Army Regulation 380–49

Security

Industrial Security Program

Headquarters
Department of the Army
Washington, DC
20 March 2013

UNCLASSIFIED

SUMMARY of CHANGE

AR 380–49
Industrial Security Program

This major revision, dated 20 March 2013--

- Adds an internal control evaluation (app C).

- Incorporates DOD policies, delineates roles and responsibilities across Army command echelons, and provides discussion on foreign ownership, control, or influence (throughout).

- Makes administrative changes (throughout).

Headquarters
Department of the Army
Washington, DC
20 March 2013

*Army Regulation 380–49

Effective 20 April 2013

Security

Industrial Security Program

By Order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army

History. This publication is a major revision.

Summary. This regulation establishes policy for the Department of the Army Industrial Security Program and implements policy from Executive Order 12829, DOD 5220.22–M, DOD 5220.22–R, DODI 5220.22, and Homeland Security Presidential Directive–12.

Applicability. This regulation applies to the Active Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff, G–2. 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 B).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

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 Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

Distribution. This regulation is available in electronic media only and is intended for command levels C, D, and E for the Active 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 380–49, dated 15 April 1982.

UNCLASSIFIED

Contents—Continued

Contents—Continued

Contents—Continued

Chapter 1
Introduction

Section I
General

1–1. Purpose
This regulation establishes policy for the Department of the Army's Industrial Security Program (ISP). This regulation pertains to classified information and also addresses controlled unclassified information (CUI) in the hands of industry. It prescribes requirements, restrictions, and other safeguards for the ISP to prevent unauthorized disclosure of classified and CUI released to current, prospective, or former contractors, licensees, grantees, and certificate holders of the DA. This regulation addresses contractor operations on Army installations or at Army facilities. This regulation does not stipulate the enhanced security requirements for Special Access Programs (SAPs). SAP security requirements are addressed in AR 380–381 and in AR 715–30. Additionally, AR 715–30 provides policy and guidance to support a secure contracting environment and activities having special security or operational requirements. The ISP is administered by the Deputy Chief of Staff, G–2 (DCS, G–2).

1–2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the glossary.

1–4. Responsibilities
Responsibilities are listed in section II of chapter 1 and chapter 7.

1–5. Guidelines
The ISP is administered by DCS, G–2 to ensure that specific classified or otherwise Governmental CUI is properly safeguarded while entrusted to industry regardless of its physical form, medium, or characteristics and regardless of whether such information was furnished to or generated by industrial contractors and/or their facilities in support of DA procurements and programs.

1–6. Scope
a. The security policies, requirements, and procedures identified in this regulation are applicable to Army personnel (military and civilian), all Army contractors performing services on an Army installation and supporting a tenant Army facility and contractors in which the Army provides oversight.

b. The National Industrial Security Program (NISP) was established by Executive Order (EO) 12829 for the protection of information classified under EO 13526, as amended, or its successor or predecessor orders and the Atomic Energy Act of 1954, as amended, placed within the hands or entrusted to the Defense Industrial Base. The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense has been designated lead agent for the NISP by the President. The Director, Information Security Oversight Office, is responsible for implementing and monitoring the NISP and for issuing implementing directives that are binding on agencies. Defense Security Service (DSS) is responsible for administering the Department of Defense (DOD) ISP on behalf of all DOD agencies, the Departments of the Army, Navy, and Air Force, to include their activities, and those federal agencies which have established NISP servicing agreements with DOD.

1–7. Waivers
DCS, G–2 will review and approve requests for waivers or exceptions to this regulation, as appropriate and as consistent with controlling law and policy. Army commands (ACOMs), Army service component commands (ASCCs), and direct reporting units (DRUs) will submit such requests with supporting justification to DCS, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

1–8. Public release of information
See AR 360–1 for additional information.

1–9. Disclosure of Army Information to foreign governments, international organizations, and representatives thereof
See AR 380–10 for additional information and guidance.

Section II
Responsibilities

1–10. The Secretary of Defense

The SECDEF is the Presidentially-designated lead agent for the NISP per Executive Order 12829 and is the cognizant security agency for all DOD components, as well as those agencies which have entered into industrial security servicing agreements with DOD (hereinafter, collectively referred to as user agencies. In accordance with DODD 5105.42, the SECDEF has designated the DSS as the cognizant security office (CSO) for DOD industrial security matters. As the CSO, DSS executes responsibilities of the SECDEF as the lead agent for inspecting and monitoring contractors, licensees, grantees, and certificate holders who require or will require access to, or who store or will store classified information; and for determining contractors, licensees, certificate holders, and grantees eligibility for access to classified information.

1–11. The Assistant Secretary of Defense (International Security Affairs)

The ASD (ISA) is the principal advisor to the Under Secretary of Defense for Policy (USD (P)) and the SECDEF on international security strategy and policy on issues of DOD interest that relate to the nations and international organizations of Europe (including the North Atlantic Treaty Organization and Russia), the Middle East, and Africa, their governments and defense establishments, and for oversight of security cooperation programs, including foreign military sales in these regions.

1–13. The Director, Defense Security Service

The Director, DSS is responsible for administering the DOD ISP on behalf of all DOD components and those federal agencies which have entered into industrial security servicing agreements with the SECDEF. The Director of DSS, under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD (I)), oversees security administration of the NISP, to include security oversight of cleared companies requiring access to classified for legitimate Government requirements, determining contractor eligibility for access to classified information, and making determinations regarding foreign ownership, control, or influence (FOCI) for U.S. companies cleared or under consideration for a facility clearance (FCL) under the NISP. DSS serves as the CSO for any contractors doing business with any user agency (except in the case of contracts falling under a SAP for which a "carve-out" contract has been established, in which instance CSO is determined on a case-by-case basis). DSS is responsible for over sighting and inspecting cleared contractor facilities not located on an Army installation; therefore, DSS does not provide oversight for embedded or integrated contractors who work on an Army installation or within a tenant organization on an Army installation. The supporting security office has oversight responsibility for embedded or integrated contractors.

1–14. Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Coordinate policies outlined in this regulation with USD (I) and other agencies involved in this program. DCS, G–2 oversees compliance with and implements policy under the provisions of DOD 5220.22–R, approves procedures for the ISP, and is designated the Army senior security official responsible for overseeing implementation of the ISP. DCS, G–2 is the implementing agent for ISP policy development, interpretation, administration, and oversight.

b. Be responsible for sensitive compartmented information (SCI) security policy, when applicable to DA awarded contracts, pursuant to AR 380–28, requiring access to SCI information or classified contracts. Furthermore, the DCS, G–2 is responsible for establishing Army SAP security policy, pursuant to AR 380–381 and AR 380–5, for all classified SAP contracts and SAP contracts requiring access to classified information and/or CUI.

c. Be responsible for formulating and overseeing implementation of ISP pursuant to AR 380–5, Army communications security (COMSEC) policy pursuant to AR 380–40, and Army personnel security policy, to include trustworthiness determinations, pursuant to AR 380–67, when applicable to DA awarded contracts.

d. Provide a member to serve and represent DCS, G–2 on the National Industrial Security Program Policy Advisory Committee. This committee is an administrative board composed of both government and industry personnel that advises the Information Security Oversight Office regarding the NISP and associated policy.

1–15. Assistant Secretary of the Army for Acquisition, Logistics and Technology

The ASA (ALT) will—

a. Develop contracting policies and procedures in support of this regulation and the ISP to ensure that classified placed in the possession of industry is protected via a contract vehicle.

b. Ensure appropriate DA management and implementation of contracting procedures and functions are properly executed.

c. Provide oversight of contract execution.

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

e. Identify critical U.S. military system-specific technologies.

f. Oversee the development, coordination, and implementation of policy and programs associated with the DA's security cooperation activities (to include but not limited to, foreign military sales, technology transfer, and direct commercial sales).

g. Serve as the Secretary of the Army's single executive for providing export policy oversight and lead and direct the Technology Transfer Security Assistance Review Panel, which serves as the executive decision authority for DA export control.

h. Administer and oversee research, development, test, evaluation, and acquisition programs, to include the execution of data and information exchange programs and cooperative research and development.

i. Provide technical experts on DA, DOD, and interagency committees, panels, and working groups that address industrial security, technology transfer, and/or military critical technologies.

j. In coordination with DCS, G–2 and the General Counsel (GC), as needed, develop effective technical and/or contractual safeguards to prevent the inadvertent disclosure of critical U.S. technology.

k. Establish a requirement for contract reviews by teams of appropriate policy proponent subject matter experts (SMEs) and technical experts (TEs) from presolicitation to contract termination for contract development, review, and oversight, to ensure DA contracts contain mandatory security clauses and other requirements. As appropriate, SMEs and/or TEs will include Deputy Chief of Staff, G–1 (DCS, G–1); DCS, G–2; Deputy Chief of Staff, G–4 (DCS, G–4); Deputy Chief of Staff, G–3/5/7 (DCS, G–3/5/7); and Chief Information Officer/G–6 (CIO/G–6) personnel. Also, a Deputy Chief of Staff, G–8 (DCS, G–8) TE will participate in development and review of any contract which requires access to a resource management database.

l. Establish supporting procedures for the contract review teams described in paragraph 1–15*k*, and ensure all personnel on such teams are advised regarding these policies and procedures.

m. Ensure the DD Form 254 (DOD Contract Security Classification Specification) and contract requirements are reviewed as required by DOD 5220.22–R, to ensure security requirements remain current and relevant throughout the contract life cycle. Ensure the DCS, G–1; DCS, G–2; DCS, G–4; DCS, G–3/5/7; CIO/G–6; and DCS, G–8 SMEs and TEs participate in these reviews, as appropriate.

n. Ensure contract documents that pertain to classified contracts inform the cleared contractor company that contractor personnel must read and sign a Visitor Group Security Agreement (VGSA) acknowledging they will adhere to local security requirements at their duty location.

1–16. Assistant Secretary of the Army (Financial Management and Comptroller)

The ASA (FM&C) will—

a. Develop financial and budgeting guidance for contracts.

b. Implement staff support and execution review for contract requirements at program appropriation level.

c. Provide cost estimating support for selected contract actions.

d. Coordinate with DCS, G–2 on ISP related issues as necessary and appropriate.

1–17. Chief Information Officer/G–6

The CIO/G–6 will—

a. Review and approve, in coordination with DCS, G–2 (DAMI–CDS), federal information processing requirements as they relate to contractors.

b. Provide technical advice and assistance on information systems security and system accreditation required in AR 25–2.

c. Provide technical experts on DA, DOD, and interagency committees, panels, and working groups that address information systems security as it relates to industrial security.

d. Provide SMEs and/or TEs to participate in contract development and the review of contract documents that contain information systems security requirements.

1–18. The General Counsel

The GC will—

a. Review all matters regarding industrial security that require coordination and/or decision at the Secretariat level.

b. Advise the Secretary of the Army on legal and policy issues related to industrial security.

c. Conduct reviews of proposed policy related to industrial security.

1–19. Deputy Chief of Staff, G–1

The DCS, G–1 will—

a. Determine personnel classification and standards.

b. Comply with existing security standards and criteria when formulating personnel management policy and procedures.

c. Provide SMEs and/or TEs to participate in contract development and review to ensure contract documents contain appropriate contractor suitability requirements.

1–20. Deputy Chief of Staff, G–3/5/7

The DCS G–3/5/7 will—

a. Provide TEs on DA, DOD, and interagency committees, panels, and working groups that address operations as they relate to cleared contractors.

b. Provide SMEs and/or TEs to participate in contract development and reviews to ensure operations security (OPSEC), strategic, tactical command and control systems, physical security, and/or nuclear and chemical requirements are included in contract documents when appropriate.

1–21. Deputy Chief of Staff, G–4

The DCS, G–4 will—

a. Provide TEs on DA, DOD, and interagency committees, panels, and working groups that address logistics support as it relates to industrial security.

b. Provide SMEs and/or TEs to participate in contract development and reviews to ensure logistics support requirements are identified and included.

1–22. Deputy Chief of Staff, G–8

The DCS, G–8 will—

a. Provide TEs on DA, DOD, and interagency committees, panels, and working groups that address resource management issues as it relates to cleared contractors.

b. Provide SMEs and/or TEs to participate in contract development and reviews to ensure contract documents contain appropriate resource management requirements, particularly as they relate to resource management database access.

1–23. The Surgeon General

TSG will provide SMEs and/or TEs to participate in contract development and reviews of classified contracts to ensure necessary medical support requirements are included for research and development and supplies and services contracts.

1–24. The Judge Advocate General

TJAG will provide legal and policy advice to Chief of Staff, Army and the Army Staff on matters related to industrial security.

1–25. Director, Army Special Programs Directorate

The Director, ASPD, consistent with the roles and responsibilities prescribed in AR 380–381, will ensure coordination with DCS, G–2 on Committee on Foreign Investment in the U.S. issues and national interest determinations (NIDs) as they relate to SAPs and sensitive activities.

1–26. Commanders of Army commands, Army service component commands, and direct reporting units

Commanders of ACOMs, ASCCs, and DRUs, hereinafter referred to as "Commanders" will—

a. Use the policy guidance contained in this regulation to establish local supplemental guidance governing interactions with contractors who require access to classified or otherwise sensitive information and/or technology, as needed. Commanders will ensure that all local supplemental policies and/or guidance receive a review from servicing legal counsel to be consistent with this regulation and relevant law and policy.

b. Ensure an industrial security specialist (ISS) is designated, in writing, to perform ISP duties.

c. Ensure that personnel performing industrial security duties are adequately trained, possess appropriate clearances, and are given access to special access and SCI material or contracts when a valid requirement exists.

d. Ensure the appropriate ISS, SMEs, and/or TEs participate in contract reviews.

e. Ensure the appropriate ISS coordinates with the contracting officer (KO) and/or contracting office representative (COR) to ensure integrated and/or embedded contractors receive all required security training.

f. Ensure the appropriate ISS is included in plans and procedures as they relate to industrial security.

g. Develop security classification guides (SCGs), in conjunction with the contracting office, the KO, COR, and/or contracting officer's technical representative for classified contracts or contracts requiring access to classified information, as appropriate, prior to release of procurement information to industry. Ensure all updated SCGs are provided to the supporting contract office.

h. Conduct and document biennial ISP oversight reviews of the subordinate commands.

i. Ensure security reviews and/or inspections are conducted as required by the DOD 5220.22–R and DOD 5220.22–M for those contractor operations designated as a cleared facility on an Army installation or within a tenant activity

in those cases where the local installation and/or activity commander has retained security oversight responsibility and DSS has relinquished such responsibility. In those instances where the ISS will conduct the reviews and/or inspections, and the commander maintains oversight of the cleared facility, DSS will be notified that the DA will retain "security oversight" for the contractor operations on the installation.

j. Consistent with DOD 5220.22–R that governs contractor activities on a user agency installation, designate contractor operations on the installation or within a tenant activity that require access to classified information as an intermittent visitor, visitor group, or cleared contractor facility.

k. Ensure contractors conducting operations located on DA installations who require or will require access to classified and/or CUI execute a VGSA, as appropriate. For contractor operations on DOD installations not controlled by the DA, the supporting ISS will comply with host base requirements for contractor operations.

l. Provide metrics annually to DCS, G–2 on ISP related information, including, but not limited to the following:

(1) The number of classified contracts (prime and subcontracts) on the installation or within a tenant activity.

(2) The number of FCLs that the installation or tenant oversee.

(3) The number of NIDs completed.

(4) Data on training provided to contractors or government personnel.

m. Ensure contractor employees whose performance occurs in DA facilities under contracts subject to the ISP receive local security briefings and sign Standard Form (SF) 312 (Classified Information Nondisclosure Agreement) and any applicable VGSA acknowledgment.

1–27. Army requiring activity program, project manager, division chief, or supervisor

The Army requiring activity program, project manager, division chief, or supervisor will—

a. Identify program unique security requirements and critical program information (CPI) for solicitations and contract documents in coordination with the supporting ISS and SMEs and/or TEs.

b. Ensure DA employees that are responsible for the contract are appropriately cleared to support the work being performed on the contract.

c. Ensure program specific security classification guidance or program information guidance is incorporated, as appropriate, into the performance work statement (PWS), statement of objectives (SOO), and/or statement of work (SOW).

d. Assist in the completion of the DD Form 254 from the security requirements identified in the PWS and/or SOW by coordinating the contractual security specifications with the KO, the responsible ISS, SMEs, and/or TEs.

e. Provide the name, title, command, or activity name, telephone number, and address of the government program manager DD Form 254, item 13, along with that individual's written certification that the requirements are complete and adequate for performance of the contract.

f. Review and revise the classification and/or declassification program specific security and/or technical guidance as required by DOD 5220.22–R and DOD 5220.22–M to ensure that the contractor handles, stores, and processes or unclassified technical data appropriately.

g. Work in concert with the KO, COR, ISS, SMEs, and/or TEs or other program offices to ensure embedded and integrated contractors understand the requirements of the DA activity (such as security, safety, badge, and day-to-day requirements) and that these requirements are incorporated into contractual obligations to the extent appropriate and feasible.

h. Ensure SMEs and/or TEs participate on contract review teams.

1–28. Contracting officer and/or contracting officer representative

The KO and/or COR will—

a. Ensure an approved acquisition plan, which includes a security specification section, is developed by the KO and requiring activity, in coordination with the supporting ISS, defining the security requirements and procedures for the duration of the contract, program, or project.

b. Ensure that required security clauses are incorporated into classified contracts and solicitations as mandated in the Federal Acquisition Regulation (FAR) and its applicable supplements.

c. Ensure that the appropriate investigative standards for access to Army installations, facilities, and Army information systems are appropriately represented in the contract and solicitations in accordance with AR 25–2, AR 380–67, and FAR, personal identity verification of contractor personnel, and applicable supplements.

d. Ensure the PWS, SOW, and/or SOO and any other requirements documents adequately reflect the security requirements for the contracts and the ISS and/or supporting security manager (SM), along with the KO and program manager (PM), collaborate in the preparation of the DD Form 254 and security requirement statements for the contract.

e. Ensure that all security requirements for contracts are reviewed and validated and the DD Form 254 is signed by the supporting ISS, per the FAR and this regulation.

f. Ensure that both the contract and security requirements include the necessary security clearance eligibility and/or suitability requirements.

g. Review the DD Form 254 and provide the COR's name, title, command, or activity name, telephone number, and address in item 13.

h. Ensure that a fully executed copy of DD Form 254 is forwarded to the DSS offices identified in blocks 6c, 7c, and 8c and all activities indicated on the distribution list in block 17.

i. Carry out any other required and/or appropriate actions outlined in the Army Federal Acquisition Regulation Supplement, Defense Federal Acquisition Regulation Supplement, and FAR.

j. Have final eligibility and/or access, as applicable, granted to the highest level stated in the PWS and/or SOW and DD Form 254.

k. Ensure the COR is adequately cleared to perform oversight functions for the contract.

l. Ensure that a listing of all proposed bidders is forwarded to the ISS for verification of FCL and safeguarding capabilities.

m. Ensure that all classified procurements have an approved and fully signed DD Form 254 and it is forwarded to the KO and/or COR for inclusion with the contract award document.

n. Review the Central Contractor Registration (CCR) to ensure that all proposed offerors who are required by FAR to register with the CCR have done so and are listed as active therein (see para 1–27*h*). The CCR is available at https://www.bpn.gov/ccr/default.aspx.

o. Coordinate with the ISS and/or supporting security managers for advice and assistance on classified contracts and contracts requiring access to classified and/or CUI.

p. Ensure that security violations on embedded and/or integrated contractors are reported to the ISS and supporting security manager and to the CSO.

q. Ensure that the ISS, supporting security manager and other appropriate offices are notified prior to the entry or exit of contractor activities or personnel, so that appropriate security actions can occur (for example, in/out briefings, Army Knowledge Online and/or information technology (IT) access approvals, and updating of access rosters).

r. Grant contractors access to classified information based upon eligibility and the need to know.

s. Ensure a local COR and/or administrative contracting officer representative is assigned to oversee the contractor's performance at all locations where contract tasks are being performed.

1–29. Industrial security specialist

The command ISS will—

a. Oversee and administer the ISP on behalf of the command and ensure compliance with applicable acquisition and security policy, regulations, and instructions for the safeguarding of classified or CUI.

b. Be designated in writing by the commander.

c. Ensure that embedded and/or integrated contractors performing on classified contracts or on contracts requiring access to classified information or CUI, who are located on DA installations or within tenant activities, are incorporated into the supporting security program.

d. Review acquisition plans, pre-award and/or draft solicitations, SCGs, SOWs, SOO, and DD Forms 254 to ensure appropriate security clauses and/or language are contained therein to address the protection of classified information, export controlled information, CPI, and CUI. The ISS must sign DD Form 254, block 16 acknowledging and accepting the security requirements.

e. Ensure that the COR and/or PM sign the DD Form 254, block 13 and that the fully executed DD Form 254 is forwarded to the COR for submission to the KO, so that it may be included with the contract award document.

f. Ensure that the distribution list of DD Form 254, block 17 includes the servicing security offices of any other installations or facilities at which contract performance will occur.

g. Verify in the DSS Industrial Security Facilities Database the contractor FCLs, commercial and government entity codes, and the storage capabilities required for each prospective bidder. The KO will provide the listing of prospective offerors.

h. Verify active status in the CCR for those contractors required to register under FAR. For contractors subject to this registration requirement, any status other than active precludes award of any government contract to the contractor. The ISS will promptly notify the KO and the COR in writing of any improprieties concerning commercial and government entity codes or FCL.

i. Monitor compliance with the provisions of this regulation and provide assistance to supported elements as dictated by program requirements.

j. Conduct security oversight and inspections of any cleared facility over which the command, program, or activity has oversight responsibilities. This includes, but is not limited to, government-owned, contractor-operated, contractor-owned, contractor-operated, or certain secure environment contracts that are located within a DA installation or tenant activity (see AR 715–30). The inspection should be conducted at least bi-annually or as determined by the commander, program executive officer (PEO), or PM or as otherwise required by the DOD 5220.22–M or DOD 5220.22–R.

k. In coordination with the KO and/or COR, direct the contractor to take corrective actions when security program

deficiencies are identified and to promptly report security violations, loss, and/or compromise of DOD and DA information.

l. Ensure that DSS is notified of all security violations, loss, and/or compromises of DA or DOD information.

m. Forward to DSS a copy of the security review and survey reports and other applicable documentation that pertains to the cleared facility on an installation or within a tenant activity, in accordance with the DOD 5220.22–R, DOD 5220.22–M, and this regulation.

n. Ensure the cognizant DA counterintelligence (CI) research and technology protection agent is informed of classified contracts.

1–30. Supporting security manager

If the supporting SM is not the ISS, the SM will—

a. Ensure that embedded and/or integrated contractors are appropriately briefed on security requirements, in-processed (to include the appropriate IT access, badges, security briefings, and/or indoctrinations), and outprocessed.

b. Ensure a servicing relationship in the Joint Personnel Adjudication System is established for all embedded and/or integrated contractors.

c. Provide advice and assistance to the ISS, KO, COR, and/or PM on security matters, as needed.

Section III
Reporting Requirements

1–31. Adverse information and suspicious contact reporting

a. Contractors who work in a cleared facility on a DA installation or who are embedded or integrated within a DA program or activity, will satisfy DOD 5220.22–M requirements to report adverse information, suspicious contacts, and other reportable incidents by submitting appropriate reports or information in writing through the KO and/or COR to the ISS.

b. Upon receipt of adverse or suspicious contact information, the ISS, in coordination with the KO and/or COR, will forward the report to the contractor's facility security officer (FSO). Any subsequent or additional reporting required by the DOD 5220.22–M to other federal offices and/or agencies (for example, the cognizant security agency, CSO, and/or Federal Bureau of Investigation), is the responsibility of the FSO.

c. The ISS will retain a copy of the adverse information or suspicious contact report in the ISS security files for 2 years.

d. The ISS is responsible for notifying other DA activities as required and/or appropriate (for example, the KO, DA CI, PEO, PM, and/or DSS).

e. All incidents involving CPI will be reported to the program office, DSS, and the local CI office.

1–32. Security violations

a. Any loss, compromise, suspected compromise or other security violations occurring on a DA installation and by an embedded and/or integrated contractor must be reported (pursuant to the DOD 5220.22–M and the DOD 5220. 22–R) through the ISS, who in-turn is responsible for notifying the KO, COR, DSS, installation, or facility commander.

b. The ISS will report contractor security violations, compromises, and other such continuing security issues to the KO and COR and the regional DSS office for cleared facilities located on the DA installation.

c. When the KO and COR receives notice of contractor security violations, the KO and COR must notify the ISS and/or supporting SM.

d. The KO, COR, ISS, and/or SM is required to report information on contractor computer intrusions (including intrusions on unclassified systems) located at the cleared contractor facility to DSS or the local DA CI office, depending upon who maintains oversight of the cleared contractor facility.

e. All contractor security violations involving classified information, CUI, or CPI will be reported to the program office, KO, COR, DSS, and the FSO.

1–33. Espionage, sabotage, and subversive activities

a. In addition to relevant reporting responsibilities defined in DOD 5220.22–R and AR 381–12, ISS must report incidents of suspected espionage, sabotage, subversive activities, and deliberate compromises of classified information or CUI (involving cleared facilities or visitor groups located on DA installations or within tenant activities) to the servicing CI representative. The CI representative will coordinate with other investigative agencies, as necessary.

b. The report should—

(1) Identify the cleared facility involved.

(2) Identify the person(s) involved, including the full name, date and place of birth, social security number, local address, present location, position with the company and/or agency, security clearance (including past or present participation in any SAPs), and a description of any plan or recommendations to suspend or revoke the individual's personnel security clearance (PCL).

(3) Describe the circumstances of the incident and identify the classified material involved.

(4) Document when (time and date) the ISS reported the incident to DSS or when DSS reported the incident to the Federal Bureau of Investigation, if known.

(5) Include a copy of any investigative reports.

(6) For the subsequent and final reporting, identify any changes in contractor procedures necessitated by the incident and any recommendations for change in the security program, which might prevent similar future incidents of loss or compromise.

c. Contractors who become aware of suspected espionage, sabotage, subversive activities, and deliberate compromises of classified information or CUI involving other contractors should report such incidents to their supporting FSO. If the incident involves government civilians and/or military personnel, the contractor should report such incidents to the supporting ISS, if any, or their supporting FSO, who will in turn report the incident to the KO and/or COR.

1–34. Loss, compromise, and possible compromise

Commands will follow this regulation and perform actions as required by the DOD 5220.22–R to report the loss, compromise, or possible compromise of classified information or CUI provided in support of contractor operations for which DA has oversight.

a. Any KO or COR that learns of contractor loss, compromise, or possible compromise of classified or CUI will immediately notify the appropriate ISS and the program office that has responsibility for the subject information. The ISS will immediately notify the command security manager (CSM).

b. The original classification authority or the organization designated by the agency head is responsible for determining whether a damage assessment is warranted and making any subsequent decisions to declassify, downgrade, or retain classification of the affected information. If the compromise or loss occurred via an Automated Information System, the organization responsible for the data spill is responsible to mitigate in accordance with AR 25–2. The original classification authority or the organization designated by the agency head notifies the DA organization responsible for the spill, DSS, and/or the contractor of decisions to declassify, downgrade, or retain classification of the affected information.

c. The ISS will provide a copy of the security incident investigation report to the CSO that has jurisdiction over the contractor facility.

d. When loss or compromise involves CPI, the incident must be reported to the local DA CI office.

Chapter 2
Security Clearances

Section I
Facility Security Clearance

2–1. General

a. A FCL is an administrative determination by DSS that a company is eligible for access to classified information or award of a classified contract. Contract award may be made prior to the issuance of a FCL. In those cases, the contractor will be processed for a FCL at the appropriate level and must meet eligibility requirements for access to classified information. However, the contractor will not be afforded access to classified information until the FCL has been granted. The FCL requirement for a prime contractor includes those instances in which access will be limited to subcontractors. Contractors are eligible for custody (possession) of classified material if they have a FCL and storage capability approved by the cognizant security agency.

(1) A FCL is valid for access to classified information at the same or lower classification level as the FCL granted.

(2) FCLs will be registered centrally by the Government.

(3) A contractor will not use its FCL for advertising or promotional purposes.

b. As a precondition for receiving a FCL, an uncleared company must execute DD Form 441 (DOD Security Agreement). The DD Form 441 is executed between the government (DSS) and the company requesting the FCL. In addition, except as provided in DOD 5220.22–R, no person will commit the government to reimburse a cleared company for funds expended in connection with the company's security program.

2–2. Reciprocity

A FCL will be considered valid and acceptable for use on a fully reciprocal basis by all Federal departments and agencies, provided it meets or exceeds the level of clearance needed. The COR, ISS, and supporting SM work together to resolve issues pertaining to reciprocity in the context of, but not limited to, inspections, surveys, audits, security

clearances, and security reviews. Elevate reciprocity issues to the next higher level of command when they cannot be resolved locally.

2–3. Facility security clearance eligibility and establishment

A contractor or prospective contractor cannot apply for its own FCL. A Government Contracting Activity (GCA) or a currently cleared contractor may sponsor an uncleared company for a FCL. A company must meet the following eligibility requirements before it can be processed for an FCL:

a. The contractor must need access to the classified information in connection with a legitimate Government or foreign government requirement.

b. The contractor must be organized and existing under the laws of any of the fifty States, the District of Columbia, or Puerto Rico, and be located in the U.S. or its territories.

c. The contractor must have a reputation for integrity and lawful conduct in its business dealings. The company and its key managers must not be barred from participating in Government contracts.

d. The contractor must not be under FOCI to such a degree that the granting of the FCL would be inconsistent with the national interest.

e. A FCL is valid for access by contractor operations to classified information at the same or lower classification level as the FCL granted by DSS. A contractor or prospective contractor cannot apply for its own FCL; however, a GCA or a currently cleared contractor company may sponsor an uncleared company for a FCL if they are selected as a subcontractor under a valid, classified DA contract. The FSO will be responsible for developing a DD Form 254 for the subcontract ensuring protection of classified material commensurate with DA requirements on the original contract. All fully executed DD Form 254s for subcontracts must be provided to the COR. The COR will ensure that the ISS also receives a copy. The company must:

(1) Need access to classified information in connection with a DA requirement.

(2) Be organized and existing under the laws of any of the 50 States, the District of Columbia, or Puerto Rico and be located in the U.S. or its territories.

(3) Have a reputation for integrity and lawful conduct in business dealings.

(4) Not be under FOCI unless a mitigating agreement has been prepared (see section II).

f. Contractors must have a final top secret FCL prior to the award of an SCI contract. A contractor that possesses an interim top secret FCL is prohibited from access to SCI.

g. The department or agency must have a valid contractual requirement to sponsor the contractor for a top secret FCL for access to SCI.

h. The FSO and/or contractor special security officer must meet Intelligence Community Directive (ICD) 704 eligibility requirements and be indoctrinated for SCI.

i. Contractor employees that will perform work on SCI contracts must meet ICD 704 eligibility requirements and be indoctrinated for SCI.

2–4. Sponsoring facility security clearances

a. The ISS is responsible for ensuring that all contractors that bid on a DA contract obtain a FCL at the appropriate level and with proper mitigation of any FOCI. Failure to obtain a FCL at the appropriate level may be justification for cancellation of the contract. The KO, PM, or another cleared facility (company) may sponsor a company for a FCL. DSS is the authorizing agent for the FCL and establishes and maintains all FCLs within the DOD ISP. DSS will advise and assist the company during the FCL process. Also see DOD 5220.22–M, DOD 5200.2–R, AR 380–67, and http://www.dss.mil for additional guidance.

b. To request an FCL sponsorship—

(1) For programs and/or PEOs, the PM will prepare a sponsorship letter for the company needing the clearance.

(2) For all others, either the ISS or KO, and/or COR will prepare a sponsorship letter for the requesting contractor company (facility).

(3) For subcontracts, the prime contractor will prepare a sponsorship letter for the subcontractor company and ensure that the KO and COR receive a copy of the signed sponsorship letter.

c. In accordance with DOD 5220.22–R, when circumstances require a contractor to be immediately eligible for access to classified information, a sponsor may request an interim FCL through DSS.

2–5. Interim facility security clearances

a. DSS automatically processes all requests for confidential and secret FCLs for interim clearances, when possible. However, DA sponsorship of interim top secret FCLs must be justified on a case-specific basis in accordance with the DOD 5220.22–M. To request an interim top secret FCL, the program, PEO, or unit, and/or activity requesting the interim clearance prepares and routes sponsorships through command channels to the command ISS for review prior to forwarding to Defense Industrial Security Clearance Office (DISCO). Each request must include the following:

(1) A justification for the interim top secret FCL.

(2) The legal name of the contractor company (facility) being sponsored, complete street address, and names and positions of people who are applying for interim top secret access authorization.

(3) The address of the authorizing DSS office.

(4) The safeguarding requirement as identified on DD Form 254.

(5) A copy of the DD Form 254.

b. Receipt of an interim top secret FCL does not authorize access to SCI if the contractor is otherwise not authorized access to SCI (see AR 380–28 and para 2–12).

Section II
Foreign Ownership, Control, or Influence

2–6. General

a. A U.S. company is considered to be under FOCI whenever a foreign interest has the power, direct or indirect (whether or not exercised), to direct or decide matters affecting the management or operations of the company in a manner that may result in the unauthorized access to classified or controlled unclassified information or adversely affect the performance of classified contracts.

b. An uncleared company determined to be under FOCI is ineligible for a FCL unless security measures have been put in place to mitigate the FOCI. In making a determination as to whether a company is under FOCI, DSS reviews the information contained on the SF 328 (Certificate Pertaining to Foreign Interests) provided by the company and any other relevant information. Whenever a company has been determined to be under FOCI, the primary concern is the safeguarding of classified information. For DA contracts, DSS, in coordination with the PM, COR, and/or ISS, is responsible for taking action that is necessary to safeguard classified information.

c. A U.S. company's FCL will be invalidated by DSS if a mitigation agreement is not in place by the time of the merger, sale, or acquisition that is the cause of the FOCI concern. If the company is under FOCI, but does not have a pending requirement for possession of classified material, DSS will administratively terminate the FCL.

2–7. Mitigating a foreign ownership, control, or influence issue

a. If DSS determines that a company is under FOCI, DSS will require the company to submit a FOCI action plan. If a FOCI action plan is not acceptable, DSS may establish a FCL that limits the level and type of classified information to which a FOCI contractor has access to ensure classified information is adequately safeguarded by the cleared company, or DSS may invalidate the FCL until the FOCI issues are resolved. Such restrictions might affect ongoing, pending, and future classified contracts with the contractor. The KO and/or COR should discuss this impact with the PM, the ISS, and servicing foreign disclosure officer.

b. There are several methods that may be applied to mitigate the risk of foreign ownership. While these methods are mentioned in relation to specific ownership and control thresholds, they should not be interpreted as policy to predetermine or select a certain mitigation plan without regard for the overall risk assessment. The following are some of the FOCI mitigation methods:

(1) *Board resolution.* When a foreign interest does not own voting interests sufficient to elect, or otherwise is not entitled to, representation on the company's governing board, a resolution by the governing board will normally be adequate. The governing board will identify the foreign shareholder and describe the type and number of foreign-owned shares; acknowledge the company's obligation to comply with all ISP and export control requirements; and certify that the foreign owner does not require, will not have, and can be effectively precluded from unauthorized access to all classified and export-controlled information entrusted to or held by the company. The governing board will request annual certifications by the cognizant security agency acknowledging the continued effectiveness of the resolution. The company will distribute to members of its governing board and to its key management personnel copies of such resolutions, and report in the company's corporate records the completion of such distribution (for example, A British national owns 10 percent of the company's voting stock and that 10 percent stock ownership does not allow the British National to appoint a representative to the company's board of directors).

(2) *Security control agreement.* A SCA is used when the cleared company is not effectively owned or controlled by a foreign entity but the foreign interest is entitled to representation on the company's governing board (for example, A Danish corporation owns 25 percent of the cleared company's voting stock and that 25 percent ownership allows the Danish corporation to appoint a representative(s) to the company's governing board). There are no access limitations under a SCA.

(3) *Special security agreement.* A SSA is used when a company is effectively owned or controlled by a foreign entity. The SSA has access limitations. Access to prescribed information by a company cleared under a SSA may require that the GCA complete a NID to determine that the release of proscribed information (top secret, SCI, SAP, COMSEC, or restricted data) to the company will not harm the national security interest of the U.S. Examples are available at the DSS Web site (https://www.dss.mil).

(4) The SCA and SSA are substantially identical arrangements that—

(a) Impose various industrial security and export control measures within an institutionalized set of corporate practices and procedures.

(b) Require active involvement in security matters of senior management and certain board members (officers, directors, and/or outside directors), who must be cleared U.S. citizens.

(c) Provide for the establishment of a Government Security Committee to oversee safeguarding of classified and export controlled information entrusted to the contractor (the Government Security Committee consists of officers, directors, and/or outside directors).

(d) Preserve the foreign shareholder's right to be represented on the board by inside directors with a direct voice in the business management of the company while denying unauthorized access to classified information.

(5) *Proxy agreement and voting trust agreement.* A PA and VTA are used when a cleared company is owned or controlled by a foreign entity. The PA and VTA are substantially identical arrangements whereby the voting rights of the foreign owned stock are vested in cleared U.S. citizens approved by DSS. Neither arrangement imposes any restrictions on the company's eligibility to have access to classified and/or CUI or to compete for classified contracts.

(a) Establishment of the PA or VTA involves the selection of three proxy holders or trustees who must be directors on the cleared company's board.

(b) The proxy holders or trustees exercise all prerogatives of ownership with complete freedom to act independently from the foreign stockholders, with the following exceptions:

1. The proxy holders or trustees must obtain approval from the foreign shareholder regarding the following matters:

a. The sale or disposal of the corporation's assets or a substantial part thereof.

b. Pledges, mortgages, or other encumbrances on the capital stock.

c. Corporate mergers, consolidations, or reorganizations.

d. The dissolution of the corporation.

The filing of a bankruptcy petition.

2. The proxy holder or trustees assume full responsibility for the voting stock and for exercising all management prerogatives in such a way as to ensure that foreign stockholders, except for the approvals enumerated in paragraph 2–7*b*(5)(a), will be insulated from the cleared facility (cleared company) and continue solely in the status of beneficiaries.

3. The company must be organized, structured, and financed to be capable of operating as a viable business entity independent from the foreign shareholder.

4. Individuals serving as proxy holders or trustees must be responsible U.S. citizens residing within the U.S. be completely disinterested individuals who are capable of exercising the management prerogatives relating to their position in a way that ensures the foreign owner(s) can be effectively insulated from the cleared company, have no prior involvement with the cleared company, the entities with which it is affiliated or the foreign shareholder, and be eligible for a personnel security clearance at the level of the FCL.

5. Management positions requiring personnel security clearances must be filled by U.S. citizens residing in the U.S.

6. The primary difference between the PA and the VTA is that under the VTA, the foreign owner transfers legal title in the company to the trustees that are approved by DSS. Under a PA, the foreign interest retains legal title to the stock at issue while relinquishing most voting rights to designated persons (that is, proxies).

2–8. Foreign ownership, control, or influence factors (refer to National Industrial Security Program Operating Manual)

The following factors relating to the company, the foreign interest, and the government of the foreign interest, as appropriate, are considered in the aggregate in determining if a company is under FOCI, its eligibility for a FCL, and the protective measures required:

a. Record of economic or government espionage against U.S. targets.

b. Record of enforcement and/or engagement in unauthorized technology transfer.

c. Type and sensitivity of the information that will be accessed.

d. Source, nature, and extent of FOCI.

e. Record of compliance with pertinent U.S. laws, regulations, and contracts.

f. The nature of any bilateral and multilateral security and information exchange agreements that may pertain.

g. Ownership or control, in whole or in part, by a foreign government.

h. Any other factor that indicates or demonstrates a capability on the part of foreign interests to control or influence the operations or management of the business organization concerned.

2–9. National interest determination

a. Prior to authorizing access to proscribed information (top secret; COMSEC, except classified keys used for data transfer; restricted data; SAP; and SCI) by contractors cleared or in process for clearance under a SSA, the Army must determine if release of proscribed information is consistent with the national security interests of the U.S. Such a determination is referred to as NID. NID package should not contain any classified information.

b. The requirement for a NID applies to new contracts, to include precontract activities in which access to proscribed information is required, and to existing contracts when contractors are acquired by or merge with foreign interests and an SSA is the proposed FOCI mitigation method.

(1) If access to proscribed information is required to complete precontract award actions or to perform on a new contract and the company is determined to be under FOCI and an SSA is the proposed mitigation, the GCA will determine if release of the information is consistent with national security interests.

(2) For contractors that have existing contracts and require access to proscribed information, have been or are in the process of being acquired by foreign interests, and have proposed an SSA to mitigate FOCI issues, DSS will notify the relevant GCA of the need for a NID.

(3) Where no interagency coordination is required because the program or requiring activity owns or controls all of the proscribed information in question, the program or requiring activity must provide a final documented decision to the DCS, G–2 (DAMI–CDS) within 30 days of the date of the DSS request for the NID. The affected GCA will provide the final documented decision to DSS. The program, requiring activity, ISS, KO, and/or COR must ensure that a copy is provided to the contractor.

(4) If the proscribed information is owned by or under the control of a department or agency other than the program or requiring activity (that is, National Security Agency, Office of the Director of National Intelligence, Department of Energy, and the ASPD for SAPs), the affected GCA in coordination with DCS, G–2 will provide written notice to that department or agency that its written concurrence is required. The original notice will be forwarded by the affected GCA, through the ACOM, ASCC, or DRU to the department or agency within 30 days of being informed by DSS of the requirement for a NID. The department or agency that owns or controls the proscribed information will provide a final documented decision to the affected GCA within 30 days of the receipt of the request for the NID.

c. In accordance with 10 USC 2536, DOD and the Department of Energy cannot award a contract involving access to proscribed information to a contractor effectively owned or controlled by a foreign government unless a waiver has been issued by the SECDEF or Secretary of Energy. The NID must be prepared and forwarded to DCS, G–2 who will, in turn, forward it to the USD (I) for a recommendation. DSS will not upgrade an existing contractor FCL under an SSA to top secret unless an approved NID covering the prospective top secret access has been issued.

d. The NID will be forwarded to the ISS, who in turn will prepare the NID in coordination with the COR and the PM. A written justification must be attached to the NID. The justification must address and explain how the FOCI contractor's product or service is crucial or is the sole available source to the Army. The justification may include, but is not limited to, fully identifying the company, foreign interest, contract (agency or number), and a brief description of the work to be performed under the contract, including proscribed information to be released to company in question during performance of the contract. The NID will be staffed through the requisite channels to the appropriate program or senior executive level for the command, unit, and/or activity for signature. All Army units subordinate to ACOMs, ASCCs, and DRUs will process their NID packages through their respective ACOM, ASCC, or DRU. The ACOM, ASCC, or DRU will forward the completed NID package to DCS, G–2 (DAMI–CDS). NIDs must be completed within 30 days of receipt.

Section III
Contractor Personnel Security Clearances

2–10. Function

A PCL is an administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted. The DISCO grants and maintains contractor PCLs. Also, DISCO terminates contractor PCLs when the contractor no longer requires a PCL or when a contractor employee is terminated. Administrative termination of a PCL for these reasons carries no adverse implications regarding the employee or the contractor.

2–11. Revocation and/or suspension

a. A contractor whose security clearance has been denied or revoked by DISCO has the opportunity to appeal the decision. EO 10865 outlines the process for contractors.

b. For contractor personnel, the denial, revocation, and appeal process is the responsibility of the Defense Office of Hearings and Appeals. The individual may request a hearing before a Defense Office of Hearings and Appeals administrative judge in order to provide additional, relevant information, and will have the opportunity to cross-examine witnesses. Upon completion of the hearing, the administrative judge will render a decision. If the decision is to deny or revoke the security clearance, the individual has the opportunity to appeal the decision to the Appeal Board. The Appeal Board will review the case file and render its decision. This decision is final and concludes the administrative appeal process.

c. At the conclusion of the appeal process, an individual whose security clearance has been denied or revoked may not reapply for a security clearance for one year from the date of the final decision. The individual may reapply for a security clearance through their company if there is a need for access to classified information. The reapplication must be accompanied by documentation that the circumstances or conditions that resulted in the denial or revocation have

been rectified or sufficiently mitigated to warrant reconsideration. Director, Defense Office of Hearings and Appeals may accept or reject the reapplication.

2–12. Interim clearances

a. DISCO automatically processes all requests for confidential or secret PCLs for interim clearances. A contractor employee who is not yet cleared for access to top secret information but needs such access to perform on an Army classified contract, may be sponsored by the employing contractor for an interim top secret PCL when the company holds a top secret FCL. Such a request will be processed as follows:

(1) The contractor will submit a request to the KO, who in turn will seek concurrence from the PM.

(2) The contractor's request must clearly explain why the individual needs an interim PCL, why contract requirements cannot be satisfied with another individual more suitably cleared, and what the potential adverse impact would be on contract performance if an interim PCL were not granted. The KO will deny contractor requests that do not meet these criteria.

(3) The KO will send favorably endorsed requests to the contractor, who then includes the endorsement in the personnel security questionnaire package for transmission to DSS for action. The KO will promptly return denied requests to the contractor.

b. Receipt of an interim top secret PCL does not authorize a contractor access to SCI (see DOD 5105.21–M–1).

2–13. Trustworthiness determinations and/or personnel security standards for persons occupying information systems positions

When contractors require unescorted entry to restricted areas, access to CUI, or access to government information systems and/or sensitive equipment not involving access to classified information, the contractor's personnel security questionnaire is processed by the sponsoring Army activity in accordance with AR 380–67, AR 25–2, and current DCS, G–2 policy.

2–14. Self-employed consultants

a. A self-employed consultant with no requirement to possess classified information away from a cleared facility or Army agency does not require a FCL. A self-employed consultant is an individual under contract to provide professional or technical assistance to a cleared company or the Army directly in a capacity requiring access to classified information. Self-employed consultants to cleared companies, who require access to classified information, must have a valid PCL. The consultant is considered an employee of the hiring cleared company. The consultant and cleared company need to jointly execute a consultant certificate specifying security responsibility. Consultants are not allowed to possess classified information except at the cleared company or in an Army facility. Consultants are not eligible for access to classified information outside the U.S., Puerto Rico, and the trust territories and possessions, unless in official travel status of not more than 90 days in any 12-month period.

b. The DA may hire self-employed consultants, but the PCL must be completed by the sponsoring security officer. In this scenario, there is no cleared company and/or FCL, and the self-employed consultant is an expert in the subject matter and the sponsoring security officer will provide security oversight—

(1) The supporting security officer will in-process the self-employed consultants in Joint Personnel Adjudication System. The supporting security officer will initiate investigations for self-employed consultants for the purpose of obtaining a security clearance. The investigation will be submitted to DISCO for any required granting of interim or final clearance eligibility and further processing to the Office of Personnel Management.

(2) For self-employed consultants who will directly work for the DA, a DD Form 254 will be executed with the appropriate security requirements. A DD Form 254 should also be reviewed by the PM and/or SMEs to ensure the appropriate security requirements are levied on the consultant.

(3) For self-employed consultants who require SCI access, the security officer is responsible for processing an investigation packet. Self-employed consultants are not processed through the Joint Personnel Adjudication System for SCI access; the security officer will follow the clearance process in paragraph 2–12, and request that the investigation packet be forwarded to the Army central clearance facility for SCI access determination. The security officer must maintain a database of these self-employed consultants for metrics purposes.

Chapter 3
Security Training and Briefing

3–1. Security training

DA classified solicitations, contracts including the appropriate contract security and/or performance defining documents (for example, PWS, SOW, and/or SOO), and DD Form 254 must stipulate contractor compliance with and participation in pertinent Army, command, and installation security training programs when performance or services will occur on a DA installation and the contractors are embedded or integrated into the DA activity or office. Some examples of this

training for embedded or integrated contractors are OPSEC, antiterrorism and force protection, information systems, North Atlantic Treaty Organization security awareness for access to the Secret Internet Protocol Router Network, and job-related training. Contractors may be exempt from such security training if they can provide documentation that they have had similar training from their FSO.

3–2. Contract specified training

When specified in a contract, the information security training requirements identified in AR 380–5 satisfy the DOD 5220.22–M training provision for contractors on an installation. Other DA functional and/or security discipline offices may use this training provision for operational efficiency; however the specific requirements must be identified in DD Form 254 and the security section of the contract document. Any training requirements that the installation or tenant facilities require of the contractors must be added to DD Form 254 and the security section of the contract document. Examples of training requirements include, but are not limited to, are information assurance and antiterrorism and force protection training.

3–3. Initial facility security officer

When a contractor operation is designated as a cleared facility on an installation, DSS will provide the initial FSO briefing in accordance with the DOD 5220.22–M and CSO guidance. The exception to this will be if DSS has been carved-out of the oversight of the cleared facility. In that event, the ISS will provide the briefings to the FSO, as well as maintain on file those briefings provided to the FSO and/or the contractors within that cleared facility.

3–4. Security Awareness Training

a. DA, the CSM, or the security officer will provide information security program training (initial, refresher, and annual) and other security awareness support to contractors on the installation and embedded or integrated in the DA activities.

b. The DA activity, working in concert with the ISS, will incorporate language into the contract and the DD Form 254, that requires contractor personnel to attend and/or receive information security training per DODM 5200.01–M and AR 380–5, as well as any additional DA training requirements such as AR 530–1, AR 25–2, and AR 525–13. CSM will ensure that contractor personnel are included in the command security education program. Security managers will monitor contractor attendance at security awareness training.

3–5. Security briefing requirements

a. The KO and COR of cleared facility contractors and embedded or integrated contractors located on an installation or within a tenant activity, in coordination with the supporting security officer, is responsible for ensuring contractor employees receive all required security briefings and debriefings as mandated by the DOD 5220.22–M and DD Form 254.

b. For contractor personnel, AR 380–5 security training requirements are equivalent to and satisfy the training requirements of the DOD 5220.22–M, where appropriate. The KO and COR will ensure contractor personnel within their area of responsibility attend security training and satisfy DOD 5220.22-M documentation requirements.

Chapter 4
Security Specifications and Guidance

Section I
Security Guidance Responsibility

4–1. Security requirements

The KO provides security guidance from the ISR, NISPOM, DOD 5200.01–M, this regulation, and installation security requirements through contract documents. KOs are the only personnel authorized to sign, modify, or negotiate changes to contracts. However, KOs should seek assistance from the appropriate ISS to review, sign, and date any modification to DD Form 254 on their behalf.

4–2. Security classification guidance or guides

The DA program, project, or activity will identify (by title, functional office of primary responsibility, and approval date) the specific security classification guidance or guides applicable to the contract on DD Form 254, block 13 or the appendix and/or SCI addendum (see DD Form 254). The requirement for SCG(s) must also be annotated on DD Form 254, block 10k. The DA activity and/or program will provide copies of the SCG to the contractor prior to the contract commencing, as long as the contractor has the appropriate FCL level in place.

Section II
DD Form 254

4–3. Completing DD Form 254

a. The designated ISS completes DD Form 254 for a prime contract and signs in block 16. Contractor input is encouraged, but it is the Government's responsibility to complete and review all security requirements prior to the issuance of a contract. The prime contractor is responsible for completing and coordinating the subcontractor's DD Form 254.

b. The DA program, project, or activity ISS assists the KO, COR, and/or PM with the preparation of the DD Form 254 for each classified contract by inserting all necessary security requirements identified in the security section of the documents which define contract requirements and performance (for example, request for bid, request for proposal, SOW, PWS, and/or SOO). Only actual requirements are stated. If the contract develops into a higher or lower classification, a revised DD Form 254 will be issued. Any revisions or modifications that require an updated DD Form 254 must be submitted to the ISS for review and signature. The ISS will include their name, activity, contact information, and signature in block 16.

c. When drafting the DD Form 254, the program, project, or activity ISS will consult with the KO and other installation, activity, or organization security personnel or staff elements affected under the terms of the solicitation or contract to ensure accuracy and completeness.

d. When contractor performance is on a DA installation, the DA program, project, or activity must identify and specify all contract performance locations on DD Form 254. Once the DD Form 254 is completed and signed by the ISS, the DD Form 254 is forwarded to the KO for inclusion in the solicitation or contract award. The contractor uses the security specifications and other contractual security requirements listed in the PWS, SOW, and/or SOO and DD Form 254 to accurately estimate the cost of security. Overstating unnecessary security requirements "just in case" places an undue burden on the contractor and increases the Government's costs. Understating the security requirements creates a potential security compromise.

e. To the greatest extent possible, the DD Form 254 should be kept unclassified unless mission requirements dictate otherwise.

f. If a contract is anticipated to involve CPI, or a strong potential for involvement of CPI exists, then block 10j (OPSEC requirements) must be checked, and block 14 should state that program protection plans will be provided as government furnished information if CPI is identified. Block 15 should provide for oversight by the DCS, G–2 to ensure program protection plans implementation and CPI protection.

4–4. Reviewing, revising, and certifying DD Form 254

a. The ISS assists the KO and/or COR and PM with the preparation of the DD Form 254 to ensure that the security classification guidance and requirements are accurate in the appropriate contract documents. The ISS annotates (signs) in block 16 as the certifying and approving official for the security requirements.

b. The DA program, project, or activity, in coordination with the COR and ISS, reviews the DD Form 254 and applicable security specifications and guidance once every 2 years at a minimum, to ensure it is accurate and current. When changes are necessary, the contract and DD Form 254 will be modified, if appropriate, and the revised DD Form 254 with new guidance will be provided to the ISS for signature.

c. The KO or COR and/or PM certify by signing the DD Form 254 in block 13, and the ISS certifies by signing in block 16.

d. When the contract is administered and/or overseen by DA, but another DOD component tasks from the contract, the DA ISS will certify by signing DD Form 254 in block 16, and the Service or agency point of contact will review and sign in block 13. In the case of a disagreement with the tasking Service or agency regarding signature authority for the DD Form 254, a memorandum of agreement between the DOD components should be concluded to outline who will sign the DD Form 254 in blocks 13 and 16 and provide oversight for security and related areas.

4–5. Distribution of DD Form 254

a. The COR is responsible for forwarding a copy of the completed and signed DD Form 254 to the CSO for the prime contractor and appropriate offices listed in the distribution section (block 17) of the DD Form 254.

b. When DSS is relieved of security oversight responsibility for cleared facilities performing on Army programs, the ISS is responsible for forwarding a copy of the completed and signed DD Form 254 to the cognizant security agency, as well as any additional offices listed in block 17.

Chapter 5
Oversight Reviews and Reporting Requirements

Section I
Industrial Security Staff Assistance Visits, Self-Inspections, and/or Inspections

5–1. Responsibility

a. DSS is responsible for conducting security reviews and inspections for all cleared contractor facilities; however, when DSS does not have security cognizance over a cleared contractor facility (for example, in the case of a carve-out), and the appropriate commander is responsible for security oversight, the supporting ISS is responsible for conducting an annual inspection for such facilities.

b. The inspection will be used to evaluate the contractor's compliance with contract specific-security requirements and pertinent DOD and Army security authorities, as outlined in the contract and DD Form 254.

c. The results of the inspection will be maintained by the ISS and a copy provided to the KO and/or COR.

5–2. Self-inspections

a. The purpose of a self-inspection is to ensure that the information system is operating as accredited and that accreditation conditions have not changed. Self-inspections should be conducted annually on the command, unit, or activity by the ISS. Self-inspections should be coordinated with the appropriate SMEs, and will include the areas of security policy and procedures, security administration, industrial security, information security, personnel security, physical security, technical security (TEMPEST and technical surveillance counter-measure), and information assurance, as related and applicable to the industrial security program. The ISS must specify in writing all findings and corrective actions taken and retain the report until the next self-inspection. Self-inspection results may be reviewed by DCS, G–2 during staff assistance visits and/or inspections.

b. The ISS must ensure that self-inspections are conducted at cleared contractor facilities on DA installations over which the commander has elected to assume security oversight. All findings and corrective actions will be in writing and retained until the next self-inspection. A copy will be provided to the ISS.

5–3. Staff assistance visits

a. DCS, G–2 will work with the ACOMs, ASCCs, and DRUs to achieve and maintain an effective and compliant Army industrial security program. This requires DCS, G–2 to coordinate with the ACOMs, ASCCs, and DRUs regarding their missions, contractual or program requirements, and other influences impacting the Army's ISP.

b. The ACOMs, ASCCs, and DRUs will work with their major subordinate commands, activities, and/or units, programs, and PEOs, as applicable, to ensure they maintain an effective and compliant industrial security program.

5–4. Scheduling staff assistance visits and/or inspections

a. An annual security review or inspection will be conducted by the supporting ISS for each cleared contractor facility on an installation for which the commander has coordinated with DSS and retained security oversight. Commanders on DA installations have the option of retaining oversight of contractor facilities, or deferring CSO responsibilities to DSS.

b. Unless conducting an unannounced security inspection on a cleared contractor facility overseen by DA, the ISS will provide the KO and/or COR and FSO at least 30 days advance written notice.

c. ACOMs, ASCCs, and DRUs will provide their major subordinate commands, activities and units, programs, and PEOs at least 30 days advance written notice of each visit or inspection.

5–5. Performing industrial security reviews and/or inspections

a. The ISS will coordinate with other DA security disciplines such as OPSEC, information security, COMSEC, and research and technology protection to provide specialized expertise when necessary to complete a security review. The staff assistance visits is complete when all security requirements imposed under the terms of the contract have been evaluated.

b. FCL files must contain all key documentation prescribed by the DOD 5220.22–R and DSS, to include a copy of DD Form 254 and related contract security requirement documents.

5–6. Post-industrial security reviews and/or inspections requirements

When DA is responsible for oversight and inspection of a cleared contractor facility, the ISS will provide a report to company senior management officials, the FSO, and the KO and/or COR with a copy furnished to DSS, within 10 days of completing each security review and/or inspection. The report should—

a. Confirm the contractor's security status as discussed during the exit interview.

b. List any deficiencies requiring corrective action in writing.

c. Within 30 days, request written confirmation on the status of any open major discrepancy (that is, a condition that resulted in, or could reasonably be expected to result in, the loss or compromise of classified information).

d. The ISS may extend the time for corrective action if required changes are significant, the contractor is making reasonable efforts to resolve the matter expeditiously, and the ISS determines that such an extension is not likely to result in the loss or compromise of any classified or sensitive information.

e. Document security reviews or inspections for a cleared facility on an installation as required by the DOD 5220. 22–R , DOD 5220.22–M, and DSS guidance. Maintain copies of completed security reviews or inspection reports with the presecurity assistance visit letter and completed post-assistance visit correspondence for 2 years from the date of the most recent security review or inspection.

5–7. Unsatisfactory industrial security reviews and/or inspections

a. When the DA has determined to retain cognizant oversight and inspection authority for a cleared contractor facility, the ISS will assign a cleared contractor facility on an installation an unsatisfactory staff assistance visits rating when one or more of the following are found:

(1) The cleared contractor facility has failed or is failing to perform its contractual security responsibilities satisfactorily.

(2) Failures in the cleared contractor company's security program have resulted in or could reasonably be expected to result in the loss or compromise of classified or CUI.

(3) The cleared contractor has failed or is failing to implement government furnished program protection plans to protect CPI.

(4) The cleared contractor has failed or is failing to adhere to the policies and procedures outlined in the DD Form 254.

(5) The cleared facility has FOCI issues that have not been mitigated by DSS and/or key management personnel have not maintained their PCLs.

b. The ISS must coordinate with DSS, the COR, the FSO, and the PM when assigning an unsatisfactory rating for a cleared contractor facility on an installation.

c. The home office facility for the cleared facility is ultimately responsible for meeting contract security requirements. When assigning an unsatisfactory rating, the ISS notifies the home office facility immediately through the KO and/or COR and requests prompt and complete corrective action. If the home office facility fails to take corrective action, the FCL may be invalidated or terminated by DSS. The servicing ISS should notify DSS if problems continue.

5–8. Invalidating the facility security clearance

a. DSS notifies the GCA in writing when the contractor company's FCL is invalidated.

b. A contractor that fails to correct security deficiencies that subsequently result in such invalidation may lose its FCL.

c. FCLs that are invalidated (administratively suspended) due to unresolved FOCI concerns will remain invalidated until FOCI mitigation instruments are put in place by DSS. An invalidated FCL limits the contractor on contract performance and bidding on new work. The contractor is permitted to continue on current classified contracts unless otherwise formally directed by DSS.

Section II
Conducting Information Security Program Reviews

5–9. Requirements

Contractors integrated and/or embedded into DA activities on an installation will be integrated into the overall Army information security inspection program per DODM 5200.01 and AR 380–5, unless the contractor has received prior training from their FSO and the COR has documentation of the training. This ensures that the embedded or integrated contractors are provided the required annual security training, as well as any additional annual training the Army may require.

5–10. Scheduling reviews

a. Schedule security inspections per DODM 5200.01 and AR 380–5 guidance.

b. The DA activity is responsible for ensuring those contractors who are embedded or integrated into the DA activity on an installation implement and comply with DODM 5200.01 and AR 380–5 requirements.

5–11. Documenting reviews

a. The COR will establish files and maintain the following documentation, as appropriate:

(1) Signed copy of DD Form 254 (for both the prime contract and any subcontracts) and any revisions.

(2) Signed copy of the tenant security agreement, if applicable.

(3) Current listing of the key management officials or representatives of the embedded or integrated contractor company.

(4) Copy of the last annual program review.

(5) Copies of last two self-inspections reports. The annual program review can be used to substitute for one of the self-inspections.

b. When DA has determined to retain responsibility for security oversight and inspection of a cleared contractor facility, the ISS who is responsible for the inspections and oversight of the cleared facility will brief key DA personnel, to include the KO and/or COR and the PM and/or PEO, on the status of the installation or unit security program. The ISS will retain copies of the inspections and provide a copy of reviews and other related assessments to the COR. A copy of the inspection report is normally not provided to DSS unless extenuating circumstances exist.

5–12. Major security deficiencies or noncompliance

The KO and/or COR must notify DSS, in writing, through the contracting office, regarding any major security program deficiencies or noncompliance with the terms of the visitors group security agreement and/or contract. When DA has retained cognizant oversight of the cleared contractor facility, the COR must ensure that the PM and/or PEO, KO, ISS, and supporting SM are all notified regarding any major security program deficiencies.

Chapter 6
Visits and Meetings

6–1. Visits and meetings between Department of the Army personnel and cleared U.S. contractors

This chapter establishes procedures and responsibilities regarding visits and meetings between cleared U.S. company personnel and Army personnel where access to classified information is involved. A company's operation may either be considered a visitor group (which follows the security procedures of the installation or the DA activity) or the commander may elect to request a FCL for the cleared company. FCLs will not be established on the installation or tenant activity solely for the purpose of permitting company personnel entry authorization into a controlled area unless access to classified information is required in the performance of the contract.

a. The ISS, in coordination with the security officer and the COR, verifies that a company has an FCL, and reviews an approved Government database to determine the PCL of the visiting cleared contractor employee. If the hosting DA activity does not have access to an approved Government database, the hosting DA activity will contact the higher echelon security organization for assistance in verifying the PCL of the visiting personnel.

b. Visit notifications are valid based on the duration the contractor is required to work, visit, and/or meet with DA personnel. The duration of the visits for embedded or integrated contractors and/or tenant activity will be left up to the installation and/or tenant activity but can be based on the expiration of the contract.

c. Visits to DA installations and/or activities outside the United States will be processed in the same manner as other classified visits by verifying the cleared contractor's clearance in the applicable Government database or relying on the cleared company's certification of the clearance of their employee. Contractors required to visit installations and/or activities outside the United States on a temporary basis, may require additional training based on local, installation, DA activity, and/or theater policies.

d. The installation commander or tenant, agency, and/or activity head is the sole authority responsible for granting contractors access to the installation, regardless of which DOD agency, military service component, or activity awarded the contract. The commander or agency and/or activity head designates contractors that require access to the installation in the performance of a Government contract as intermittent visitors, embedded or integrated contractors, or cleared facility contractors.

6–2. Contractor visits to an Army installation, tenant, agency, and/or activity

DOD cleared contractors located on or visiting a DA installation, tenant, agency, and/or activity in support of a classified contract must comply with the DOD 5220.22–R, the DOD 5220.22–M, visit requirements, this regulation, and other DA policy on visit requirements of the installation to be visited. Advance notification of pending contractor visits will be provided to the command ISS by the FSO using the applicable Government database.

6–3. Foreign visitors and foreign disclosure requirements

Guidance regarding visits and meetings between cleared U.S. contractors and personnel representing foreign contractors, as well as visits and meetings between the DA and personnel representing foreign contractors. AR 380–10 provides policy on government-to-government disclosure.

Chapter 7
Subcontracting

7–1. Prime contractor responsibilities

a. Prime contractor FSOs are responsible for ensuring their subcontractors are knowledgeable of and comply with relevant law, policy, and other security requirements (see DOD 5220.22–M, DA regulations, or installation requirement) as identified in the contract, DD Form 254, and/or other contracting documents.

b. Prime contractors are responsible for issuing a subcontractor DD Form 254 for any classified work or material that the subcontractor will have access to while working for the prime contractor. The FSO will sign DD Form 254, block 16 and ensure that program, and/or Army activity points of contact information are included on DD Form 254, block 13. The prime contractor FSO will provide the KO and/or COR with a copy of all subcontract DD Form 254s to be attached to the prime contract. The KO and/or COR will provide a copy of all subcontract DD Form 254s to the ISS.

c. The ISS will ensure that the COR maintains a record of all prime and subcontracts for metrics purposes.

d. Prime contractors have a responsibility to provide oversight of their subcontracts in accordance with the DOD 5220.22-M, and must identify and report to DSS, and the COR any security measures or requirements that are found either to be inadequate or excessive, and request a revision to the DD Form 254.

7–2. Subcontractor responsibilities

a. Subcontractors are responsible for ensuring that any changes to their company status, key management personnel, FCL, and/or contractor personnel are provided to the prime contractor FSO.

b. Subcontract FCLs cannot be at a level higher than the FCL of the prime contract.

Chapter 8
Information Technology and Automated Information System Security

8–1. System accreditation

a. When ISP oversight is retained by the DA for cleared facilities on an installation, the KO and/or COR coordinates IT system accreditation, COMSEC, and TEMPEST requirements with the responsible installation security office, the ISS, and DSS as appropriate.

b. Integrated contractors and visitors will use approved DA IT and/or networks to process classified and CUI, and will comply with all DOD and DA information assurance policy guidance and requirements.

8–2. Contractor access to Army information technology and/or automated information system

a. Contractor employees who require access to government IT under the terms of a government contract must be determined to be trustworthy by a designated Government official prior to grant of IT access in accordance with AR 25–2 and AR 380–67.

b. For contractors, the minimum background investigation requirement for access to Government information systems will be determined in accordance with AR 25–2.

c. Foreign national contractor personnel who are sponsored by their government as part of an official visit or assignment to work on a DA installation or facility and require access to a DA network, may be eligible for IT access. The official visit request will contain the clearance or investigative level authorized by that government and must satisfy the minimum investigative standard required by DOD and DA policies.

d. Access trustworthiness determinations will be processed in accordance with DOD 5200.2–R, AR 25–2, and AR 380–67.

e. This requirement for contractor access to IT systems, at a minimum, must be specified in the basic solicitation and/or contract documents for classified contracts.

f. Contracts or solicitations (classified and unclassified) involving contractor access, use, operation, or maintenance of a Government IT system will be routed through the ISS for review and coordination with the appropriate DA staff organization.

g. Contractor access to Government IT or Automated Information Systems does not permit contractor access to caution-proprietary information without further appropriate authorization.

h. All contractors who require access to a DA network must be processed in the Contractor Verification System database for a common access card (CAC).

(1) The FSO and/or contractor must complete an online CAC application, which is submitted to the DA trusted agent for review.

(2) The trusted agent is responsible for establishing the contractor's need for logical and physical access to a DA network, validating the Tier 1 investigation or equivalent, and approving or disapproving each application.

(3) Each contractor who requires access to a DA network and a CAC must undergo, at least a Tier 1 national agency check with inquiries investigation which includes the requirement for a fingerprint card.

Chapter 9
Special Requirements

9–1. Special access programs

Army special access programs use DSS for security oversight of industrial contractors authorized SAP access unless DSS is specifically carved out by the Deputy Secretary of Defense. Requests for carve-out status must be staffed to the Army special access program coordination office, the technology management office. In accordance with AR 380–381, the Army special access program coordination office assigns oversight responsibility for security oversight when DSS is carved out of oversight of an Army SAP (see AR 380–381).

9–2. Sensitive compartmented information

The U.S. Army Intelligence and Security Command contractor support element (CSE) provides dedicated SCI security support and oversight of the Army SCI ISP. The CSE, contract monitor (CM), FSO, and/or contract special security officer will track contractor access in the Army Contractor Automated Verification System for the contractor employee. For Army SCI contracts, signal intelligence officers, CMs, FSOs, and contract special security officers will e-mail CSE (cseoperations@mi.army.mil). All SCI contractor nominations must be submitted through the Army Contractor Automated Verification System and approved by the COR.

a. DA contracts requiring contractor access to SCI will be managed in accordance with DOD 5105.21–M–1, AR 380–28, AR 715–30, intelligence community policy guidance (as appropriate), the Army Handbook for SCI Contracts, and this regulation.

b. The release of SCI information to a DA or self-employed consultant requires specific security safeguards in addition to those specified in the DOD 5220.22-M. The U.S. Army Intelligence and Security Command, DCS, G–2, through the CSE or its successor organization, acting on behalf of DCS, G–2 is the cognizant security agency for the DA, has exclusive administrative security oversight responsibility for all SCI released to the contractor or developed under the DA contract.

9–3. Contracting process

a. Pursuant to AR 380–28, DA personnel involved with SCI contracts will coordinate with the CSE for guidance to meet the special security requirements for the protection of SCI material and documents. AR 380–28 also delineates the specific SCI responsibilities assigned to the CSE, COR, CM, and contract special security officer.

b. AR 380–381 provides specific contracting process responsibilities for the SAP security officer.

c. For contracts requiring contractor access to SCI, a COR and/or CM will be appointed, in writing, to be responsible for drafting the DD Form 254. The COR and/or CM will coordinate the draft DD Form 254 with the ISS and CSE prior to any solicitation or contract award. Any revisions to DD Form 254 will be incorporated into the contract via contract modification.

d. A DSS final top secret FCL is a prerequisite for award of a DA SCI contract to a specific contractor. The KO, COR, PM, CM, contract special security officer, and ISS will all be cleared at the top secret and/or SCI level for all SCI contracts.

e. The ISS will maintain copies of the SOW and/or PWS, prime contract DD Form 254, and CM appointment letters, as applicable, for all classified contracts for 2 years after contract completion. Retained files can be either hard copies or electronic.

f. DSS has security inspection responsibility for the collateral classified contractor areas and information maintained in those areas. DSS is not responsible to inspect SCI storage areas or information. For DA contracts, the CSE is the cognizant security activity for SCI contracts and information.

g. The contractor must obtain a final top secret FCL prior to initiating the SCI portion of the contract. Failure by the KO and/or COR to obtain a final top secret FCL is justification for termination of the contract.

Chapter 10
International Security Requirements

10–1. Procedures for contractor operations overseas

a. DOD policy does not allow a FCL to be issued for contractors located outside the U.S., Puerto Rico, or a U.S. possession or trust territory.

b. DOD contractor operations supporting the DA overseas will be required to follow DA regulations, unless applicable international or interagency agreements specify otherwise.

10–2. Disclosure of information to foreign visitors and/or interests

a. Contacts with and disclosure of information to foreign nationals not representing their governments in an official capacity—

(1) DOD and/or DA contractor contact with or disclosure of information to foreign nationals not representing their governments or an international organization in an official capacity is governed by the requirements of the International Traffic in Arms Regulation (ITAR), DOD 5220.22–M, and, where applicable, the Export Administration Regulations (EAR), as well as AR 190–13.

(2) If DA chooses not to sponsor a visit, the affected COR may still choose to allow the visit to proceed. However, in the absence of licensure from appropriate authorities, information disclosure during such a visit must be limited to unclassified information, the release of which is not prohibited under the EAR, ITAR, or other Federal law, regulation or policy, as described in the DOD 5220.22–R. User agency sponsored visits must not be used to avoid the licensing requirements of the ITAR or the EAR.

(3) Any disclosure of classified information by a DA contractor to a foreign visitor must be approved by the appropriate DA official.

b. Contacts with and disclosure of information to representatives of foreign governments and international organizations—

(1) Contacts between U.S. contractors under the cognizance of the DA and representatives of foreign governments and international organizations, as well as the disclosure of information by U.S. contractors to such representatives, is governed by the requirements of the ITAR, DOD 5220.22-M, and, where applicable, the EAR, as well as AR 380–10.

(2) Only visits by representatives of foreign governments and international organizations to U.S. contractors under the cognizance of the DA (whether located on a DA installation or not) that require access to classified or controlled unclassified information should be processed under the Foreign Visits System in accordance with AR 380–10.

(3) A foreign visit request approved by DCS, G–2 is required prior to any contact beyond administrative coordination between U.S. contractors under the cognizance of the DA and representatives of foreign governments or international organizations when the requested visit involves access to classified or controlled unclassified information for which the DA is the originator or proponent.

(4) Alternatively, if DCS, G–2 chooses not to sponsor a visit, the affected COR may still choose to allow the visit to proceed. However, in the absence of licensure from appropriate authorities, information disclosure during such a visit must be limited to unclassified information, the release of which is not prohibited under the EAR, ITAR, or other Federal law, regulation, or policy, as described in the DOD 5220.22–R. User agency sponsored visits must not be used to avoid the licensing requirements of the ITAR or the EAR.

10–3. Foreign visits

All visit requests submitted by or on behalf of a foreign visitor must be processed through the command foreign disclosure office, at least 30 days in advance of the intended arrival date.

Chapter 11
Marking, Handling, and Safeguarding Controlled Unclassified Information

11–1. Technical controlled unclassified information

a. Technical CUI is export controlled and must be marked with the export control warning statement cited in DODD 5230.24 (see AR 380–5).

b. The export control warning statement should be applied to every page of a document, or equivalent in other media, where export controlled classified and/or unclassified information is present.

c. Technical CUI will be handled and safeguarded in the same manner as for official use only information (see AR 380–5 on the standards for safeguarding).

11–2. Security provisions for the safeguarding of technical controlled unclassified information in contracts

a. Appendix B provides an industrial security checklist of security provisions that should be considered for incorporation in Army contracts with contractors for the safeguarding of technical CUI.

b. ISS, in coordination with the KO, will ensure that DA contracts incorporate specific security provisions to ensure

that any involved technical CUI is properly identified, marked, handled, and safeguarded. ISS and KO are responsible for ensuring that any CUI in the deliverables is identified appropriately.

Chapter 12
TEMPEST

12–1. General

TEMPEST is an unclassified short name referring to any action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment or facility that electronically processes information to technical exploitation of classified and/or sensitive information (see AR 380–27 for additional information).

12–2. TEMPEST requirements

a. TEMPEST countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to the national security should the information be intercepted and analyzed by a foreign intelligence organization. It is the responsibility of the GCA to identify in writing what TEMPEST countermeasures may be required. The GCA will identify any TEMPEST requirements within the U.S. to the cognizant security agency for approval prior to imposing requirements for TEMPEST countermeasures on contractors. Prime contractors may not impose TEMPEST countermeasures upon their subcontractors without GCA and cognizant security agency approval.

b. The Government is responsible for performing threat assessment and vulnerability studies when it is determined that classified information may be exposed to TEMPEST collection.

c. Contractors will assist the GCA in conducting threat and vulnerability surveys by providing the following information upon request:

(1) The specific classification and special categories of material to be processed or handled by electronic means.

(2) The specific location where classified processing will be performed.

(3) The name, address, title, and contact information for a point of contact at the facility where processing will occur.

12–3. Limited access authorizations for non-U.S. citizens

Only U.S. citizens are eligible for a security clearance non-U.S. citizens do not qualify for a security clearance. However, if a non-U.S. citizen requires access to U.S. classified information and meets the requirements in DOD 5220. 22–M, a limited access authorization, at no higher than the secret level may be issued. For limited access authorizations on non-U.S. citizens who are not working on cleared contracts, see AR 380–67 for guidance.

Appendix A
References

Section I
Required Publications

AR 190–13
The Army Physical Security Program (Cited in para 10–2*a*(1).)

DOD 5200.2–R
Personnel Security Program (Cited in paras 2–4*a*, 8–2*d*.) (Available at http://www.dtic.mil/whs/directives/.)

DOD 5220.22–R
Industrial Security Regulation (Cited in paras title page, 1–14*a*, 1–15*m*, 1–26*i*, 1–26*j*, 1–27*f*, 1–29*j*, 1–29*m*, 1–32*a*, 1–33*a*, 1–34, 2–1*b*, 2–4*c*, 2–5*a*, 4–1, 5–5*b*, 6–2, 10–2*a*(2), 10–2*b*(4), B–2*d*, and terms.) (Available at http://www.dtic.mil/whs/directives/.)

DOD 5220.22–M
National Industrial Security Program Operating Manual (Cited in paras title page, 1–26*i*, 1–27*f*, 1–29*j*, 1–31*a*, 1–31*b*, 1–32*a*, 2–4*a*, 3–2, 3–3, 3–5*a*, 3–5*b*, 4–1, 5–6*e*, 6–2, 7–1*a*, 7–1*d*, 9–2*b*, 10–2*a*(1), 10–2*b*(1), and B–2*e*.) (Available at http://www.dtic.mil/whs/directives/.)

DODM 5200.01
DOD Information Security Program: Overview, Classification, and Declassification (Cited in paras 5–9, 5–10*a*, 5–10*b*, and terms.) (Available at http://www.dtic.mil/whs/directives/.)

DODI 5220.22
National Industrial Security Program (Cited on the title page.)

EO 12829
National Industrial Security Program (Cited in paras title page, 1–6*b*, 1–10*a*.) (Available at http://www.gpo.gov/fdsys/.)

EO 13526
Classified National Security Information (Cited in paras 1–6*b*, terms.) (Available at http://www.gpo.gov/fdsys/.)

HSPD–12
Policy for a Common Identification Standard for Federal Employees and Contractors (Cited on the title page.) (Available at http://www.dhs.gov/homeland-security-presidential-directive-12.)

Section II
Related Publications
A related publication is a source of additional information. The user does not have to read it to understand this regulation. DOD publications are available at http://www.dtic.mil/whs/directives/.

AFARS
(Available at http://farsite.hill.af.mil/VFAFAR1.HTM.)

AR 11–2
Managers' Internal Control Program

AR 25–2
Information Assurance

AR 25–30
The Army Publishing Program

AR 25–55
The Department of the Army Freedom of Information Act Program

AR 70–31
Standards for Technical Reporting

AR 360–1
The Army Public Affairs Program

AR 380–5
Department of the Army Information Security Program

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives

AR 380–28
Department of the Army Special Security System (U)

AR 380–40
Safeguarding and Controlling Communications Security Material

AR 380–67
Personnel Security Program

AR 380–381
Special Access Programs (SAPs) and Sensitive Activities

AR 381–12
Threat Awareness and Reporting Program

AR 381–20
The Army Counterintelligence Program

AR 525–13
Antiterrorism

AR 530–1
Operations Security (OPSEC)

AR 715–30
Secure Environment Contracting

Army Handbook for SCI Contracts
(Contact DCS, G–2 (DAMI–CDS/Industrial Security Office), 1000 Army Pentagon, Washington, DC 20310–1000.)

DA Pam 5–20
Competitive Sourcing Implementation Instructions

DA Pam 25–30
Consolidated Index of Army Publications and Blank Forms

DA Pam 710–2–1
Using Unit Supply System (Manual Procedures) (Standalone Pub)

DA Pam 710–2–2
Supply Support Activity Supply System: Manual Procedures

DCID 6/7
Intelligence Disclosure Policy (Available at http://www.fas.org/irp/offdocs/dcid.htm.)

DFARS
(Available at http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html.)

DOD 5105.38–M
Security Assistance Management Manual (SAMM)

DODD 5000.01
The Defense Acquisition System

DODD 5105.42
Defense Security Service (DSS)

DODD 5142.01
Assistant Secretary of Defense for Legislative Affairs (ASD(LA))

DODD 5205.02E
DOD Operations Security (OPSEC) Program

DODD 5205.07
Special Access Program (SAP) Policy

DODD 5210.48
Polygraph and Credibility Assessment Program

DODD 8500.01E
Information Assurance (IA)

DODD 8570.01
Information Assurance Training, Certification, and Workforce Management

DODI 5205.08
Access to Classified Cryptographic Information

DODI 5210.02
Access to and Dissemination of Restricted Data and Formerly Restricted Data

DODI 5210.91
Polygraph and Credibility Assessment (PCA) Procedures

DODI 5230.24
Distribution Statements on Technical Documents

DODI 8523.01
Communications Security (COMSEC)

EAR
Export Administration Regulation (15 CFR 730–774) (Available at http://www.bis.doc.gov/policiesandregulations/ear/index.htm).

EO 10865
Safeguarding classified information within industry (Available at http://www.gpo.gov/fdsys/.)

FAR
(Available at https://www.acquisition.gov/far/.)

ICD 704
Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and other Controlled Access Program Information (Available at http://www.dni.gov/electronic_reading_room/ICD%20704.pdf.)

ITAR
Internal Traffic in Arms Regulation (22 CFR 120–130) (Available at http://pmddtc.state.gov/regulations_laws/itar_official.html).

10 USC 2536
Award of certain contracts to entities controlled by a foreign government: prohibition (Available at http://www.law.cornell.edu/uscode/text/10/2536.)

48 USC 1681
Continuance of civil government for Trust Territory of the Pacific Islands; assistance programs; maximum fiscal year costs; reimbursement (Available at http://www.law.cornell.edu/uscode/text/48/1681.)

Section III
Prescribed Forms
This section contains no entries.

Section IV
Referenced Forms
Except where otherwise indicated below, the following forms are available as follows: DA Forms are available on the APD Web site (http://www.apd.army.mil) and DD Forms are available on the Office of the Secretary of Defense Web site (http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm). 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

DD Form 254
Contract Security Classification Specification

DD Form 441
DOD Security Agreement

OFI 79A
Report of Agency Adjudicative Action on OPM Personnel Investigation (Available at http://www.opm.gov/.)

SF 312
Classfied Information Nondisclosure Agreement

SF 328
Certificate Pertaining to Foreign Interests

Appendix B
Industrial Security Checklist

B–1. Information
The following checklist is to be used as a template and may vary for your command. This checklist should be used as a guide.

B–2. Questions
a. Has the command established an ISP?
b. Has the command or activity appointed in writing an ISS?
c. Does the command or activity have the current AR 380–49 (electronic or hard copy)?
d. Does the command or activity have the current DOD 5220.22–R?
e. Does the command or activity have the current DOD 5220.22–M?
f. Does the command or activity have procedures for reviewing and approving DD Form 254?
g. Does the command or activity have procedures for forwarding the signed DD Form 254, subsequent modifications, and the final to DSS?
h. Is the designated ISS signing DD Form 254, block 16?
i. Is the requiring activity and COR listed on DD Form 254, block 13?

j. Is the contracting office or COR distributing the DD Form 254 to DSS and other offices, per block 6c, block 8c, and block 17?

k. Has the command imposed any program protection plans on its contractors via the contract and has a copy of the program protection plan been provided to the contractors as Government furnished inventory?

l. Is the contract being reviewed for CPI?

m. If the contract will contain CPI, are block 10j and block 13–15 annotated when CPI is identified?

n. Has the commanding officer established or coordinated oversight for classified work carried out by cleared contractor employees in spaces controlled or occupied at ACOMs?

o. Does the command KO or COR:

(1) Review, provide contact information and sign on DD Form 254s, block 13?

(2) Validate all contractor security clearances?

(3) Verify contractor storage capability prior to authorizing release of classified information?

(4) Provide additional security requirements via the contract or DD Form 254?

(5) Review all reports of industry security violations and forward to program managers?

(6) Coordinate DD Form 254 reviews and guidance, as needed?

(7) Verify the requirement is listed in the DD Form 254 and cleared contractor employees who are used as couriers have been briefed on their courier responsibilities?

p. Is classified intelligence information disclosed only to those contractors cleared under the NISP and as authorized on the DD Form 254?

q. Are contractor trustworthiness investigations being submitted and adjudicated by the security office for contractor access to IT systems and/or networks?

r. Is the OFI 79A (Report of Agency Adjudicative Action on OPM Personnel Investigation) for non-NISP contractor trustworthiness forwarded to OPM and a copy filed?

s. Are contractors who require access to secure internet protocol router network briefed for North Atlantic Treaty Organization, and the DD Form 254 reflected that the contractor only requires access to secure internet protocol router network and not North Atlantic Treaty Organization documents?

Appendix C
Internal Control Evaluation

C–1. Function

The function covered by this evaluation is the ISP.

C–2. Purpose

The purpose of the evaluation is to assist unit commanders in establishing a functional ISP to ensure that policies and responsibilities are followed when contract performance requires access to classified information.

C–3. Instructions

Answers must be based on testing of the key internal controls such as document analysis, direct observation, and interviewing. Answers that indicate deficiencies must be explained and the corrective action indicated in supporting documentation. Certification that the evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

C–4. Test questions

a. Is an individual appointed to implement and monitor these procedures and oversee these responsibilities of an ISP?

b. Are required publications in this regulation available to individual assigned to oversee industrial security responsibilities? (They do not have to be maintained on hand.)

c. Have personnel been identified to assist KOs prepare DD Form 254 when contract performance requires access to classified information?

d. Are procedures in place to ensure all personnel, including contractors, are aware of the provisions of this publication?

e. Have all personnel involved in the conduct of industrial security execution received formal training in industrial security from the Defense Security Service Center for Development of Security Excellence?

f. Are incidents and security violations involving contractors reported properly in accordance with this publication?

C–5. Supersession
Not applicable.

C–6. Comments
Help make this a better tool for evaluating management controls. Submit comments to Headquarters, Department of the Army, Deputy Chief of Staff, G–2 (DAMI–CDS), 1000 Army Pentagon, Washington, DC 20310–1000.

Glossary

Section I
Abbreviations

ACOM
Army 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

ASD (ISA)
Assistant Secretary of Defense (International Security Affairs)

ASPD
Army Special Programs Directorate

CAC
common access card

CI
counterintelligence

CIO/G–6
Chief Information Officer/G–6

CM
contract monitor

COMSEC
communications security

COR
contracting office representative

CPI
critical program information

CSE
contractor support element

CSM
command security manager

CUI
controlled unclassified information

DA
Department of the Army

DCS, G–1
Deputy Chief of Staff, G–1

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

DCS, G–8
Deputy Chief of Staff, G–8

DCID
Director of Central Intelligence Directive

DISCO
Defense Industrial Security Clearance Office

DOD
Department of Defense

DRU
direct reporting unit

DSS
Defense Security Service

EAR
Export Administration Regulation

EO
Executive Order

FAR
Federal Acquisition Regulation

FCL
facility clearance

FOCI
foreign ownership, control, or influence

GC
General Counsel

HSPD
Homeland Security Presidential Directive

ISP
Industrial Security Program

ISS
industrial security specialist

IT
information technology

ITAR
International Traffic in Arms Regulation

KO
contracting officer

NID
national interest determination

NISP
National Industrial Security Program

OPSEC
operations security

PM
program manager

PEO
program executive officer

PWS
performance work statement

SAP
Special Access Program

SCG
security classification guide

SCI
sensitive compartmented information

SECDEF
Secretary of Defense

SF
standard form

SM
security manager

SME
subject matter expert

SOO
statement of objectives

SOW
statement of work

SSA
special security agreement

STE
secure terminal equipment

TE
technical expert

TJAG
The Judge Advocate General

TSG
The Surgeon General

USD (I)
Under Secretary of Defense for Intelligence

USD (P)
Under Secretary of Defense for Policy

Section II
Terms

Carve-out contracts
Contracts that support Army SAP requirements, which exclude DSS from performing contractor industrial security inspections (see AR 380–381).

Classified contract
Any contract requiring access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified). The requirements prescribed for a "classified contract" also are applicable to all phases of precontract activity, including solicitations (bids, quotations, and proposals), precontract negotiations, post contract activity or other GCA program or project which requires access to classified information by a contractor.

Classified information
Classified information is defined as information and/or material that has been determined, pursuant to EO 13526, as amended, or any predecessor or successor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form.

Cleared facility
A nongovernment owned and operated industrial, educational, commercial, or other facility which DOD has administratively determined to require access to and be eligible for classified information up to and including a certain category (confidential, secret, and top secret).

Cognizant security office
The CSO is the Department of Defense activity responsible for administering the industrial security program on behalf of DOD regarding a particular contractor and/or facility. The SECDEF has designated DSS to perform this function. The Director of DSS has further delegated this responsibility to the DSS regional directors, who provide industrial security administration for DOD contractor facilities located within their respective geographical areas of responsibility. An exception applies to those DOD contractors on Army installations that have been designated as "visitor groups:" security oversight of such contractors is provided by the appropriate command ISS. When used, the language CSO always refers to DSS or an entity thereof.

Critical program information
Elements or components of an Research, Development, and Acquisition Program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. Includes information about applications, capabilities, processes, and end-items. Includes elements or components critical to a military system or network mission effectiveness. Includes technology that would reduce the U.S. technological advantage if it came under foreign control. CPI information will be identified early in the research, technology development and acquisition processes, but no later than when a DOD agency or military component demonstrates an application for the technology in an operational setting, in support of a transition agreement with a pre-systems acquisition or acquisition program, or in exceptional cases, at the discretion of the laboratory and/or technical director. Presystems acquisition and acquisition programs will review their programs for CPI when technologies are transitioned from research and development or inherited from another program, during the technology development phase, throughout program progression, and as directed by the milestone decision authority.

Controlled unclassified information
Unclassified information that does not meet the standard for National Security Classification under EO 13526, but is pertinent to the national interest of the United States or originated by entities outside the U.S. Federal government, and under law or policy requires protection from disclosure, special handling safeguards, and prescribed limits on exchange or dissemination. It includes U.S. information that is determined to be exempt from public disclosure in accordance with AR 70–31 and AR 25–55 or that is subject to export controls in accordance with the International Traffic in Arms regulations or the EARs.

Embedded and/or integrated contractor
Embedded and/or integrated contractors are those who operate out of government-supplied on-base space. An on-base contractor operation, cleared per the NISP or DOD 5220.22–R, which requires access to classified information and operates under the direct oversight of the Army. The embedded and/or integrated contractor is authorized to function in accordance with AR 380–5 and per the VGSA. The Army maintains control of all classified information in this type of contractor operation

Facility (security) clearance
An administrative determination that, from a security viewpoint, a company is eligible for access to classified information at a level up to and including the level of clearance granted

Government contracting activity
An element of an agency designated by the agency head and delegated broad authority regarding acquisition functions.

Industrial security specialist
The ISS is the individual designated in writing by the appropriate commander to be responsible for implementing the installation or unit industrial security program, and for providing oversight of contractors who perform classified contractual activities on Army installations or within activities in order to ensure compliance with governing security regulations.

Integrated visitor groups
An on-base contractor operation cleared per the NISP or the Industrial Security Regulation and requires access to classified information and operates under the direct control/supervision of the Army. The integrated visitor group is authorized to function in accordance with DODM 5200.01 and the VGSA. The Army maintains control of all classified and provides day-to-day supervision over this type of contractor operation. It basically differs from the on-base cleared facility because of its close interaction and/or relationship with the DA organization it supports.

Interim facility security clearances
Interim FCL are temporary, limited company security clearances established by the DSS. An interim FCL does not permit access to restricted data, COMSEC, North Atlantic Treaty Organization, SCI, SAP, or Arms Control and Disarmament Agency classified information. However, if an interim top secret FCL is issued, the contractor may access these categories of information at a level of classification not to exceed secret. Interim FCLs may not be appropriate for all contractual needs and are not available for all sponsored companies.

Intermittent visitor
A contractor or company, cleared per the NISP or DOD 5220.22–R, that require entry to an Army installation for brief periods of time on a scheduled or on call basis to perform contractual duties. An intermittent visitor's presence on an installation usually does not exceed 90 consecutive days.

Invalidation
The temporary suspension of an FCL due to changed conditions or performance which warrant revocation of the FCL in the absence of prompt, appropriate corrective actions.

Trust territory
This term applies only to the trust territory of the Pacific Islands that the U.S. administers under the terms of a trusteeship agreement concluded between this Government and the Security Council of the United Nations pursuant to authority granted by Joint Resolution of Congress, July 18, 1947 (48 USC 1681). According to this agreement, the U.S. has "full power of administration, legislation, and jurisdiction" over the territory; this Government, however, does not claim "sovereignty." Three major archipelagoes make up the trust territory: Carolines (including the Palau Islands), Marshalls, and Marianas (excluding Guam) (see DOD 5220.22–R).

User agency
In accordance with DOD 5220.22–R, this term refers to the OSD (including all boards, councils, staffs, and commands), the DOD agencies, and the Departments of the Army, the Navy, and the Air Force (including all of their activities); the National Aeronautics and Space Administration; the General Services Administration and the Small Business Administration; the National Science Foundation; the Environmental Protection Agency; and the Departments of State, Commerce, Treasury, Transportation, Interior, Agriculture, Labor, and Justice; the U.S. Arms Control and Disarmament Agency, the Federal Emergency Management Agency, the Federal Reserve System; the General Accounting Office; and the U.S. Information Agency.

Visitor Group Security Agreement
A documented and legally binding contractual agreement between a DA activity and a DOD contractor whereby the contractor commits to complying with, rendering or performing specific security tasks or functions for compensation. The VGSA attests to and certifies the existence of such an agreement, including applicable changes and amendments, attachments, supplements and exhibits.

Section III
Special Abbreviations and Terms

CCR
Central Contractor Registration

CSO
cognizant security office

FSO
facility security officer

GCA
Government Contracting Activity

PA
proxy agreement

PCL
personnel security clearance

SCA
security control agreement

VGSA
Visitor Group Security Agreement

VTA
voting trust agreement