**Army Regulation 715–30**

**Procurement**

# Secure Environment Contracting

**Headquarters**
**Department of the Army**
**Washington, DC**
**23 September 2019**

**UNCLASSIFIED**

# *SUMMARY of CHANGE*

AR 715–30
Secure Environment Contracting

This major revision, dated 23 September 2019—

- Amends policies and procedures in the introduction (para 1–6*c*(2)).

- Corrects assignments of responsibilities, addresses, points of contact, and changes references to revised organizations and offices (chaps 1, 2, and 3).

- Changes Head of the Contracting Activity/Principal Assistant Responsible for Contracting conducted Procurement Management Review frequency for their Security Environment Contracting offices to align with the procurement management review frequency set forth in the Army Federal Acquisition Regulation Supplement (para 2–15).

- Changes requirements in the application, collection, and storage of past performance in source selection, contract award reporting for secure environment contracting, and audit follow-up (chap 3).

- Changes requirements and inserts policies and procedures in the contracting process for Special Access Programs (para 3–12).

- Revises the Requiring Activity Contract Support Guidelines (app B).

**Headquarters**
**Department of the Army**
**Washington, DC**
**23 September 2019**

# *Army Regulation 715–30

**Effective 23 October 2019**

**Procurement**

# Secure Environment Contracting

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
*General, United States Army*
*Chief of Staff*

Official:

KATHLEEN S. MILLER
*Administrative Assistant*
*to the Secretary of the Army*

**History.** This publication is a major revision.

**Summary.** This regulation concerns contracts and purchases made using procurement procedures executed and administered in a secure environment. It also establishes policies, procedures, doc-mentation, reporting requirements, and oversight responsibilities for such contracts.

**Applicability.** This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. It also applies to all procurement actions required to be conducted in a secure environment (secure environment contracting). Secure environment contracting applies to support of Special Access Programs, sensitive compartmented information requirements, Top Secret requirements, and other approved secure contracting requirements.

**Proponent and exception authority.** The proponent of this regulation is the Assistant Secretary of the Army (Acquisition, Logistics and Technology). The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field-operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

**Army internal control process.** This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix C).

**Supplementation.** Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (SAAL–PP), 103 Army Pentagon, Washington, DC 20310–0103.

**Suggested improvements.** Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Assistant Secretary of the Army (Acquisition, Logistics and Technology) (SAAL–PP), 103 Army Pentagon, Washington, DC 20310–0103.

**Distribution.** This regulation is available in electronic media only and is intended for command levels the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

**Contents** (Listed by paragraph and page number)



*This regulation supersedes AR 715–30, dated 1 February 2013.



**UNCLASSIFIED**

## Contents—Continued

## Chapter 1
## Introduction

### 1–1. Purpose
This regulation ensures contracts executed and administered in support of acquisitions by and for the activities listed in paragraph 1–6*a* are conducted in accordance with existing laws and regulations, and provides related policies and procedures. This regulation is applicable to all classified contracts. Secure environment contracting (SEC) is necessary to support activities with special security, operations security (OPSEC), or special access needs beyond those normally afforded collaterally classified documents. This regulation establishes policies, procedures, documentation, reporting requirements, and oversight responsibilities in support of contracts that require SEC procedures and emphasizes planning, execution, exceptions, and accountability.

### 1–2. References and forms
See appendix A.

### 1–3. Explanation of abbreviations and terms
See glossary.

### 1–4. Responsibilities
Responsibilities are listed in chapter 2.

### 1–5. Records (recordkeeping) management requirements
The records management requirement for all record numbers, associated forms, and reports required by this regulation are addressed in the Records Retention Schedule-Army (RRS – A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS – A, see DA Pam 25 – 403 for guidance.

### 1 –6. Policies and procedures
*a.* The policies and procedures in this regulation include but are not limited to the following:

(1) Contracts with Special Access Program (SAP) requirements (see para 3–12 and AR 380–381).

(2) Contracts involving sensitive compartmented information (SCI) requirements (other than for purely personnel clearance purposes) (see AR 380–28).

(3) Contracts funded with intelligence contingency funds.

(4) Foreign materiel acquisition (FMA) program requirements (see AR 381–26).

(5) Collaterally classified contracts.

(6) Contracts where the true identity of either or both parties must be concealed (see AR 381–102).

*b.* The SEC generally supports the following principal mission areas, organizations, and activities:

(1) Special operations forces.

(2) Special intelligence operations.

(3) Research, development, and acquisitions associated with sensitive advanced weapons and technology.

*c.* It is Army policy to use SEC procedures for all contracts in the activities described in paragraph 1–6*a*. The steps for determining when SEC procedures apply are as follows:

(1) After consulting with requirements, security, and legal representatives, the contracting officer will determine if SEC methods are applicable. Disagreements will be resolved by the Principal Assistant Responsible for Contracting (PARC) or their designee who possesses the appropriate security clearance level and/or is read on to the SAP, if applicable.

(2) SEC responsibilities will be accomplished by appropriately cleared and indoctrinated personnel through the chain of command and the Head of the Contracting Activity (HCA) or the PARC when the Deputy Assistant Secretary of the Army for Procurement (DASA (P)) has delegated SEC authority to the PARC as requested by the HCA. All personnel within the chain of command will possess security clearances commensurate with their duties. Personnel with oversight responsibilities (such as supervisors, managers, or policy staff) will be indoctrinated, as necessary, to provide oversight of the SEC function.

(3) SEC will be planned, executed, and administered in accordance with the body of law and regulations pertaining to the contracting function. The requirement for security clearances and program indoctrinations will not be used to eliminate

participation of requisite personnel in the SEC process or restrict access to information necessary to properly plan, review, award, and administer and oversee the contracting requirements. SEC will not be considered an exception to the requirement to perform advanced procurement planning. The references at appendix A prescribe pertinent contracting and security laws, regulations, policies, and ethics for affected Army personnel.

*d.* Classification guides prepared in accordance with AR 380–5 and AR 380–381 will include guidance on classification of procurement and related acquisition documents.

*e.* SEC will only be conducted by warranted contracting officers, duly authorized representatives of the contracting officer, and properly appointed ordering officers. The contracting officer, legal counsel, and other functional personnel will be indoctrinated to a program at a level commensurate with their responsibility to plan, review, award, and administer the contracting requirement. Disagreements regarding the need to indoctrinate contracting personnel will be resolved by the PARC and/or HCA.

*f.* Contracting personnel will be granted access to all information necessary to perform their duties and will be indoctrinated or briefed when a valid need-to-know exists. Disagreements regarding requests for access will be resolved by the access approval authority and PARC and/or HCA.

*g.* Contracts will comply with all applicable statutes and Federal, Department of Defense (DOD), and Department of the Army (DA) regulations. For contracting in a secure environment, established contracting offices and officials may be authorized to obtain or approve deviations from procedures prescribed by regulations, but only as specified in those regulations. Notwithstanding the need for security, flexibility, and adherence to sound contracting procedures is mandatory, including as a minimum:

(1) Authorization and validation of requirements.

(2) Certification of fund availability.

(3) Legal sufficiency.

(4) Procurement integrity.

(5) Fair and reasonable price.

(6) Appropriate determinations.

(7) Appropriate contract audit and administration.

(8) Retention of contract files.

(9) Personal accountability for all actions taken.

*h.* In addition to the normal contracting process, SEC procedures require additional considerations:

(1) Requests for assistance and guidance will be submitted through SEC procurement channels to the DASA (P) (SAAL–PS), Potomac Gateway North, 4th Floor, Arlington, VA 22202–4907:

*(a)* Authorization to use procedures not otherwise authorized by this regulation.

*(b)* Obtaining SEC support from existing Army HCAs and contracting offices.

*(c)* Functional procedures and use of appropriate contracting techniques to achieve unique or complex objectives.

*(d)* Processing of classified procurement documents by appropriately cleared and indoctrinated personnel, such as justifications, deviations, and waivers and other procurement actions requiring authorization or approval by the DASA (P) or Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA (ALT)).

(2) Use of special procedures, when authorized per paragraph 1–6*h*(1), may be required during the contracting process to minimize risks of security compromise. These would include special procedures for the following:

*(a)* Solicitation and justification and approval for other than full and open competition.

*(b)* Audit.

*(c)* Reporting of statistics.

*(d)* Collection and use of past performance information (exemption from reporting performance information into Contractor Performance Assessment Reporting System (CPARS) database).

*(e)* Storage of information.

*(f)* Resolution of disputes.

*(g)* Payments (for example, use of government purchase card (GPC) or cash).

*(h)* Use of a prime contractor to mask identification of contracting parties.

*(i)* Contract administration.

(3) SEC programs will establish procedures for reporting alleged or suspected criminal activity to the U.S. Army Criminal Investigation Command (USACIDC) per Department of Defense Instruction (DODI) 5505.02 , AR 195–2, and AR 380–381.

*i.* SEC will use information technology (IT) capabilities that comply with Federal Information Security Management Act (FISMA); Title 44, United States Code, Section 3554 (44 USC 3554); 5 Code of Federal Regulations (CFR) Part 731 (5 CFR 731); 5 CFR 732; Executive Order 10450 (EO 10450); EO 13526; and EO 12968 requirements and Army procedures prescribed by the CIO and Commander, U.S. Army Cyber Command (ARCYBER).

### 1–7. Exceptions

Requests for exceptions to this regulation will be submitted to the DASA (P) (see address in para 1–6*h*(1)) and will include the following:

*a.* A reference to the provisions to which the exception is required.

*b.* A brief statement of the facts in support of the exception and mission impact if the exception is not approved.

*c.* A reference to any other provision of law or regulation that affects the exception.

*d.* An indication of when (in time) the exception is required to meet planned procurement lead times.

### 1–8. Objectives

Objectives of this regulation are as follows:

*a.* To establish and maintain a secure contracting capability that provides user and procurement personnel with appropriate procedures for acquiring supplies, services, and construction in a manner that is legal, supports the mission and security requirements, and is in the best interest of the Government.

*b.* To ensure the identification and use of adequate checks and balances, accountability, and oversight, and to define reporting responsibilities for SEC in order to assure adherence to appropriate laws, regulations, policies, and procedures.

## Chapter 2
## Responsibilities

### 2–1. Chief of Staff, Army

On behalf of the CSA, the Director, Army Special Programs Directorate/Army Special Access Program Central Office (ASPD/SAPCO) will—

*a.* Provide oversight of SEC supporting SAP.

*b.* Coordinate with SEC offices, ASA (ALT) System Special Programs Directorate (SAAL–SSPD), and the cognizant program security officer(s) (PSO) to ensure SEC Special Access Program Facilities (SAPF) are appropriately accredited to store, discuss, and process the supported SAPs.

*c.* Coordinate with ASA (ALT) to ensure execution of SEC for SAP is compliant with AR 380–381 and applicable DOD policy and instructions.

*d.* Review the DD Form 254 (Department of Defense Contract Security Classification Specification) for all Army SAP SEC contracts.

*e.* Provide supplemental SAP security guidance for SAP SEC, as required.

*f.* Coordinate with the Chief Information Officer/G6 (CIO/G–6) SAP Authorizing Official to ensure appropriate authorization of Information systems (IS) processing SAP SEC.

*g.* Coordinate with the Department of the Army Inspector General (DAIG) and Army Audit Agency to ensure SEC offices are included on the Army Sensitive Activities List and inspected/reviewed, as required.

### 2–2. Assistant Secretary of the Army (Acquisition, Logistics and Technology)

The ASA (ALT) will—

*a.* Develop SEC policies and special contracting procedures and support.

*b.* Assure appropriate Army management and implementation of SEC procedures.

*c.* Provide oversight of SEC execution and management.

*d.* Coordinate SEC actions with the appropriate DA and DOD staff elements.

*e.* Approve exceptions to this regulation.

*f.* On behalf of the ASA (ALT), the DASA (P) will—

(1) Ensure that personnel performing SEC duties are adequately trained, possess appropriate clearances, and are indoctrinated when a valid need-to-know exists.

(2) Process SEC actions requiring Headquarters, Department of the Army (HQDA) or higher-level approval.

(3) Execute an oversight program to assess the efficiency and effectiveness of SEC contracting offices, to include the following:

*(a)* Revalidating all SEC contracting activities.

*(b)* Establishing reporting requirements (for example, contract awards and notification of pending external inspections).

*(c)* Conducting procurement management reviews (PMRs) and/or participating in contracting command PMRs of SEC offices.

(4) Develop and promulgate procurement policies affecting SEC.

(5) Respond to requests for assistance and guidance.

(6) Designate specific contracting offices as requested by the HCA to plan, execute, and manage SEC contracts for their command.

### 2–3. Assistant Secretary of the Army (Financial Management and Comptroller)

The ASA (FM&C) will—

*a.* Develop financial and budgeting guidance for SEC.

*b.* Provide staff support and execution review for SEC requirements at the program appropriation level.

*c.* Provide cost estimating support for selected SEC actions.

*d.* Ensure coordination with ASA (ALT) on SEC activities.

### 2–4. Chief Information Officer/G–6

The CIO/G–6 will—

*a.* Prescribe Army IT strategy, policy, portfolio management, architecture, and strategic communication involving SEC activities and projects.

*b.* Prescribe IT Service Portfolio Management policy and practices that maximize business values and align, prioritize, and minimize risk.

*c.* Enforce compliance with FISMA; 44 USC 3554; 5 CFR 731.102; and EO 13526, Section 4.1a concerning SEC activities and projects.

*d.* Review and approve SEC Federal information processing requirements in coordination with ASA (ALT).

*e.* Ensure coordination with ASA (ALT) on SEC activities.

### 2–5. Deputy Chief of Staff, G–2

The DCS, G–2 will—

*a.* Coordinate with and assist other Army staff agencies in intelligence assessment, threat assessment, and necessary counterintelligence support for the execution of SEC. Provide counterintelligence support to SEC offices, as requested.

*b.* Identify requirements for nonstandard items for sensitive intelligence activities.

*c.* Identify requirements for Foreign Material Acquisition (FMA) in accordance with AR 381–26. Coordinate FMA SEC with applicable Army Staff offices.

*d.* Ensure all DCS, G–2 activities develop applicable security classification guidance for the activity's SEC actions and promulgate this guidance to SEC offices and ASA (ALT). Ensure applicable Security Classification Guides (SCG) for sensitive intelligence activities using SEC are made available to SEC personnel executing the support.

*e.* Ensure coordination with ASA (ALT) on SEC activities.

### 2–6. Deputy Chief of Staff, G–3/5/7

The DCS, G–3/5/7 will—

*a.* Review combat developments, concepts, systems, and operations.

*b.* Approve requirements for acquisition of nonstandard items of equipment for special operations forces.

*c.* Ensure coordination with ASA (ALT) on SEC activities.

### 2–7. Deputy Chief of Staff, G–4

The DCS, G–4 will—

*a.* Provide guidance and oversight of integrated logistics support efforts for programs requiring SEC.

*b.* Support requirements for procurement of nonstandard items of equipment for special missions, to include requirements for expedited procurement requests.

*c.* Ensure coordination with ASA (ALT) on SEC activities.

### 2–8. Chief of Engineers

The COE will—

*a.* Provide military construction support for all Army approved facilities.

*b.* Provide reimbursable construction support for Army SEC customers, Non-Army DOD SEC and Non-DOD SEC customers when requested by the host installation commander, as demonstrated in the installation master plan, AR 210–20, or with a waiver by the Army command (ACOM), Army service component command (ASCC), or direct reporting unit (DRU) owning the installation.

*c.* Acquire real property, to include lease, for SEC customers in accordance with AR 405–10.

*d.* Ensure coordination with ASA (ALT) on SEC activities.

*e.* Comply with paragraphs 2–11 and 2–14.

*f.* Provide engineering services for programming, design, environmental investigation and remediation, which often accompany construction.

*g.* Provide contracting support that captures existing services provided to cleared contractors.

### 2–9. The Surgeon General

TSG will—

*a.* Provide support for medical research, development, acquisition, and packaging of medical supplies and services, as required.

*b.* Review and approve all medical program SEC requirements.

*c.* Ensure coordination with ASA (ALT) on SEC activities.

### 2–10. The Judge Advocate General

TJAG will—

*a.* Provide legal advice on SEC.

*b.* Review all policy guidance on SEC for legal sufficiency.

*c.* Provide a legal member to the ASA (ALT) SEC oversight team.

### 2–11. Commanders, Army commands, Army service component commands, and direct reporting units

Commanders, ACOMs, ASCCs, and DRUs will—

*a.* Establish capability or a memorandum of understanding (MOU) for support to execute and monitor SEC in assigned commodities and/or areas of responsibility, including any special training required for acquisition team personnel.

*b.* Ensure that personnel performing SEC duties are adequately trained, possess appropriate clearances, and are indoctrinated when a valid need-to-know exists.

*c.* Provide for adequate secure facilities to conduct SEC and secure telecommunications.

*d.* Provide for legal review of actions as identified in the Federal Acquisition Regulation (FAR), Defense Federal Acquisition Regulation Supplement (DFARS), and Army Federal Acquisition Regulation Supplement (AFARS) of all SEC for which they are designated as the responsible HCA or PARC.

*e.* Assure financial and budgetary support is available for SEC.

*f.* Assure security clearance and OPSEC support to SEC.

*g.* Develop (SCG for items to be procured by SEC) prior to release of procurement information to industry. Ensure SCG are made available to SEC contracting offices and ASA (ALT).

### 2–12. Commanding General, U.S. Army Criminal Investigation Command

The CG, USACIDC will—

*a.* Investigate all suspected or alleged criminal activity in or directed against SEC per AR 195–2 and DODI 5505.03.

*b.* Conduct periodic economic crime threat assessments, crime prevention surveys, and target analysis in the SEC to identify crime-conducive conditions and undetected criminal activity and assist in risk assessment per AR 195–2 and AR 380–381.

### 2–13. Commander, U.S. Army Cyber Command

The Commander, ARCYBER plans, coordinates, integrates, synchronizes, directs, and conducts network operations and defense of all Army networks, including networks involving SEC offices and projects and designate specific contracting offices as requested by the HCA to plan, execute, and manage SEC contracts for their command.

### 2–14. Heads of contracting activities

HCAs will—

*a.* Establish a SEC capability or an MOU with an existing SEC office, to accommodate any SEC requirements that may arise.

*b.* Ensure that personnel performing SEC duties are adequately trained, possess appropriate clearances, and are indoctrinated when a valid need-to-know exists.

*c.* Develop and promulgate implementing SEC policies and procedures to the extent necessary.

*d.* Provide for adequate secure space to conduct SEC and secure telecommunications.

*e.* Perform oversight of their SEC offices and actions and ensure that appropriate internal controls are in place.

*f*. Conduct and document PMRs on their SEC offices at least once every 36 months in accordance with AFARS 5101.690, furnishing a copy of the review report to the DASA (P) Review and Oversight Director within 60 days of completing the PMR at the nonsecure internet protocol router network e-mail address for the DASA (P) Review and Oversight Directorate listed at AFARS 5101.290(b)(2)(ii)(B). If a secure internet protocol router network address is needed for transmitting the PMR report, contact the Review and Oversight Director.

*g*. Ensure the requirements of AR 380–381 apply when the SEC is in a SAP facility.

### 2–15. Program, project, and product managers and other managers with requirements

Program, project, product managers, and other managers with requirements for SEC will—

*a*. Verify that the cognizant contracting officer, legal counsel, and other functional personnel (such as, auditors, cost and/or price analysts, logisticians, and reviewing officials) are eligible and suitably vetted for need-to-know at a level commensurate with their responsibilities.

*b*. Furnish the contracting officer all documents necessary to validate requirement approvals.

### 2–16. Contracting officers

*a*. All contracting officers and supporting personnel engaged in the SEC process will be familiar with the contents and requirements of this regulation.

*b*. The contracting function must be supported by accurate and complete data from the requiring activity (including documentation such as market research, an independent Government estimate, technical input to justifications and approvals and determinations and findings, statement of work, statement of objectives, performance work statement, and procurement planning information). Data supporting SEC procurements will not be "sanitized" to classify it at a lower level. Communications between contracting officers and the requiring activity will not be impeded for security reasons, however security requirements must be observed. The contracting officer, contracting activity security manager, and requiring activity will work together to ensure all necessary security conditions (such as program briefings, secure work areas, storage capabilities, and secure telecommunications equipment) are met to enable complete and timely participation by the contracting office. In order to enhance the contracting officer and customer relationship and to provide general guidance for requiring personnel, contracting officers will provide the requiring activity contract support guidelines to customers along with any command or local supplementation when approved by ASA (ALT) (see app B).

## Chapter 3
## Classified Contracting Procedures

### 3–1. Scope

This section addresses procedures and processes that may be used throughout the SEC cycle as necessary to protect sensitive activities and integrity of the procurement process. It also addresses special decision and approval levels and procedures.

### 3–2. Requirements decision process

Reference the Requiring Activity Contract Support Guidelines (see app B). Appendix C provides a checklist to assist in the evaluation of SEC internal controls.

### 3–3. Contracting process

*a*. All classified contracts executed in a secure environment will be accomplished in accordance with appropriate statutes, regulations, and procedures, including those set forth in this regulation.

*b*. Full and open competition will be obtained in accordance with 10 USC 2304, as implemented by Federal Acquisition Regulation Part 6 (FAR 6). The sensitivity of SEC may necessitate contracting in circumstances requiring other than full and open competition. Contract approval authorities for justification for other than full and open competition are contained in FAR 6. In keeping with security considerations, it may be necessary to restrict competition to only cleared sources. When disclosure of the Army's requirements (through synopsis or otherwise) would compromise national security (for example, would violate security requirements), the authority of 10 USC 2304, as implemented by FAR 6.302–6, will be used as the principal authority to limit the number of sources from which it solicits bids or proposals. It will not be used merely because the acquisition is classified or because access to classified matters will be necessary to submit a proposal or to perform the contract. Unacknowledged Army special access programs will not execute full and open competition since the program's existence is classified within the SAP and disclosure compromises national security. Acknowledged

SAPs may execute less than full and open competition when an appropriate justification for exclusion is provided. Contracts awarded using this authority will be supported by written justifications and approvals (see FAR 6, DFARS, and AFARS). Contracting officers will request offers from as many potential sources as is practicable under the circumstances. When limited special security billet structures preclude soliciting all cleared contractors in the competition, efforts should be made to distribute recurring procurement opportunities among different cleared sources.

*c.* When a contractor requires access to classified information, the cognizant security officer is responsible for preparing, signing, and any subsequent revisions of DD Form 254 (Department of Defense Contract Security Classification Specification). These actions will be in coordination with the program or project officer and the cognizant contracting officer prior to any solicitation or award and during the entire life of the contract to include all modifications. The security manager is the official certifying that the security requirements are complete and adequate for performance of the classified contract. AFARS 5104.403 designates the security manager sign as the certifying official (block 17). The contracting officer will be responsible for incorporating DD Form 254 and any revisions into the contract. The contracting officer will forward the completed DD Form 254 to the cognizant security office in Block 6C of DD Form 254. DD Form 254 should be prepared in accordance with AR 380–49, the DD Form 254 Handbook (see http://www.dami.army.pentagon.mil/site/industsec/pub.aspx), and this regulation. See AR 380–28 or appendix C for the applicable addendums.

*d.* SEC will use IT capabilities that comply with FISMA requirements and Army data management and data storage policies and protocols prescribed by the CIO/G–6; DCS, G–2; the Army SAPCO, and Commander, ARCYBER.

### 3–4. Announcement of contract awards

*a.* FAR 5.303, Defense Federal Acquisition Regulation Supplement Part 205.303 (see DFARS 205.303), and AFARS require congressional and public announcement of contract awards. If such announcement may be made in an unclassified manner, follow the standard procedures outlined in AFARS. However, national security considerations may preclude such announcement. Where the exception at FAR 5.202(a)(1) is applicable, no announcement is required.

*b.* For any other congressional notification requirement, a secure notification process must be followed if release of classified information is involved.

### 3–5. Application and collection of past performance in source selection

*a.* To properly consider past performance in source selection for SEC awards, contracting officers will solicit information from offerors on recent and relevant classified (non-SAP) as well as unclassified prior contractual efforts. As a minimum for non-SAP classified efforts, offerors will be required to identify the relevant contract number and a point of contact at the contracting or contract administration organization.

*b.* Contracting officers will use the CPARS, as required by AFARS, for unclassified past performance data.

*c.* Contracting officers are encouraged to manually register and complete assessment reports on science and technology contracts and delivery/task orders under budget accounts for business sectors 6.1 (Basic Research), 6.2 (Applied Research), and 6.3 (Advanced Technology Development) over $1,000,000, consistent with the threshold for services, although completion of past performance evaluations is not mandatory for these types of contracts.

*d.* For classified past performance information, SEC offices should establish and maintain a local repository, which may be the SEC office contract file, with information that contracting officers may use during source selection. The assessment reports format employed should be consistent with the CPARS format for unclassified efforts.

### 3–6. Protest procedures

When a SEC contracting officer receives a protest, the contracting officer will promptly notify the appropriately cleared servicing legal office.

### 3–7. Contract reporting for secure environment contracting

SEC actions will be reported in accordance with Procedures, Guidance, and Information 204.606. SEC actions are not exempt from the contract reporting requirements in DFARS 204.606, unless the purchases are made under classified contracts, agreements, or orders.

### 3–8. Audit follow-up

*a.* SEC contracting offices must comply with the audit follow-up requirements of DODI 7640.02. SEC contracting officers for SAP and other highly classified contract actions are to use the full audit services of the Defense Contract Audit Agency (DCAA) and fully comply with audit follow-up requirements.

*b.* PARCs will establish Overage Audit Review Boards when required by AFARS. The only difference in the process described in AFARS is the requirement to use properly cleared and indoctrinated personnel to review overage reportable

SEC audits. PARCs will ensure that an Overage Audit Review Board is established and operating for all SEC offices as well as their other contracting offices.

*c.* Whenever security requirements permit, reportable audits will be reported using the Army Contract Audit Follow-up Automated Program. When security requirements prohibit the use of the automated program, the reportable audit information identified in AFARS will be maintained in the contract file. The submission point for contract audit follow-up reports that require special handling due to security requirements will be DASA (P) (see address in para 1–6*h*(1)).

### 3–9. Contract closeout

SEC contracts should be closed using normal closeout procedures in accordance with FAR 4.804–1 and DFARS 204.804 with the understanding that all documents require treatment at the original level of classification until eligible for destruction. Contract documents shall be destroyed in accordance with approved secure procedures; for example, burn bag, secure shredder, and designated SAP shredder for that specific program only.

### 3–10. Freedom of Information Act

*a.* All SEC Freedom of Information Act (FOIA) requests will be processed through a cleared and indoctrinated FOIA officer who has been designated to handle such requests. The FOIA officer must seek legal advice from a cleared attorney in the servicing legal office. There is an exemption in the FOIA for properly classified documents, but this does not necessarily mean all documents in support of a classified program may be denied.

*b.* An appropriate security review must be completed for any information proposed for release prior to the rendering of a release determination.

### 3–11. Staffing procedures for secure environment contracting approvals

Following the established chain of command, all SEC documents requiring approval above the HCA level will be submitted to the DASA(P) address cited in paragraph 1–6*h*(1).

### 3–12. Requirements for Special Access Programs

*a.* Special Access Programs are established for a specific class of classified information imposing safeguarding and access requirements that exceed those normally required for information at the same classification level.

*b.* Army contractual efforts supporting SAPs will be managed in accordance with the following regulations and manuals prescribing the management, administration, oversight, and security requirements unique to SAP:

(1) AR 380–381.
(2) DODD 5205.07.
(3) DODI 5205.11.
(4) DODM 5205.07.
(5) Joint SAP Implementation Guide (JSIG).
(6) Additionally contractors will comply with the current version of the DOD 5220.22–M.
(7) Army SAP Insider Threat Implementation Guidance.

*c.* Contracting officers planning, executing, or managing a contract protected as special access required or requiring access to classified information within a SAP will comply with the above documentation, the guidance provided in this regulation, and any supplemental guidance promulgated by the ASPD.

*d.* All Army SAPs will align with an designated SEC cell.

*e.* SEC supporting SAPs must be conducted within an appropriately accredited SAPF.

*f.* Personnel executing SEC supporting SAPs must be accessed to the requisite programs. Program access will be coordinated with the cognizant PSO.

*g.* SEC supporting SAPs must be processed on information systems (IS) authorized by the CIO/G–6 SAP Authorizing Official.

*h.* Use of automated contracting writing software (for example, Army Contract Writing System) is prohibited for SAP contracts on non-authorized information systems. This includes SAP contracts authorizing access to SCI in addition to SAP.

*i.* All contracts requiring access to SAP information will include a DD Form 254 (Block 10f marked “Yes”) and an appropriately completed SAP Attachment A establishing the security requirements, policies, and procedures for contract execution (see app C template). A list of the relevant security reference documents including applicable Security Classification Guide(s) will be provided in the DD Form 254, block 13.

*j.* Announcement of SAP contract award will be in accordance with the exception at FAR 5.202(a)(1). If the exception does not apply, an unclassified award announcement will be vetted through the cognizant SAP program manager (PM) and PSO to the Army SAPCO for a determination to release.

*k.* Use of Defense Contract Management Agency (DCMA) and the Defense Audit Agency to support SAP SEC as specified in paragraph 3–19 is authorized provided the supporting personnel, facilities, and IS comply with paragraphs 3–12*e*, 3–12*f*, and 3–12*g*.

### 3–13. Requirements for Sensitive Compartmented Information contracts

*a.* Army contractual efforts containing SCI will be managed in accordance with AR 380–28, which is used in conjunction with the following manuals:

(1) DODM 5105.21, Volume 3.

(2) Defense Intelligence Agency Directive 8500.100.

*b.* The release of SCI to an Army contractor or consultant requires specific security safeguards in addition to those specified in DODM 5105.21, Volumes 1–3 and DODM 5220.22, Volume 2. Commander, U.S. Army Intelligence and Security Command, through the contractor support element (CSE) or its successor organization, acting on behalf of DCS, G–2, as the cognizant security authority for the Army, has exclusive administrative security oversight responsibility for all SCI released to the contractor or developed under the Army contract. All Army SCI contracts will be processed through the Army Centralized Contracts & Security. (ACCS), which is overseen by the CSE. See the handbook for SCI contracts and the ACCS User Guide for additional guidance and responsibilities for CSE, contracting officer representative (COR), and facility security officers. Copies of the handbook can be obtained from the Army Contractor Automated Verification System website once an account has been established. Accounts are available at https://accs.army.mil/registration/.

*c.* The Defense Security Service has security inspection responsibility for DOD SCI contractors and retains responsibility for all collateral information released or developed under the contract and held within the DOD contractor's Sensitive Compartmented Information Facility.

*d.* The contractor must obtain a final top secret facility clearance prior to initiating the SCI portion of the contract. Failure to obtain a Top Secret facility clearance is justification for terminating the contract.

*e.* DODM 5105.21, Volume 3 contains information on completion or termination of contracts, visitor control, information security, administrative handling, and accountability of SCI. DIAD 8500.100 contains information regarding compartmented computer operations.

### 3–14. Secure contracting requirements using other than simplified acquisition procedures

SAP, SCI, and FMA requirements will follow SEC procedures. Simplified purchases will follow secure environment simple purchases (SESP) procedures as outlined in paragraph 3–16 through paragraph 3–18 of this regulation. Use of SEC procedures for any other requirement requires prior approval by the HCA or PARC, if delegated. Such approval may be obtained on a program or project basis as follows:

*a.* Commanders or heads of HQDA activities generating a SEC requirement other than a SAP, SCI, or FMA requirement will forward requests for approval to use SEC procedures to their supporting contracting command HCA, via their cleared command and/or contracting channels prior to initiating any contract action. The request must contain the following:

(1) Justification for request.

(2) Description of the item or non-personal service to be acquired. Personal services may be procured under limited circumstances such as in overseas locations, in support of intelligence organizations, or in support of DOD Special Operations Command (see 10 USC 129 and DFARS 237.104).

(3) Estimated cost.

(4) Date supply or service is required.

(5) Proposed SEC contracting office.

(6) Any other special considerations.

*b.* The project sponsor or other requiring activity will submit complete and proper documentation to the designated SEC contracting office for execution of the procurement action (see app B).

### 3–15. Secure environment contracting office designation process

The DASA (P) will designate specific contracting offices as requested by the HCA to plan, execute, and manage SEC contracts for their command. Contracting officers will not process a requirement in this category without ascertaining that the DASA (P) has designated their office to perform SEC for their command. The DASA (P) authority to designate SEC offices may not be delegated.

### 3–16. Secure environment simple purchases

*a.* Simple purchases may be made to satisfy secure environment operational requirements using simplified acquisition procedures as set forth in FAR 13 and this regulation. Secure environment simplified purchasing may also be used by contracting officers in satisfying purchase requirements under the simplified acquisition threshold when cover is required (see AR 381–102). SESP contracting officers or properly appointed secure environment ordering officers may perform required SESP as authorized by the HCA or PARC and their contracting officer's warrant or ordering officer's appointment.

*b.* The SESP contracting or ordering officer may use a Standard Form (SF 44) (Purchase Order Invoice Voucher) when contracting in a secure environment (regardless of location). The SF 44 may be used to acquire goods or services that do not exceed the simplified acquisition threshold (or micro-purchase threshold, when applicable) and when use of the GPC is impracticable. Maximum micro-purchase threshold limitation applies to ordering officers (AFARS). When SF 44s are used in a secure environment to protect the buyer's identity, the seller will not provide a signature. Therefore, attach the receipt from the vendor to the SF 44 when submitting for processing. When circumstances do not permit obtaining a receipt from the vendor, the contracting or secure environment ordering officer will execute a certification of the expenditure. The certification of expenditure will include:

(1) The date and location of the purchase.
(2) A description of the goods or services.
(3) The cost of the goods or services.
(4) The name of the vendor (seller).
(5) The signature of the SESP contracting or ordering officer.

### 3–17. Secure environment simple purchases procedures

*a.* SESP procedures provide guidance for Army support of sensitive operations, are pre-approved for SEC, and are not addressed by FAR 13. When contingency contracting officers are involved in SEC contracting actions, they will comply with this regulation.

*b.* SESP contracting and ordering officers will ensure that all SEC actions are justified and supported by appropriate documentation, such as required justification, a statement of work or schedule or performance period, and appropriate funding.

*c.* These procedures apply to all Army activities supporting operations whose requirements are such that security considerations are of critical importance. Their functions must also be performed in ways that will not compromise or preclude accomplishment of sensitive operations, yet comply with applicable laws and regulations.

### 3–18. Secure environment simple purchases methods of operation

*a.* Authorized SESP contracting and ordering officers will exercise contracting and secure environment ordering officer authority only when necessary for mission performance.

*b.* HCAs (through the PARC) will perform functional reviews of SESP contracting and ordering officers for control purposes.

### 3–19. Contract administration and contract audit support

*a.* Contracting officers may delegate SEC contract administration authority and responsibility to the DCMA. DCMA can provide the full range of contract administration support for SEC contracts, to include pricing support.

*b.* Contracting officers may also use the DCAA audit assets and services. DCAA has responsibility for the full range of contract audit support for SEC contracts.

*c.* DCMA and DCAA have appropriately cleared personnel to provide requisite support. If used to support SAP SEC, contracting officers will coordinate with the cognizant SAP PSO for requisite SAP access(es), facility accreditation and IS authorization.

*d.* Contact the DASA (P) for referral to these agencies.

### 3–20. Security support

For security support for collateral contracts, refer to AR 380–49. For SCI contracts, refer to AR 380–28. For SAP contracts, refer to AR 380–381.

### 3–21. Criminal investigative support

*a.* Contracting officers will report all instances of known or suspected criminal activity within SEC to USACIDC, field investigative unit.

*b.* Contracting officers will support the field investigative unit in its periodic update of the SEC Economic Crime Threat Assessments Survey.

## Appendix A

## References

### Section I

### Required Publications

**AR 380–5**
Department of the Army Information Security Program (Cited in para 1–6*d*.)

**AR 380–381**
Security Special Access Programs (SAPS) and Sensitive Activities (Cited in para 1–6*a*(1).)

**AR 405–10**
Acquisition of Real Property and Interests Therein (Cited in para 2–8*c*.)

**AR 750–43**
Army Test, Measurement, and Diagnostic Equipment (Cited in para B–4*i*.)

**DOD 5500.7–R**
Joint Ethics Regulation (JER) (Cited in para B–2*b*(1).)

**DODI 7640.02**
Policy for Follow-up on Contract Audit Reports (Cited in para 3–8*a*.)

### Section II

### Related Publications

A related publication is a source of additional information. The user does not have to read a related publication to understand this regulation. AFARS is available at http://farsite.hill.af.mil. CFRs are available at http://www.efcr.gov/. DFARs are available at http://www.acq.osd.mil. EOs are available at http://www.archives.gov. DOD publications are available at http://www.dtic.mil/whs/directives/. FARs publications are available at http://www.acquisition.gov/far/. USCs are available at http://www.gpo.gov/fdsys/.

**AFARS**
Army Federal Acquisition Regulation Supplement

**AR 11–2**
Managers' Internal Control Program

**AR 11–7**
Internal Review Program

**AR 25–1**
Army Information Technology

**AR 25–2**
Army Cybersecurity

**AR 25–30**
The Army Publishing Program

**AR 70–1**
Army Acquisition Policy

**AR 70–13**
Management and Oversight of Service Acquisitions

**AR 195–2**
Criminal Investigation Activities

**AR 210–20**
Real Property Master Planning for Army Installations

**AR 380–28**
Army Sensitive Compartmented Information Security Program

**AR 380–49**
Industrial Security Program

**AR 381–10**
U.S. Army Intelligence Activities

**AR 381–26**
Army Foreign Materiel Program (U)

**AR 381–102**
Army Cover Program

**AR 381–141**
Intelligence Contingency Funds

**AR 530–1**
Operations Security

**AR 600–85**
The Army Substance Abuse Program

**AR 710–2**
Supply Policy below the National Level

**DA Pam 70–3**
Army Acquisition Procedures

**DFARS Part 242**
Contract Administration and Audit Services

**DFARS 204.606**
Reporting Data

**DFARS 204.804**
Closeout of Contract Files

**DFARS 205.303**
Announcement of Contract Awards

**DFARS 208.7003–1**
Assignments under Integrated Materiel Management (IMM)

**DFARS 215.470**
Estimated Data Prices

**DFARS 237.104**
Personal Services Contracts

**DIAD 8500.100**
Security of Compartmented Computer Operations (Available via SIPRNET at http://www.di-ateams.dse.dia.smil.mil/sites/issuances/default.aspx.)

**DOD 5220.22–M**
National Industrial Security Program Operating Manual

**DODD 5205.07**
Special Access Program (SAP) Policy

**DODI 5205.11**
Management, Administration and Oversight of DoD Special Access Programs (SAPs)

**DODI 5505.02**
Criminal Investigations of Fraud Offenses

**DODI 5505.03**
Initiation of Investigations by Defense Criminal Investigative Organizations

**DODI 8510.01**
Risk Management Framework (RMF) for DoD Information Technology (IT)

**DODM 5105.21, Volume 1-3**
Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities

**DODM 5200.01 Series**
DOD Information Security Program

**DODM 5200.01, Volume 1**
DOD Information Security Program: Overview, Classification, and Declassification

**DODM 5200.01, Volume 2**
DOD Information Security Program: Marking of Classified Information

**DODM 5200.01, Volume 3**
DOD Information Security Program: Protection of Classified Information

**DODM 5200.01, Volume 4**
DOD Information Security Program: Controlled Unclassified Information (CUI)

**DODM 5205.07 Series**
DoD Special Access Program (SAP) Security Manual

**DODM 5205.07, Volume 1**
DoD Special Access Program (SAP) Security Manual: General Procedures

**DODM 5205.07, Volume 2**
DoD Special Access Program (SAP) Security Manual: Personnel Security

**DODM 5205.07, Volume 3**
DoD Special Access Program (SAP) Security Manual: Physical Security

**DODM 5205.07, Volume 4**
DoD Special Access Program (SAP) Security Manual: Marking

**DODM 5220.22, Volume 2**
National Industrial Security Program: Industrial Security Procedures for Government Activities

**EO 10450**
Security Requirements for Government Employment

**EO 12333**
United States Intelligence Activities

**EO 12829**
National Industrial Security Program

**EO 12968**
Access to Classified Information

**EO 13526**
Classified National Security Information

**FAR Part 6**
Competition Requirements

**FAR Part 13**
Simplified Acquisition Procedures

**FAR 3.104**
Procurement Integrity

**FAR 3.104–4**
Disclosure, Protection, and Marking of Contractor Bid or Proposal Information and Source Selection Information

**FAR 4.804–1**
Closeout of Contract Files

**FAR 5.201**
General

**FAR 5.202**
Exceptions

**FAR 5.303**
Announcement of Contract Awards

**FAR 6.302**
Circumstances Permitting Other Than Full and Open Competition

**FAR 6.302–6**
National Security

**FAR 7.402**
Acquisition Methods

**FAR 13.1**
Procedures

**FAR 15.4**
Contract Pricing

**FAR 17.2**
Options

**FAR 17.5**
Interagency Acquisitions

**FAR 23.3**
Hazardous Material Identification and Material Safety Data

**FAR 37.104**
Personal Services Contracts

**FISMA**
Federal Information Security Management Act (Available at https://www.nist.gov/programs-projects/federal-information-security-management-act-fisma-implementation-project.)

**ICD 503**
Information Technology Systems Security Risk Management, Certification and Accreditation (Available at https://www.dni.gov/.)

**ICD 704**
Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information (Available at https://www.dni.gov/.)

**ICD 705**
Sensitive Compartmented Information Facilities (Available at https://www.dni.gov/.)

**JSIG**
Joint Special Access Program (SAP) Implementation Guide (Available at https://www.dss.mil/Portals/69/documents/io/rmf/JSIG_2016April11_Final_(53Rev4).pdf.)

**PGI 204.606**
Reporting Data (Available at http://www.acq.osd.mil/dpap/dars/pgi/pgi_htm/pgi204_6.htm.)

**5 CFR 731**
Suitability

**5 CFR 732**
National Security Positions

**10 USC 129**
Civilian personnel management

**10 USC 129b**
Authority to Procure Personal Services

**10 USC 1588**
Authority to Accept Certain Voluntary Services

**10 USC 2304**
Contracts: Competition Requirements

**31 USC**
Money and Finance

**31 USC 1301**
Application

**31 USC 1341**
Limitations on Expending and Obligating Amounts

**31 USC 1342**
Limitation on Voluntary Services

**31 USC 1517**
Prohibited Obligations and Expenditures

**31 USC 1519**
Criminal Penalty

**44 USC 3544**
Federal agency responsibilities

**44 USC 3554**
Federal agency responsibilities

## Section III

## Prescribed Forms

This section contains no entries.

## Section IV

## Referenced Forms

Unless otherwise indicated, DA Forms are available on Army Publishing Directorate at website http://armypubs.army.mil. DD Forms are available at OSD website http://www.dtic.mil/whs/directives/infomgt/forms/. SFs are available at http://www.gsa.gov.

**DA Form 11–2**
Internal Control Evaluation Certification

**DA Form 2028**
Recommended Changes to Publications and Blank Forms

**DA Form 3953**
Purchase Request and Commitment

**DD Form 254**
Department of Defense Contract Security Classification Specification

**DD Form 1423**
Contract Data Requirements List

**SF 44**
Purchase Order Invoice Voucher (Stocked and Issued from GSA at the Federal Supply Service.)

## Appendix B

## Requiring Activity Contract Support Guidelines

### B–1. Introduction

The following guidance assists requiring activity personnel with the submission of requirements packages. The intent is to familiarize non-contracting personnel with the Federal contracting process. It is not intended to substitute as a review of the pertinent statutes and procurement and finance regulations or for obtaining appropriate legal reviews of proposed contract actions.

### B–2. Ethics

*a.* In all contract-related functions, emphasis is placed upon the importance of protecting the interests of the Government and avoiding acts that may compromise the DA. Public confidence in the integrity of the relationships between the Government and industry is essential.

*b.* To avoid a conflict of interest or even the appearance of a conflict, the following guidance is provided:

(1) The DOD Joint Ethics Regulation is contained in DOD 5500.7–R. Procurement integrity requirements are implemented in FAR 3.104 and its supplements.

(2) An individual should never be in a position to influence or participate in dealings on behalf of the Government with any firm in which the individual has a financial or personal interest. If such a situation is likely to develop, the individual will disclose the matter to his or her supervisor, the cognizant contracting officer, and the ethics advisor. The individual will be removed from activities where a conflict or an apparent conflict of interest may be present.

(3) Government personnel will (in accordance with the DOD Joint Ethics Regulation) refuse any offer of favors, gratuities, considerations, assistance, meals, or entertainment offered to themselves or members of their family by any contractor with whom they are conducting business or expect to conduct business. Contracts may be terminated and penalties applied against a contractor who has been found to have offered gratuities, particularly those that may be defined as bribes. If offered a bribe, the individual will refuse and report the incident to their supervisor.

### B–3. Acquisition

*a. Market research.*

(1) Technical and contracting personnel will jointly conduct market research to identify the availability of commercial or modified commercial items to meet the need and identify potential sources for solicitation and relevant industry terms, conditions, and practices. Market research may be accomplished by one or all of the following means:

*(a)* Review of literature.

*(b)* Contact with trade or professional associations.

*(c)* Contact with organizations having similar missions.

*(d)* Synopsis is posted at http://www.fbo.gov by the contracting officer.

*(e)* Internet research.

*(f)* Conduct site visits/attend trade shows, conferences.

*(g)* Query Government Databases (FPDS–NG), PPIRS, General Services Administration (GSA), FedBizOps (Sources Sought if possible), SBA Dynamic Search.

*(h)* Review recent market research on similar or like items.

(2) While conducting market research, technical personnel must be careful not to disclose specific information that would give a contractor a "competitive advantage." Information made available to one competing contractor must be made available to all. A contracting officer is the proper individual to disseminate such information. The intent of market research is to determine whether there are sources (for example, commercial sources) available to meet the Government's needs. This rule is to preserve the integrity of the Federal procurement system by ensuring that all potential contractors are treated equally to the greatest practical extent. To give a contractor advance procurement details may discriminate against competing contractors. This could result in a sustainable protest, which would prevent contract award.

*b. Communications with industry.*

(1) Often it is essential that a dialogue between Government and industry be opened long before the final preparation of the requirements package. Although the Government's need for preliminary information is sometimes critical, the methods used to obtain information are limited by rules based upon criminal statutes, administrative regulations, and procurement policy. These rules cannot be taken lightly since they are designed to safeguard the integrity of the procurement system, the confidentiality of proprietary information, and the expenditure of appropriated funds.

(2) Technical personnel must guard against revealing specific procurement information on the assumption that there are no competitors to be harmed by the disclosure. The Government's negotiation position may be significantly undermined by untimely disclosure of procurement information. The rules surrounding communications with industry will not be relaxed in apparently noncompetitive situations.

(3) When specific advance information must be disclosed, the disclosure will be made to all potential competitors at the same time. The contracting officer will make all disclosures to potential contractors. This ensures that no single firm will receive a competitive advantage as a result of disclosure. Restricting information flow to only those potential sources known to be properly cleared is authorized.

(4) Proprietary or restricted information (for example, trade secrets or confidential commercial information), as marked by the contractor, must be protected as required by FAR 3.104–4. Review the contractor's markings; if in doubt, ask a procurement official.

(5) When communicating with contractors, care must be taken not to direct a contractor or their personnel to incur costs or perform work. When a Government employee, without procurement authority directs a private entity to incur costs or perform work, it becomes an unauthorized commitment. Only duly appointed or specifically authorized contracting officers and ordering officers, acting within the scope of their warrant or other written authority, can financially obligate the Government. This is particularly sensitive during the preliminary phase of the procurement cycle when communicating with industry about the Government's needs and contractor's capabilities. The best practice is to preface each communication with words to the effect that nothing stated should be interpreted as creating an obligation of the Government to award a contract or to otherwise pay for information.

(6) Generally, absent express statutory authority, the Government may not accept voluntary services. 31 USC 1342 states that no Federal officer or employee will accept voluntary or personal services for the U.S. except in certain emergencies. This law states that any voluntary services rendered to the Government in violation of the law will not legally obligate the Government to make payment and can result in adverse consequences to the Government employee who accepted them. The Government may accept gratuitous services only in limited circumstances allowed by statute (for example, 10 USC 1588), and in those cases, the private entity must agree in writing and in advance to waive any and all claims against the U.S. for such services. However, legal consultation should be sought before accepting.

### B–4. Preparation of a requirements package

*a. General.*

(1) The quality of any contract action, particularly the contract, is dependent upon the quality of the specification and performance work statement, statement of objectives, or statement of work received. In order to get the desired product or result, the description of what is to be purchased must be clear not only to procurement personnel throughout the process, but the prospective contractors. Contractors cannot submit sound proposals without knowing what the Government requires.

(2) Plans, drawings, specifications, purchase descriptions, and statements of work, performance work statements, or statements of objective must state in performance terms the essential valid needs of the Government. They will describe the supplies and services in a manner that will encourage optimum competition (for example, performance results based specifications) and eliminate, to the extent practicable, restrictive features that might unduly limit acceptable offers. Much of the information on what is feasible and acceptable to meet the need will be obtained through market research described in paragraph B–3*a*. Commercial products or services and industry-related commercial practices will be identified and employed to the maximum extent practicable, given mission and security requirements.

*b. Fiscal matters.* 31 USC provides statutory restrictions on the obligation and expenditure of appropriated funds. The following provisions apply to contracting:

(1) 31 USC 1341 and 31 USC 1350 make it a criminal offense for a Federal officer or employee to willfully:

*(a)* Make an obligation or expenditure in excess of the funds available.

*(b)* Authorize an obligation or expenditure in excess of funds available.

*(c)* Involve the U.S. in an obligation in advance of appropriation.

(2) 31 USC 1517 and 31 USC 1519 make it a criminal offense for a Federal officer or employee to willfully violate certain administrative funding limitations.

(3) The Bona Fide Needs Rule requires that appropriated funds be used to meet the bona fide needs of the period for which the funds were available for obligation.

(4) 31 USC 1301 requires that appropriated funds be used for the specific purposes for which they are appropriated or for those objectives that are reasonably necessary for such purposes.

(5) Normally, a commitment document, DA Form 3953 (Purchase Request and Commitment) is prepared and provided as a part of the procurement package. The commitment document furnishes a fund citation with full accounting and appropriation data for the total estimated cost of the procurement.

(6) Advice and assistance should be requested from a budget or financial analyst or resource manager in the chain of command if there are questions in this area.

*c. Sources of supply.* Each requirements package will contain a suggested list of sources and a justification for any proposed limitation of sources. The FAR requires that every proposed procurement in excess of the simplified acquisition threshold be publicly advertised at http://www.fbo.gov, unless covered by the limited exceptions found in FAR 5.202(a)(1) (the local contracting support office is available for advice).

*d. Justification to use other than full and open competition.*

(1) 10 USC 2304 authorizes, under certain conditions, contracting without providing for full and open competition. Contracting without providing for full and open competition or full and open competition after exclusion of sources is a violation of statute, unless permitted by one of the exceptions in FAR 6.302. A justification for use of other than full and open competition must contain specific facts and rationale to justify soliciting from only one or a limited number of sources. The contents and format for this justification are described in AFARS, as supplemented.

(2) It is improper to base a justification for other than full and open competition on the following factors:

*(a) "Goldplating."* The Government is only permitted to purchase supplies or services that meet its actual needs (this does not mean that the Government cannot demand quality in the context of critical applications and life cycle considerations).

*(b) Cost of competition.* The cost reductions achieved through competition generally offset any additional costs that may be associated with the competition. Competition can also save time because time consuming approvals are not necessary and streamlined methods are used to ensure fair and reasonable pricing (for example, cost or pricing data is not required when adequate competition is achieved).

*(c) Opinion or preferences.* Requests for limitation of sources must always be accompanied by supporting factual evidence and rationale.

*(d) Duplication of work.* The sole fact that some minor duplication of earlier efforts would be required is inadequate. The request for limited competition must show specifically the expected cost of such duplication in terms of time and dollars.

(3) The documentary basis for a justification for restricting competition must be prepared by the requesting activity and be a part of the requirements package.

*e. Additional requirements.*

(1) *Delivery schedules.* Delivery schedules must be realistic and responsive to the Government's needs. A compressed schedule may increase both the cost and risk.

(2) *Place of delivery or performance.* The shipping address, as well as marking instructions must be provided for supply items. For services, the places of performance must be specified.

(3) *Packaging and packing.* When the requirement is for supply items, the level of packaging and packing must be specified.

(4) *Quality control.* The contractor is responsible for establishing manufacturing quality and inspection controls to ensure supplies and services delivered to the Government conform to the contract. The quality level expected must be specified.

(5) *Inspection and acceptance.* Specify place of inspection and acceptance.

(6) *Service contracts.* Personal services may generally not be contracted for except for (for example, overseas activities and contingency operations) (see FAR 37.104 and AFARS 5137.104). Personal services can be procured under limited circumstances such as in overseas locations, in support of intelligence organizations, or in support of DOD Special Operations Command (see 10 USC 129b and DFARS 237.104).

(7) *Government-furnished property.* It is Federal policy that contractors will provide all property and supplies required to perform Government contracts. When the program or project officer and the contracting officer determine that Government-furnished property (GFP) must be provided (usually based on factors such as relative cost of acquisition, tracking, and final disposition, including environmental issues), items or information to be provided to the successful contractor as GFP must be specifically identified. Specify dates when the property or information is required and available to be furnished to the contractor.

(8) *Property administrator.* When the procurement office retains contract administration for GFP, a qualified individual will be nominated to perform the duties of property administrator.

(9) *Contracting officer's representative.* When required to ensure that the Government's interests are protected after award of a contract, a qualified individual is nominated by the program or activity and provided as part of the procurement package to the contracting officer who appoints them as the COR. Such appointment is made formally (in writing) and delineates specifically the COR's authority and limitations.

(10) *Hazardous material identification and material safety data.* Refer to FAR 23.3, as supplemented, if there is any question as to whether the requirement will involve contractor delivery of hazardous materials.

(11) *Options.* It may be appropriate to include options in contracts. An option is a unilateral right of the Government to purchase additional supplies or services set forth in the contract, providing the conditions set forth in the FAR 17.2, as supplemented, are met. The justification for a noncompetitive contract containing an option clause will be approved at the level required for the total estimated contract value, including the option(s).

*f. Technical data and computer software requirements.* The Government only acquires rights in technical data or computer software that are required for use of the material or data or software to be delivered under the contract. If data will be needed, the data should be requested and a DD Form 1423 (Contract Data Requirements List) prepared as required by DFARS 215.470.

*g. DD Form 254 requirements.* A DD Form 254 must be a part of the procurement package when release of classified information to the contractor and/or the generation of classified information or material by the contractor are required. Prepare DD Form 254 in accordance with AR 380–49, AR 380–28, or AR 380–381 for the applicable addendums. The DD Form 254 will be signed by the appropriate industrial security specialist (ISS).

*h. Independent Government estimate.* An independent Government estimate provides what the requirement would cost, if provided by a contractor (including overhead and profit). A meaningful independent Government estimate must be provided with every procurement request package as one of the means by which the contracting officer can determine reasonableness of bids or proposals (see FAR 13.1 and FAR 15.4). The complexity of the estimating technique will be commensurate with the complexity of the acquisition.

*i. Test, measurement, and diagnostic equipment.* Prior to submitting a requirement for test, measurement, and diagnostic equipment, approval must be obtained from the test, measurement, and diagnostic equipment product manager (SFAE–CSS–FT–T), Redstone Arsenal, AL 35898–5400, in accordance with AR 750–43. The approval document must be a part of the requirements package.

*j. Commodity assigned items.* Prior to submitting a procurement request package for the local purchase of a commodity assigned item, the requiring activity will comply with the requirements of DFARS 208.7003–1. The supporting contracting office or local director of logistics or equivalent office can provide assistance, as needed.

*k. Leases.* Leasing may be appropriate under certain circumstances. However, the criteria in FAR 7.402, as supplemented, must be followed and an analysis must be done to determine if the cumulative leasing costs will be less than the purchase cost. This analysis should be forwarded to the contracting officer with the requirements package.

*l. Use of government purchase card.* The GPC will be used by contracting and requirements personnel as a simplified purchasing method for commercial supplies and services that do not exceed the micro-purchase threshold. GPCs will only be issued to personnel who have completed mandatory training. Chiefs of contracting offices will provide training, guidance, and oversight to GPC card holders (see AFARS or the supporting contracting officer for more details).

## Appendix C

## Special Access Program Addendum Template

This template will be completed and attached as an addendum to all contracts wherein the DD Form 254 indicates access to Special Access Program information (Block 10f checked "Yes"). Italicized text requires insertion of language specific to the program issuing the contract and adjusted to incorporate current policy and regulation.

### C–1. Introduction

The SAP addendum to DD Form 254 is attached to all contracts wherein the DD Form 254, block 10f is checked "Yes," indicating access to Special Access Program information is required for contract performance.

### C–2. Preparation of a Special Access Program Addendum to DD Form 254

*a.* The requirement for completion of a SAP addendum applies to classified information, facilities, materials, and equipment based on the determination that normal security protections are not adequate for contractor performance and that enhanced security protections are required. The requiring activity is responsible for filling in all technical and security requirements in the addendum to DD Form 254, in conjunction with the Security Manager of the requiring activity. The Contracting Officer will provide assistance as needed.

*b.* The addendum is for use in contracts with U.S. firms. For non-U.S. firms contact the "Nondisclosure Office" in the contingency environment for guidance.

*c.* The addendum to DD Form 254 is part of the contract and a source of expanded security guidance provided by the Government and shall be used to expand or explain information referenced in other sections of the DD Form 254. List applicable clearance levels, government manuals, SCGs, contractor personnel training requirements, page numbers, and other helpful designations in the addendum.

*d.* Each addendum page will be noted with the contract number and page number. There is no set page limit for the addendum. At a minimum, the following should be included.

(1) *Block 13 continued* 1. This attachment establishes the SAP security requirements for the performance of contract "Contract Number" (specify subtasks, if necessary).

(2) Insert coordinating language with other security control programs which are part of the contract (for example, SAP, SCI, FOUO) to establish which program takes precedence in the event of conflicting guidance. Example: Security guidance and requirements provided for contract "*Contract Number"* as stated in the DD Form 254, the DD Form 254 Continuation Pages, the SCI Addendum (Enclosure 1 to the DD Form 254) and the For Official Use Only (FOUO) Addendum (Enclosure 2 to the DD Form 254) will apply unless more stringent requirements are specified in this DD Form 254 Addendum.

(3) *Block 10 (insert block letter a-k).* Contractor personnel must have Insert Clearance, Investigation, and be eligible for Access Requirements. Address all required accesses. Example below*:*

(4) *Block 10e.* Contractor must be eligible for the following SCI accesses: SI, TK. Contractor personnel must:

(5) Have a TOP SECRET security clearance based on a Tier 5 Background Investigation or a periodic review (PR) completed within 6 years of the date of access.

(6) *Maintain a current investigation.* Requests for re-investigation will be submitted 6 months prior to the completion date of the individual's current investigation.

(7) *Block 10f. Contractor personnel granted access to Special Access Program information must:*

(8) Meet access, clearance and investigative requirements as stated in paragraph 3*a*, 3*a*(1), and 3*a*(2).

(9) Be eligible for SAP access in accordance with DODM 5205.07, Volume 2.

(10) Contractor personnel will comply with the following regulations, directives, instructions, and manuals: (*Ensure all relevant references are included. The list below IS NOT all inclusive):*

*(a)* DOD 5200.22–M.

*(b)* DODD 5205.07.

*(c)* DODI 5205.11.

*(d)* DOD Manual 5205.07 Series---

(1) Volume 1 – General Procedures, 18 June 2015.

(2) Volume 2 – PERSEC, 24 November 2015.

(3) Volume 3 – Physical Security w/Change 2, 12 February 2018.

(4) Volume 4 – Marking 10 October 2013, w/Change 1, 9 May 2018.

*e.* DOD Manual 5200.01 Series---

(1) Volume 1. Overview, Classification, and Declassification

(2) Volume 2. Marking of Classified Information w/change 2.

(3) Volume 3. Protection of Classified Information w/change 2.

(4) Volume 4. DoD Information Security Program: Controlled Unclassified Information (CUI) w/change 1.

*f.* DODI 8510.01 – Risk Management Framework (RMF) for DoD Information Technology (IT), Chapter 2, 28 July 2017.

*g.* Joint SAP Implementation Guide (JSIG).

*h.* Intelligence Community Directive 503 (certification/ accreditation of IS dual processing SCI/SAP).

*i.* Intelligence Community Directive 705 (facility accreditation requirements).

*j.* Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities Version 1.3, 10 September 2015 (physical security standards).

*k.* AR 380–381.

*l.* AR 25–2.

*m.* U.S. Army Security Marking Guide for Special Access Programs, 14 February 2013.

*n.* Program Security Classification Guide. (Use Unclassified title).

*o.* Army Special Access Program and Sensitive Activities Insider Threat Training available at https://www.lms.army.mil/saba/web/main/.

(5) *Block 11.* Insert appropriate language for storage, generation, processing, or discussion of SAP information at the contractor's facility. (Example: Block 11a. The Contractor is not authorized to store, generate, process, or discuss SAP information in its facility. Access to SAP information and all Special Access work will be performed at the facilities listed in DD Form 254, block 13. If contractor personnel is authorized to use IS to process, store, and/or transmit SAP information, the IS must be authorized to operate in accordance with the JSIG and current Defense Security Service policy unless carved out.)

(6) *Special Security requirements.* (Example: Block 11l. Contractor personnel performing are subject to random selection for Counterintelligence Scope Polygraph examination in accordance with DoD Directive 5210.48 and random selection for Urinalysis in accordance with AR 600–85. Failure of selected individuals to submit to polygraph examination or urinalysis may result in suspension of access to SAP information.)

(7) *Training.* Contractor personnel will complete the training listed below at the frequency indicated:

*a.* Special Access Program Security Training not later than 30 days after access.

*b.* Special Access Program Security Refresher Training – Annual.

*c.* Army Special Access Enterprise Portal Training – not later than 30 days after access.

*d.* HQDA Computer User Training – not later than 30 days after access. (IS User agreement).

*e.* HQDA Sensitive Information Handling – not later than 30 days after access, then annually.

(1) CIO/G6 Information Assurance Training, Handling Sensitive Information.

(2) OPSEC.

(3) Handling of For Official Use Only Information.

(4) Release of Information to the Media.

(5) Release of Information to Congress.

(6) Badge Security Awareness.

*f.* Information Security for DAA, IAM, IASO – Annual.

*g.* DOD/Army Information Assurance Training – Annual.

*h.* Antiterrorism/Force Protection – Annual.

*i.* Threat Awareness and Reporting Program (TARP) – Annual.

*j.* If contractor personnel are required to use removable media containing SAP content, Army SAP Data Transfer Agent Training – Initial and Annual Refresher.

## Appendix D

## Internal Control Evaluation

### D–1. Function

The function covered by this evaluation is the administration of the SEC as required by AR 11–2.

### D–2. Purpose

The purpose of this evaluation is to assist unit managers and internal control administrators in evaluating key SEC internal controls outlined below. It is not intended to cover all controls.

### D–3. Instructions

Answers must be based on the actual testing (that is, document analysis, direct observation, sampling, or interview) of key SEC internal controls. Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

### D–4. Test questions

*a. SUBJECT: Contract Security Considerations.*

(1) Does the contracting officer have the required security clearance and indoctrination for the program(s) executing SEC? Does the necessary contracting office staff have the applicable security clearance and program access to enable accomplishment of assigned tasks? Are cleared subject matter or functional experts (such as, security, lawyers, cost and pricing experts, applicable technical personnel, and/or other required personnel) available to provide appropriate support for the procurement and the contracting officer?

(2) If not, are steps being taken in coordination with cognizant activity security managers to clear required personnel as necessary to meet procurement lead-times?

(3) Does the contracting office have accredited facilities to store, discuss, and process the level of classified material that will need to be handled in support of its procurement(s)?

(4) Do contracting officers have SCGs for supported programs and other applicable program security guidance?

(5) Does the contracting office have required supporting equipment such as secure telephones, secure fax machines, approved storage containers and computer workstations authorized at the appropriate security level?

(6) Can the contracting officer identify the appropriate points of contact for review, staffing, and approval at each level, through and including HQDA, who are properly accessed to review documentation in support of their programs?

(7) Are contracting activity security managers properly verifying security clearance levels and program access through applicable security channels?

(8) Are contracting officers ensuring that contract specialists are knowledgeable about appropriate points of contact for their programs?

(9) Have the contracting officer and staff had some form of training by the contracting activity security manager on proper review of DD Form 254?

(10) Are contracting officers ensuring that the DD Form 254 is signed by the certifying official?

(11) Are contracting officers returning improperly marked or incomplete DD Form 254 to the requiring activity for correction?

(12) Are copies of DD Form 254 for classified contracts being provided to the appropriate officials?

(13) Are contracting elements adequately addressed in the applicable SCG to enable contracting or contractor personnel to make proper classification decisions for contract elements?

(14) Is the DD Form 254 properly marked in accordance with the applicable SCG? Do contracting officers and contract specialists have the proper level of security clearance specified by the requiring activity as codified in the DD Form 254?

(15) Do contracting officers and contract specialists understand how to properly handle and safeguard and mark classified documents? Is marking guidance readily available?

(16) Are classified documents that are part of the contract file properly marked, handled, and stored?

(17) Are contract files periodically reviewed to ensure classified documents are properly filed in accordance with applicable policy/regulation?

(18) Has the contracting office Security Manager received the necessary training to execute the security requirements for the types of information processed within the facility?

(19) Have SEC personnel received appropriate security training to ensure their knowledge of the security requirements for the types of information they will be using to execute SEC? (for example, security awareness, physical security, document or information security, marking, personnel security, industrial security, and other requiring activity specified training)?

(20) Does the contracting office have a secure contracting database not accessible to uncleared personnel?

*b. SUBJECT: Planning and Pre-solicitation.*

(1) Are requiring activities providing evidence that the proposed requirement is properly approved as an SEC requirement?

(2) Does the procurement request package contain a properly completed DD Form 254 that references all applicable SCG and security guidance documents?

(3) Do contracting officers review all purchase requests to ensure that their SEC contracting office is designated or otherwise appropriate to support the request?

(4) Are contract actions reviewed by the SEC chief or designated SEC review personnel to ensure adherence to rules and include appropriate contract security clauses?

(5) If the requirement is proposed to go outside the DoD, has a determination been made in advance that proper authority exists (such as the Economy Act, Clinger-Cohen, or assigned agency responsibility) and that all relevant acquisition regulations have been complied with (for example, FAR 17.5)?

(6) Are contracting officers and requiring activities cooperating to ensure appropriate advance acquisition planning to allow adequate procurement lead time?

(7) If there are significant numbers of urgent requirements, are the request packages adequately supported (for example, to support a contingency or declared emergency)?

*c. SUBJECT: Audit and administration.*

(1) Are all SEC procurements properly receiving pre-solicitation and pre-award reviews and/or audits by the appropriate DCAA office, where applicable, or including a properly justified waiver? Do local procedures address SEC review of actions prior to award?

(2) Is Audit follow-up being properly conducted for SEC?

(3) Is contract administration delegated to the appropriate DCMA office, when applicable?

(4) If contract administration is not delegated to DCMA, is it justified (for example, does it fall under a DFARS 242 exception or an element of an executed MOU)?

*d. SUBJECT: Secure Environment Simplified Purchases.*

(1) Are SESP files periodically reviewed by higher headquarters?

(2) Is corrective action taken when SESP ordering and contracting officers do not comply with laws and regulations?

(3) Are ordering and contracting officers receiving training before being appointed?

*e. SUBJECT: Use of Government Commercial Purchase Card for Secure Environment Contracting.* Are chiefs of contracting offices providing training, guidance, and oversight to SEC GPC card holders in accordance with AFARS?

### D–5. Supersession

This evaluation replaces the evaluation previously published in AR 715–30, dated 1 February 2013.

### DD– 6. Comments

Help this be a better tool for evaluating internal controls. Submit comments to ASA (ALT) (SAAL–PS), 103 Army Pentagon, Washington, DC 20310–0103.

## Glossary

### Section I

### Abbreviations

**ACAVS**
Army Contractor Automated Verification System

**ACCS**
Army Centralized Contracts & Security

**ACOM**
Army command

**AFARS**
Army Federal Acquisition Regulation Supplement

**ARCYBER**
U.S. Army Cyber Command

**ASA (ALT)**
Assistant Secretary of the Army (Acquisition, Logistics and Technology)

**ASA (FM&C)**
Assistant Secretary of the Army (Financial Management and Comptroller)

**ASCC**
Army service component command

**ASPD**
Army Special Program Directorate

**CFR**
Code of Federal Regulations

**CG**
commanding general

**CIO/G–6**
Chief Information Officer/G–6

**COE**
Chief of Engineers

**COR**
contracting officer's representative

**CPARS**
Contractor Performance Assessment Reporting System

**CSA**
Chief of Staff Army

**CSE**
Contractor support element

**DA**
Department of the Army

**DAIG**
Department of the Army Inspector General

**DASA(P)**
Deputy Assistant Secretary of the Army for Procurement

**DCAA**
Defense Contract Audit Agency

**DCMA**
Defense Contract Management Agency

**DCS, G–2**
Deputy Chief of Staff, G–2

**DCS, G–3/5/7**
Deputy Chief of Staff, G–3/5/7

**DCS, G–4**
Deputy Chief of Staff, G–4

**DFARS**
Defense Federal Acquisition Regulation Supplement

**DIAD**
Defense Intelligence Agency directive

**DOD**
Department of Defense

**DODI**
Department of the Defense Instruction

**DRU**
direct reporting unit

**EO**
executive order

**FAR**
Federal Acquisition Regulation

**FISMA**
Federal Information Security Management Act

**FMA**
foreign materiel acquisition

**FOIA**
Freedom of Information Act

**FOUO**
for official use only

**GFP**
government-furnished property

**GPC**
government purchase card

**GSA**
General Service Administration

**HCA**
head of contracting activity

**HQDA**
Headquarters, Department of the Army

**IT**
information technology

**JSIG**
Joint SAP Implementation Guide

**MOU**
memorandum of understanding

**OCONUS**
outside the continental United States

**OPSEC**
operations security

**PARC**
Principal Assistant Responsible for Contracting

**PGI**
Procedures, Guidance, and Information

**PM**
program manager

**PMR**
procurement management review

**PSO**
program security officer

**SAP**
Special Access Program

**SAPCO**
Security Assistance Policy Coordinating Office

**SAPF**
Special Access Program Facility

**SCG**
security classification guide

**SCI**
sensitive compartmented information

**SEC**
secure environment contracting

**SESP**
secure environment simple purchases

**SF**
Standard Form

**TARP**
Threat Awareness and Reporting Program

**TJAG**
The Judge Advocate General

**TSG**
The Surgeon General

**USACIDC**
U.S. Army Criminal Investigation Command

**USC**
United States Code

## Section II

## Terms

**Classified contract**
Any contract that requires or will require access to classified information by the contractor or the contractor's employees in the performance of the contract. A contract may be classified even though the contract document is unclassified.

**Contracting officer's representative**
Appropriately indoctrinated personnel (military or civilian) appointed by the contracting officer to monitor the activities of all assigned contracts including those at SCI and SAP levels.

**Foreign materiel acquisition**
Contracting for materiel normally denied the U.S. Government by the country of origin. Foreign Materiel Program Activities that include gaining physical possession of or access to an item of foreign materiel or technology registered at HQDA using the procedures described in this regulation, prior to contract execution.

**Full and open competition**
All responsible sources are permitted to compete.

**Intelligence activity**
An activity that an agency within the intelligence community is authorized to conduct under EO 12333.

**Intelligence contingency funds**
Funds expended for worldwide intelligence activities of such confidential, extraordinary, or emergency nature that they cannot or should not be accounted for in detail outside of the intelligence community.

**Operations security**
A process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information. OPSEC is a methodology that denies critical information to an adversary. Unlike security programs that seek to protect classified information, OPSEC measures identify, control, and protect generally unclassified evidence that is associated with sensitive operations and activities.

**Other secure contracting requirements**
Any other secure mission requirement that necessitates procedures outlined in this regulation. Requirements may be classified or unclassified. The actual supplier may not know who is actually going to use the supply or service or the supplier may not even know that the supply or service is being acquired by the Army. The use of an intermediary contractor is authorized to mask Army involvement. The use of SEC must be by a contracting office requested by the HCA as set forth in this regulation.

**Read–on**
Authorized to review.

**Secure environment contract**
(1) Contracts involving SAP requirements, (2) contracts involving SCI requirements (other than for purely personnel clearance purposes), (3) contracts funded with intelligence contingency funds, (4) FMA program requirements, (5) collaterally classified top secret contracts, and (6) contracts where the true identity of either or both parties must be concealed (see AR 381–102).

**Secure environment contracting**
Contracting conducted under conditions of extraordinary security by properly cleared personnel as follows:
*a.* When especially sensitive types of information comprise part of the statement of work or are part of deliverables.
*b.* When contracting personnel may require access to this especially sensitive classified information to properly discharge their independent professional judgment and responsibilities.
*c.* When this type of classified information may be provided to the contractor to enable performance.

**Secure environment simple purchase**
An acquisition of goods or services that does not exceed the simplified acquisition threshold in the FAR and that requires the use of SEC procedures.

**Secure environment simple purchase contracting officer**
A military or civilian Federal employee appointed as a contracting officer by the supporting HCA with contracting authority limited as indicated on the certificate of appointment.

**Secure environment simple purchase ordering officer**
A military or civilian Federal employee appointed in accordance with AFARS that may make over-the-counter purchases not exceeding the micro-purchase threshold per purchase using the SF 44.

**Security classification guide**
A document approved by an original classification authority that prescribes the level of classification and the appropriate declassification instructions for specified information.

**Sensitive activities**
Sensitive activities include special access or code word programs, clandestine operational or intelligence activities, cover, special plans, special activities, and sensitive support to non-Army agencies and/or activities excluded from normal staff review and oversight.

**Sensitive compartmented information**
Information and material requiring special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

**Sensitive compartmented information facility**
An area that has been accredited by the cognizant security agency for the receipt, storage, discussion, and use of SCI.

**Special Access Program**
A program established for a specific class of classified information imposing safeguarding and access requirements that exceed those normally required for information at the same classification level.

**Special activity**
An activity or function in support of such activity conducted in support of national foreign policy objectives abroad that is planned and executed, so that the role of the Government is neither apparent nor acknowledged publicly.

**Special operations**
Operations conducted by specially trained, equipped, and organized DOD forces against strategic, economic, or psychological objectives. These operations may be conducted during periods of peace or hostilities. They may support conventional operations or they may be prosecuted independently when the use of conventional forces is either inappropriate or infeasible.

**Special security officer**
The individual through whom the cognizant security authority accomplishes responsibility for the security, use, and dissemination of SCI.