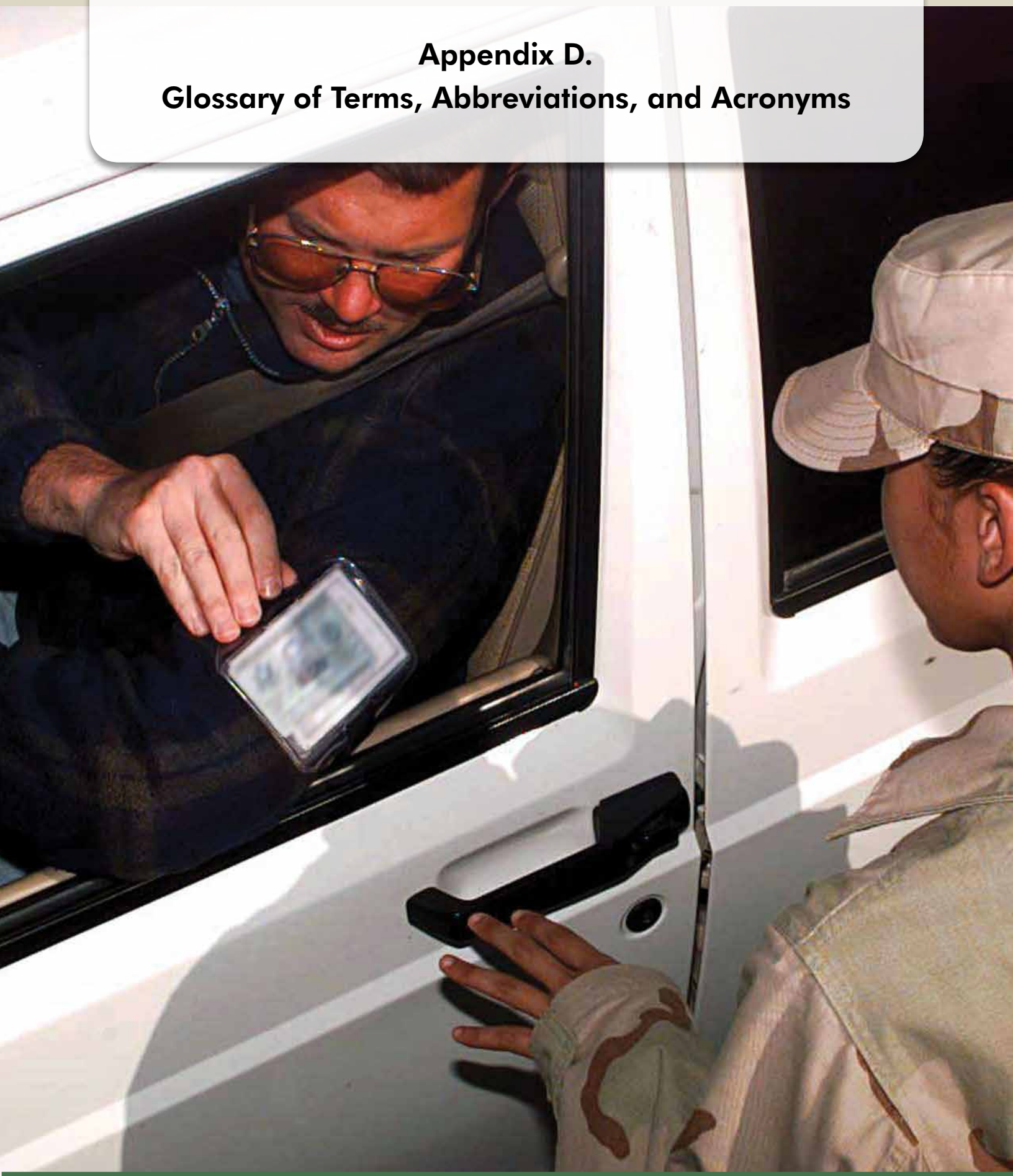
## Contingency Examples

- **LN employee identification in contingency environments.**
  - All LN contractor employees working on an installation or facility will wear distinctively colored overalls when on the facility. Said overalls will be provided by the Government and returned to the installation property book officer upon completion or termination of the contract.

- **Integration into the military convoy system.**
  - The contractor is responsible to incorporate all vehicles into military convoys as directed by [123rd Transportation Company (or applicable replacement unit)].* Contractor drivers must follow all convoy commander safety and emergency procedure instructions.

*Use relevant contractor details and describe services [XXX] in detail when filling out the form.

# Appendix D.
# Glossary of Terms, Abbreviations, and Acronyms



# Section I. Abbreviations and Acronyms

| | |
|---|---|
| 3C ASI | operational contract support planning and management additional skill identifier |
| ALARACT | All Army Activities |
| AR | Army regulation |
| AT | antiterrorism |
| ATCTS | Army Training Certification Tracking System |
| ATO | antiterrorism officer |
| ATTP | Army tactics, techniques, and procedures |
| COR | contracting officer representative |
| DA | Department of the Army |
| DFARS | Defense Federal Acquisition Regulation Supplement |
| FPCON | force protection condition |
| HQDA | Headquarters, Department of the Army |
| IA | information assurance |
| IAW | in accordance with |
| IT | information technology |
| LN | local national |
| NCIC | National Crime Information Center |
| NCO | noncommissioned officer |
| OPR | office of primary responsibility |
| OPMG | Office of the Provost Marshal General |
| OPSEC | operations security |
| QASP | quality assurance surveillance plan |
| SOP | standard operating procedure |
| SOW | statement of work |
| TA | trusted agent |
| TASS | Trusted Agent Sponsorship System |

# Section II. Glossary of Terms

**area of performance.** The actual location of the work being provided under a service contract.

**antiterrorism.** The prevention or abatement of terrorist activities directed against U.S. Government personnel and/or facilities.

**background checks.** In addition to NCIC and terrorist screening databases, law enforcement background checks could include:

local law enforcement background check

National Law Enforcement Telecommunications System (NLETS)

Defense Incident Based Reporting System (DIBRS)

**contractors authorized to accompany the force.** Contingency contractor employees who are specifically authorized through their contract to accompany the force and have protected status IAW international conventions.

**contracting officer.** A Service member or Department of Defense civilian with the legal authority to enter into, administer, and/or terminate contracts.

**contracting officer representative.** A Service member or Department of the Army civilian appointed in writing by a contracting officer responsible to monitor contract performance and perform other duties specified by the appointment letter.

**critical information.** Information important to the successful achievement of U.S. objectives and missions, or that may be of use to an adversary of the United States. Critical information consists of specific facts about friendly capabilities, activities, limitations (including vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishments. Critical information is vital to the mission: if an adversary obtains it, correctly analyzes it, and acts upon it, that will prevent or seriously degrade mission success. Critical information can be classified or unclassified information. It can also be an action that provides an indicator of value to an adversary and places a friendly activity or operation at risk.

**critical information list.** A consolidated list of a unit or organization's critical information.

**cyber security.** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

**information assurance.** The protection of systems and information in storage, processing, or transit from unauthorized access or modification; denial of service to unauthorized users; or the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats. IA encompasses communications security, computer security, and control of compromising emanations.

**operations security.** A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to

a. Identify those actions that can be observed by adversary intelligence systems.
b. Determine indicators that hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

**performance work statement.** A performance-based description of the user's technical, functional, and performance requirements. It addresses the quality of work in terms of desired outcome and accurately reflects the actual Government requirement, including performance standards. Sometimes called a statement of work or SOW.

**quality assurance surveillance plan.** A plan for measuring contractor performance to ensure that the U.S. Government receives the quality of services called for under the contract and pays only for the acceptable level of services received.

**requiring activity.** The organization that requests a specific contracted support requirement and is responsible to assist the contracting organization with contract management assistance, normally in the form of COR support.

**requirements package.** The detailed work documentation provided by the requiring activity that includes a funding document, justification for the requirement, SOW/PWS (for a service contract) or item description (for a commodity request), cost estimate, draft QASP, and other documents needed locally for submission to approval or contracting officials.

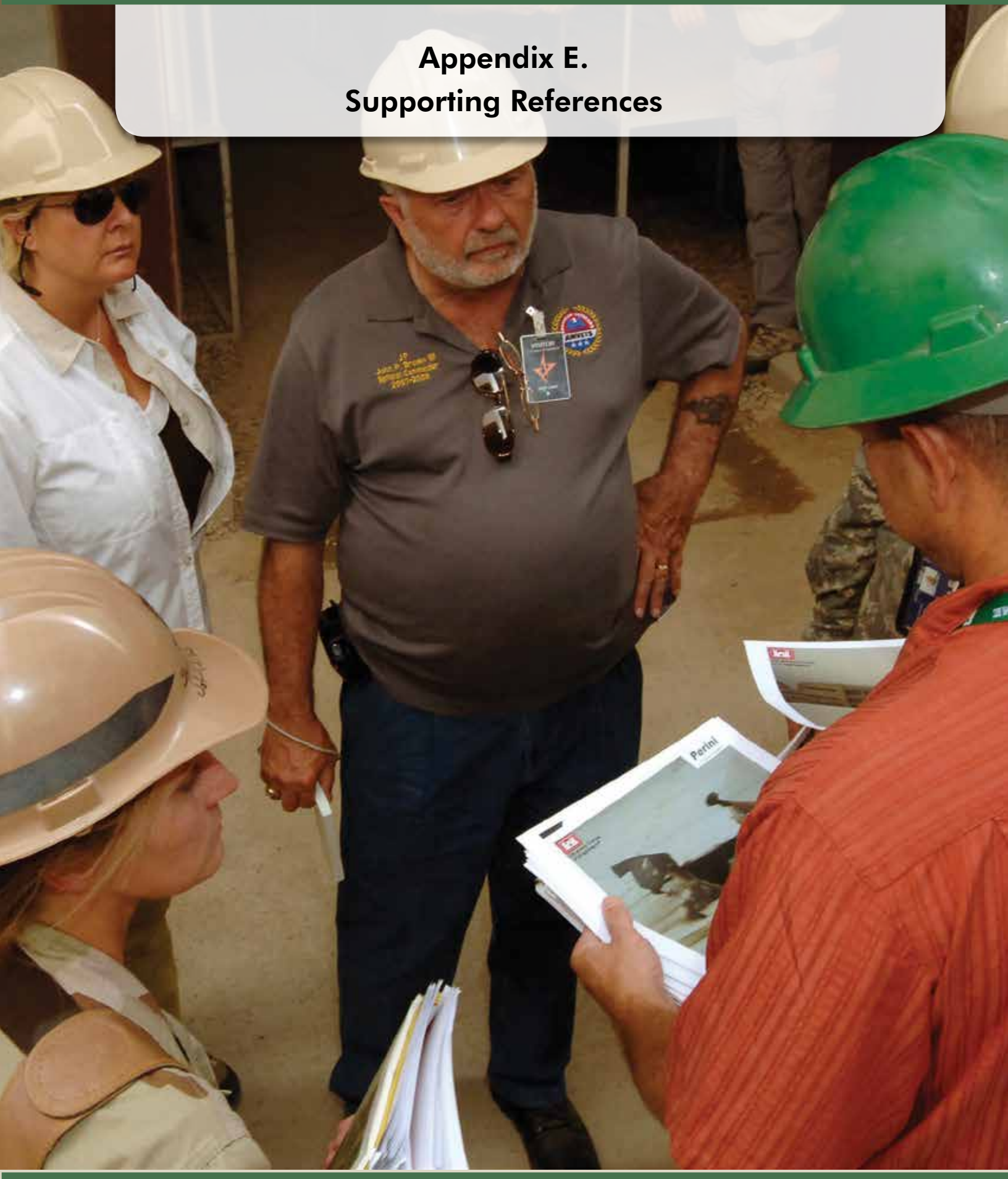
**statement of work.** A formal document that captures and defines the work activities, deliverables, and timeline a vendor must execute in performance of specified work for a client. The SOW usually includes detailed requirements and pricing, with standard regulatory and governance terms and conditions.

**supported unit.** The unit, activity, or organization receiving dedicated contracted support. The supported unit may or may not be the requiring activity.

**Trusted Associate Sponsorship System (TASS).** A web-based system that allows affiliated volunteers (requiring DoD Network access), DoD and uniformed service contractors, foreign affiliates, non-DoD Civil Service employees, non-Federal Agency Civilian Associates, non-US Non-Appropriated Fund Employees, OCONUS hires, and other Federal Agency contractors to apply for a Common Access Card or other Government credential electronically through the Internet. Government sponsors approve the applications to receive Government credentials.

**trusted agent.** A Government employee who administers the Contractor Verification System for an organization by performing the following tasks: (1) creating new contractor accounts in TASS; (2) approving, rejecting, or returning contractor applications; and (3) re-verifying contractor Common Access Card requirements.

# Appendix E.
# Supporting References



Homeland Security Presidential Directive-12, Subject: Policies for Common Identification Standard for Federal Employees and Contractors, 27 August 2004

FARS 52.204-9, Personal Identity Verification of Contractor Personnel

DFARS 225.74, *Defense Contractors Outside the United States*, revised June 2011. http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

DFARS Clause 252.225-7040, *Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed Outside the United States*, revised June 2006. http://farsite.hill.af.mil/zoomcgi/search.cgi

DFARS Clause 252.225-7043, *Antiterrorism/Force Protection Policy for Defense Contractors Outside the United States*, revised March 2006. http://farsite.hill.af.mil/zoomcgi.search.cgi

DFARS 252.239-7001, *Information Assurance Contractor Training and Certification*, revised January 2008. http://farsite.hill.af.mil/zoomcgi/search.cgi

DoD 8570.01-M, *Information Assurance Training, Certification, and Workforce Management*, 15 August 2004, certified current as of 23 April 2007. http://www.dtic.mil/whs/directives/index.html

DoDD 5205.02, *DoD Operational Security Program*, 6 March 2006. http://www.dtic.mil/whs/directives/index.html

DoDD 8570.01M, *Information Assurance Workforce Improvement Program*, 19 December 2005, Incorporating Change 2, 20 April 2010. http://www.dric.mil/whs/directives/index.html

FAR 52.204-2, *Security Requirements* (revised August 1996). https://www.acquistion.gov/far

JP 4-10, *Operational Contract Support*, 16 July 2014. http://www.dtic.mil/doctrine/new_pubs/jointpub.htm

Army Directive 2011-08 (Army Implementation of Homeland Security Presidential Directive-12), 26 May 2011

Army Directive 2014-05 (Policy and Implementation Procedures for Common Access Card Credentials and Installation Access for Uncleared Contractors), 7 March 2014

AR 25-2, *Information Assurance*, 23 March 2009. http://www.apd.army.mil

AR 190-13, *The Army Physical Security Program*, 13 February 2011. http://www.apd.army.mil

AR 380-10, *Foreign Disclosure and Contacts with Foreign Representatives*, 22 June 2005. http://www.apd.army.mil

AR 525-13, *Antiterrorism*, 11 September 2008. http://www.apd.army.mil

AR 530-1, *Operations Security*, 19 April 2007. http://www.apd.army.mil

AR 715-9, *Operational Contract Support Planning and Management*, 20 June 2011. http://www.apd.army.mil

Army ALARACT 110/2011 Message Subject: Potential Installation Access Control Vulnerability with Non CAC Eligible Contractors DTG: 212251Z Mar 11

ATTP 4-10, *Operational Contract Support Tactics, Techniques, and Procedures*, 20 June 2011. http://www.apd.army.mil

This publication supersedes the previous edition, "Integrating Antiterrorism and Operations Security Into the Contract Support Process: Desk Reference," dated 25 January 2012.

This publication is available at the Army Antiterrorism Enterprise Portal (https://west.esps.disa.mil/army/sites/APP/OPMG/OPS/antiterror/ATEP/default.aspx)

**Publication Information**

Offices of primary responsibility:
Headquarters, Department of the Army (HQDA), Office of the Provost Marshal General (OPMG)

Developed in coordination with:
Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology

Send suggested changes to:
HQDA OPMG, aocatbranch@conus.army.mil



Always Ready, Always Alert
*Because someone is depending on you*