

DEPARTMENT OF THE ARMY
US ARMY GARRISON FORT BELVOIR
Fort Belvoir, Virginia 22060-5928

FB Regulation 380-49

26 March 2007

Security
INDUSTRIAL SECURITY PROGRAM

FOR THE COMMANDER:

DISTRIBUTION:
F

BRIAN W. LAURITZEN
Colonel, USA
Installation Commander

OFFICIAL:



JOSEPH PANTELOGLOUS
Adjutant General

History. This is a new regulation.

Summary. The regulation provides policy for protecting classified national security and sensitive unclassified information (regardless of its classification, sensitivity, physical form, media or characteristics) and sensitive government resources entrusted to industry. It assigns responsibility for implementing and managing the Fort Belvoir Industrial Security Program and interfaces with other security program publications to protect the United States national security interests.

Applicability. It is applicable to all active US Army, Fort Belvoir organizations, US Army activities and contractors having government classified contracts and receiving security assistance from the Installation Security and Intelligence Office (ISIO). Assistance is provided in accordance with (IAW) Department of Defense (DoD), Department of the Army (DA), Installation Management Command (IMCOM), and Fort Belvoir directives and currently approved Intra/Inter-Service Support Agreements (ISAs) between the installation and organizations receiving support.

Suggested Improvements. The proponent of this regulation is the US Army Garrison Fort Belvoir, Directorate of Plans, Training, Mobilization and Security (DPTMS), Fort Belvoir, VA. Users should send comments and suggested improvements on DA Form 2028, Recommended Changes to Publications and Blank Forms, to the Directorate of Plans, Training, Mobilization and Security, 9820 Flagler Road, Fort Belvoir, VA 22060-5929.

TABLE OF CONTENTS

	Paragraph	Page
Chapter 1		
General		
Purpose	1	3
References	2	3
Proponent	3	3
Chapter 2		
Responsibilities		
Installation Commander	1	3
Director DPTMS	2	3
Installation Security Manager	3	3
Garrison staff and Directors	4	4
Tenants organizations	5	5
Contractors	6	6
Facility Security Clearance	7	6
Exception Policy	8	6
Points of Contact	9	6
Chapter 3		
Procedures		
Security Compromise	1	6
Security Investigation	2	6
DD Forms 254	3	6
Appendix A		
References		A-1
Appendix B		
Abbreviations and Acronyms		B-1
Appendix C		
Terms		C-1
Appendix D		
Appointment Memorandum		D-1
Appendix E		
FB Industrial Security Program Checklist		E-1
Appendix F		
Industrial Security DD Forms 254 Guide		F-1

Chapter 1 General

1. Purpose. The security of Fort Belvoir and the United States depends in part upon proper safeguarding of the classified information released to industry. The purpose of this document is to set forth the Fort Belvoir policies, practices and procedures to ensure maximum effectiveness and consistency with applicable directives and regulations.
2. References. Required publications are listed in Appendix A.
3. Proponent. Directorate of Plans, Training, Mobilization and Security (DPTMS), Installation Security Manager (ISM), (703) 805-4012. No modifications may be made to this document except in coordination with DPTMS, ISIO.

Chapter 2 Responsibilities

1. The Installation Commander (IC) will:
 - a. Designate the ISM as the authority to perform Industrial Security Program oversight for on-installation contractor operations.
 - b. Oversee the implementation of the guidelines prescribed in the Department of Defense Regulations/Manuals, Department of Army Regulations, Installation Management Command, and local directives governing the Installation Industrial Security program.
2. The Director, DPTMS will:
 - a. Monitor the Industrial Security Program for the Installation.
 - b. Keep the Commander informed on the status of the Installation Industrial Security Program and serve as the Commander's executive agent for coordination of all issues concerning the program with internal and external agencies.
3. The Installation Security Manager (ISM) will:
 - a. Act with the authority of the IC in overseeing and administering the Installation Industrial Security Program (IISP).
 - b. Provide program oversight IAW the guidelines prescribed in the Department of Defense Regulations/Manuals, Department of Army Regulations, Installation Management Command, and local directives governing the IISP.

c. Maintain a database of Garrison staff and tenant organizations who issue classified contracts, Department of Defense Contract Security Classification Specification, DD Forms 254.

d. Review pre-award documentation to ensure appropriate security clauses and language are contained therein and address the protection of government information and resources.

e. Coordinate contractor requests for information with the Contracting Officer Representative (COR) prior to release of information.

f. Ensure DD Forms 254 are generated by Garrison staff and tenant organizations for contractors who have access to classified information per classified contracts and contain adequate classification guidance. Conduct biannual review of DD Forms 254.

g. Ensure contractors provide clearance verification for all employees performing work associated with a classified contract.

h. Conduct annual reviews of Garrison staff and tenant organizations that issue classified contracts and do not have a certified industrial security program.

i. Ensure all contractor activities are knowledgeable of their training requirements as defined in DoD Regulation 5220.22 R, Industrial Security Regulation; DoD 5220.22-M, National Industrial Security Program Operating Manual, and DoD 5220.22-M-Sup 1, Industrial Security Program Operating Manual Supplement. Records of training, briefings, debriefings, access, and access termination must be maintained IAW the applicable directives.

j. Provide agencies and organizations having classified contracts a CD containing the Fort Belvoir Industrial Security Program (Access database) for maintaining contractor data identified in this regulation.

4. Garrison staff and Directors will:

a. Appoint a primary and alternate representative in writing to serve as points of contact (POCs) when establishing a classified contract. POCs coordinate and act on Industrial Security matters. Appointments should be updated annually and/or upon changes in appointment.

b. Ensure all DD Forms 254 prepared are forwarded through the ISIO to validate compliance with the installation Industrial and Information Security programs and in turn are forwarded to the appropriate approval authority.

c. Inform the ISM immediately of any possible security violations or changes to the contract(s)/DD Form 254. During duty hours notify the ISO at 805-4012/2416/2817, after normal duty hours, for emergencies, notify the ISM through the Installation Staff Duty Officer at (703) 304-7258. All violations will be handled IAW Chapter 10 of AR 380-5.

d. Maintain for the current and previous two fiscal years (three years total) a database for investigation and inspection purposes. Include all contractor names, contract numbers, dates and status of contracts, cage codes, and DD Forms 254.

e. Maintain for the current and previous two fiscal years (three years total) a database for investigation and inspection purposes. Include all visit requests for contractors who have/had access to classified information per classified contracts.

f. Provide required annual training as defined in the Installation Security Training Program for all government program managers. Maintain a database for the current and previous fiscal year's (two years total) annual training. As a minimum, it must include the trainee's name, type of training, and date completed.

5. Tenant organizations will:

a. Appoint a primary and alternate person to serve as the Industrial Security points of contact (POCs) for their organization/activity. The POCs coordinate and act on Industrial Security matters.

b. Ensure all DD Forms 254 prepared are forwarded through the ISIO to validate compliance with the Fort Belvoir Industrial and Information Security Programs and in turn are forwarded to the appropriate approval authority.

c. Inform the ISM immediately of any possible security violations or changes to the contract/DD Form 254. If during duty hours, notify the ISO at 805-4012/2416/2817, after duty hours, for emergencies, notify the ISM through the Installation Staff Duty Officer at (703) 304-7258. All violations will be handled IAW Chapter 10 of AR 380-5.

d. Maintain for the current and previous two fiscal years (three years total) a database for investigation and inspection purposes. Include all contractor names, contract numbers, dates and status of contracts, cage codes, and DD Forms 254.

e. Maintain for the current and previous two fiscal years (three years total) a database for investigation and inspection purposes. Include all visit requests for contractors who have/had access to classified information per classified contracts.

f. Provide required annual training as defined in governing directives for all government program managers. Maintain a database for the current and previous fiscal year's (two years total) annual training. As a minimum, it must include the trainee's name, type of training, and date completed.

6. Contractors. IAW their applicable statement of work (SOW), contractors will maintain the prerequisite security clearance(s). Any lapse(s) to a security clearance(s) or events that may change the status of a clearance(s) will be reported to the ISIO. If during duty hours, notify the ISIO at 805-4012/2416/2817, after duty hours, for emergencies, notify the ISM through the Installation Staff Duty Officer at (703) 304-7258. All violations will be handled IAW Chapter 10 of AR 380-5.

7. Facility Security Clearance. The Installation Commander determines if a contractor on the installation requires a Facility Security Clearance (FCL), the Commander can either retain security cognizance or request that Defense Security Service (DSS) do so. Reference DoD 5220.22 R, Industrial Security Regulation and Army Regulation 380-49.

a. If the Installation Commander retains security cognizance, the Commander is responsible for all aspects of the contractor's operations.

b. If DSS accepts security cognizance, then DSS is responsible. Responsibility cannot be split between the Installation Commander and DSS.

8. Exemption Policy. Tenant organizations having a certified Industrial Security Program may request exemption from Fort Belvoir oversight by submitting a memorandum from their major area command indicating oversight and certification of their program.

9. Point of Contact (POC). All Garrison Staff and tenant organizations on Fort Belvoir having responsibility to the Installation Industrial Security Program will appoint a primary and alternate POC. Initial submissions are requested by memorandum, reviewed annually, and updates provided when there are changes in appointed personnel.

Chapter 3 Procedures

1. Security Compromise/suspected compromise. The Installation Security Manager (ISM) will be notified during normal duty hours at (703) 805-4012/2416/2817 in the event of an actual or suspected security compromise. During non-duty hours, for emergencies, the ISM must be contacted through the Installation Staff Duty Officer at (703) 304-7258.

2. Security Investigation. Preliminary investigation reports involving an actual/suspected security compromise will be staffed by the organization Security Manager (SM) IAW the guidance contained in DoD, DA, IMCOM, NERO directives and this regulation. The SM will copy furnish the ISM all correspondence, notifications and reports pertinent to violations, compromises, or suspected compromise investigations.

3. DD Forms 254. Garrison and tenant organizations with classified contracts will provide copies of all Department of Defense Forms 254 (DD 254s), including changes, to the ISIO, Headquarters building #269, Room 017.

Appendix A
References

Section I
Required Publications

Executive Order 12829, National Industrial Security Program, 6 Jan 93.

Executive Order 12958, Classified National Security Information, 17 Apr 95.

Executive Order 13292, Amendment to Executive Order 12958, 25 Mar 03.

DoD Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, 16 Jun 92.

DoD 5200.1-R, Information Security Program, Jan 97.

DoD 5220.22-R, Industrial Security Program, 4 Dec 85.

DoD 5220.22-C, Carrier Supplement to Industrial Security Manual for Safeguarding Classified Information, Oct 86.

DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), 28 Feb 06.

AR 380-5, Department of the Army Information Security Program, 29 Sep 00.

AR 380-10, Foreign Disclosure and Contracts with Foreign Representatives, 22 Jun 05.

AR 380-49, Industrial Security Program, 15 Apr 82.

AR 380-67, Department of the Army Personnel Security Program, 9 Sep 88.

Section II
Prescribed Forms

DD Form 254, DoD Contract Security Classification Specification.

DD Form 441, DoD Security Agreement.

DD Form 441-1, Appendage to Department of Defense Security Agreement.

DD Form 2875, System Authorization Access Requirements.

SF Form 328, Certificate Pertaining to Foreign Interests.

Appendix B
Abbreviations and Acronyms

ACO - Administrative Contracting Officer
 AIS - Automated Information System
 COMSEC - Communications Security
 CO - Contracting Officer
 COR - Contracting Officer Representative
 CSO - Cognizant Security Office
 DOD - Department of Defense
 DPTMS - Directorate of Plans, Training, Mobilization, and Security
 DRU - Direct Reporting Unit
 DSS - Defense Security Service
 DSS-OCC - Defense Security Service - Operating Center Columbus
 FAR - Federal Acquisition Regulation
 FBI - Federal Bureau of Investigations
 FCL - Facility Security Clearance
 FOA - Field Operating Agency
 FOCI - Foreign Ownership, Controlled, or Influenced
 HOF - Home Office Facility
 IC - Installation Commander
 IPR - Inprocess Program Review
 IISP - Installation Industrial Security Program
 ISIO - Installation Security and Intelligence Office
 ISM - Installation Security Manager
 MACOM - Major Command
 NISP - National Industrial Security Program
 OPR - Office of Primary Responsibility
 OPSEC - Operations Security
 PCL - Personnel Security Clearance
 PCO - Procuring Contracting Officer
 PM - Program Manager
 POC - Point of Contact
 RFB - Request for Bid
 RFP - Request for Proposal
 RFQ - Request for Quote
 SAP - Special Access Program
 SAV - Staff Assistance Visit
 SCI - Sensitive Compartmented Information
 SM - Security Manager
 SOO - Statement of Objectives
 SOW - Statement of Work
 VGSA - Visitor Group Security Agreement

Appendix C

Terms

Classified Contract - Any contract that requires or will require access to classified information by the contractor or the employees in the performance of the contract. A contract may be classified even though the contract document itself is not classified.

Cleared Facility - A non-government owned and operated industrial, educational, commercial, or other facility for which DoD has made an administrative determination (from a security viewpoint) that the entity is eligible for and requires access to classified information of a certain category (Confidential, Secret, or Top Secret).

Cognizant Security Office - The designated Department of Defense (DoD) agency responsible for Industrial Security program administration. The Secretary of Defense (SECDEF) has designated the Defense Security Service (DSS) to perform this function. The Director of DSS has further delegated this responsibility downward within the agency. DSS Regional Directors provide industrial security administration for DoD contractor facilities located within their respective geographical area. One exception, for which ISM has responsibility, is DoD contractors on Army installations who have been designated as "visitor groups." When used, the language "Cognizant Security Office" (CSO), always refers to DSS or an entity thereof.

Installation - An area in which the Army holds a real property interest or real property over which the Army has jurisdiction by agreement or by right of occupancy. The term installation also includes all auxiliary off-base or detached installations under the jurisdiction of the commander of the primary installation.

Installation Security Manager (ISM) - This DA entity implements and administers the installation's information, personnel and industrial security programs. The ISM is responsible for supervising and overseeing on-base contractor's security programs and/or operations.

Integrated Visitor Groups - An on-base contractor operation, cleared per the NISP or ISR, that 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 DOD 5200.1-R 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) - Interim FCLs are temporary, limited company security clearances established by the DSS. It does not permit access to Restricted Data, COMSEC, North Atlantic Treaty Organization (NATO), SCI, SAP, or Arms Control and Disarmament Agency classified Information. However, if an interim Top Secret FCL is issued, the contractor may access such information at the level of Secret and Confidential. Interim FCLs may not be appropriate for all contractual needs and are not available for all sponsored companies.

Appendix C **Terms**

Intermittent Visitor - A contractor or company, cleared per the NISP or ISR, that requires “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 - A condition at a cleared facility caused by changed conditions or performance under which the facility may no longer be eligible for an FCL unless the facility promptly initiates appropriate corrective actions.

Major Discrepancy - A condition, which resulted in or could reasonably be, expected to result in the loss or compromise of classified information.

On-Base Cleared Facility - An on-base contractor operation cleared under the provisions of the NISP and established at the discretion of the IC per DOD 5220.22-R. These entities operate under NISPOM guidance and the ISM has been designated by the IC to provide security oversight.

Reciprocity - A reciprocal condition, relationship, mutual or cooperative agreement, between two or more agencies, components, or departments agreeing to recognize and accept the efforts (requirements, procedures, actions, etc.) of the other in exchange for the same compensation.

Visitor Group - Any on-base contractor operation, cleared per the NISP or ISR, that requires access to classified information. The installation commander determines their “official” on-base designation.

(NOTE: All on-base contractor operations are considered “visitor groups,” per this directive. The IC assesses and evaluates the working relationship and interactions between the visitor group and DA activity to determine their “official” designation, i.e., cleared facility, integrated visitor group or intermittent visitor).

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.

Appendix D
Appointment Memorandum

ORGANIZATION LETTERHEAD

Office Symbol

Date

MEMORANDUM FOR the Installation Security Manager

SUBJECT: Letter of Appointment

1. The following personnel are hereby appointed as the responsible agents for the organization Industrial Security Program.

<u>Name</u>	<u>Office Symbol</u>	<u>E-mail Address</u>	<u>Phone</u>	<u>Sample Signature</u>
-------------	----------------------	-----------------------	--------------	-------------------------

Primary

Alternate

2. Point of contact for this memorandum is _____ at (000) 000-0000. Appointments will be reviewed annually and or updates provided upon changes in personnel.

Organization Commander
Signature Block

Appendix E
FB Industrial Security Program Checklist

Purpose: This checklist is provided as a guide for development and review of the Installation Industrial Security Program (IISP). It should be used in conjunction with Department of Defense (DoD), Department of the Army (DA), Defense Security Service (DSS), Installation Management Command (IMCOM), and local directives in conducting development and program reviews.

Section I: Establishing An Industrial Security Program			SAT	UNSAT	N/A	REMARKS
1.1	Critical	Has the installation commander (IC) designated the Installation Security Manager (ISM) as the servicing security activity for industrial security and authority for oversight of on-base contractor operations?				
1.2	Critical	Is the ISM administering the Industrial Security Program and coordinating with the contracting office (CO), Cognizant Security Office (CSO), and other installation security discipline OPRs?				
1.3	Critical	Are procedures in place to integrate on-base contractor's operations into the installation's information security program? Proof – i.e. training rosters				
1.4	Non-Critical	If the Installation Commander desires the Defense Security Service (DSS) security oversight for on-base contractor facilities, has a request been forwarded to DSS?				

Section 2: Security Reviews and Host Security Agreements			SAT	UNSAT	N/A	REMARKS
2.1	Critical	Does the ISM review solicitation and contract documents to ensure they include appropriate security clauses or language and address the protection of government information and sensitive resources? (Check Block 13 of DD 254)				
2.2	Critical	Does the ISM conduct security reviews of on-base cleared facilities IAW contract specific security requirements and pertinent DoD and DA security instructions?				

Appendix E
FB Industrial Security Program Checklist

Section 2: Security Reviews and Host Security Agreements			SAT	UNSAT	N/A	REMARKS
2.3	Critical	Does the ISM have procedures in place to ensure contractor security violations and compromises are reported and resolved promptly? <u>Must be shown in the Visitor Group Security Agreement (VGSA) .</u>				
2.4	Non-Critical	If the Installation Commander is conducting security reviews of on-base cleared facilities (using a designated ISM) has DSS been notified of this decision?				
2.5	Critical	When DSS is relieved of security oversight responsibility for visitor groups on the installation, is this indicated on the DD Form 254? <u>Check in Block 15, 14, or 13</u>				
2.6	Non-Critical	Is DSS provided with facility surveys, security review reports and other related contract security documents?				

Section 3: Scheduling Inspections/Staff Assistance Visits/Reviews			SAT	UNSAT	N/A	REMARKS
3.1	Critical	Is the ISM inspecting cleared facilities according to frequency schedules established by DoD and providing the cleared facility or visitor group management 30 days advanced written notification with the exception of conducting unannounced security reviews?				
3.2	Non-Critical	Is the ISM inspecting Visitor Groups according to frequency schedules established in DoD 5200.1-R? <u>Information Security Program/Should be checked when IPR is conducted – Check to see if IPR is on record</u>				

Section 4: Oversight Reviews And Reporting			SAT	UNSAT	N/A	REMARKS
4.1	Critical	Do Facility Security Clearance (FCL) files contain all key documentation including DD Form 254, Contract Security Classification Specification, and related documents?				

Appendix E
FB Industrial Security Program Checklist

Section 4: Oversight Reviews And Reporting			SAT	UNSAT	N/A	REMARKS
4.2		Does the ISM, unit security manager, and integrated visitor group establish files and maintain all documentation?	--	--	--	--
Within the contract folder is the ISM maintaining: (Self explanatory)						
4.2.1	Critical	Signed copies of DD 254s and any revisions? Block 16e				
4.2.2	Critical	Signed copies of VGSA's?				
4.2.3	Critical	Current listing of key on-base management officials or representative?				
4.2.4	Critical	Copy of last annual program review?				
4.2.5	Critical	Copies of last two self-inspections or last self-inspection and annual program review? <u>IPR may be used as one of self-inspections</u>				
4.2.6	Critical	Copies of contractor's visit authorization letters (VAL)? <u>(1) Check expiration dates</u> <u>(2) Required for all contractors</u> <u>(3) Check for contract number</u> <u>(4) Check for cage code</u>				
4.3	Critical	Does the ISM keep copies of completed security review reports, pre-inspection visit memos and completed post-inspection correspondence for 2 years from date of the most recent inspection? <u>Check for past IPRs/self-inspections, and Corrective Action Reports</u>				
4.4	Non-Critical	Does the ISM send a letter to the senior management official of on-base cleared facilities within 10 days following a security review confirming contractor security status and deficiencies requiring corrective action and addressing the following: (4.4.1, 4.4.2, and 4.4.3)?				

Appendix E
FB Industrial Security Program Checklist

Section 4: Oversight Reviews And Reporting			SAT	UNSAT	N/A	REMARKS
4.4.1	Non-Critical	Confirming contractor's security status as discussed during the exit review?				
4.4.2	Non-Critical	Listing any deficiencies requiring corrective action?				
4.4.3	Non-Critical	Requesting written confirmation on the status of any open major discrepancy within 30 days?				

Section 5: Reviewing Visitor Groups – applies only to on-base contracts			SAT	UNSAT	N/A	REMARKS
5.1	Non-Critical	For Visitor Groups operating under DoD 5200.1-R, Information Security Program requirements: does the activity limit the Visitor Group's access to "need to know" contract-specific performance information only? <u>Must have a "need to know" statement in the VGSA - if they have a VGSA package then you MAY assume this exists</u>				
5.2	Non-Critical	Does the Visitor Group Security Agreement clearly reflect DA is accountable for and controls all classified information? <u>Must have a "accountability" statement in the VGSA - if they have a VGSA package then you MAY assume this exists</u>				
5.3	Non-Critical	Do visitor groups operating under the Information Security Program use approved government information systems or networks to process classified information? <u>If a Contractor has its own classified AIS it must have DA approval – request to see document</u>				

Appendix E
FB Industrial Security Program Checklist

Section 5: Reviewing Visitor Groups – applies only to on-base contracts			SAT	UNSAT	N/A	REMARKS
5.4	Critical	Has the installation commander or designee executed Visitor Group Security Agreements with all contractors located on the installation that require access to classified information? <u>If DD Form 254 lists FB in block 8a there must be a VGSA</u>				
5.5	Critical	Do visitor group security agreements (VGSA) stipulate specific security requirements and procedures unique to the installation that are applicable to individual visitor groups specific? (DoD 5220.22-R) <u>Are there references to specific requirements for FB in VGSA - if they have a VGSA package then you can assume this exists</u>				
5.6	Critical	Are all subcontractors covered by either separate VGSA's with the installation or included by attachment to a prime contractor's VGSA? <u>Is there a document that stipulates that the subcontractor must comply to the terms of the prime contractor's VGSA</u>				
5.7	Critical	Do VGSA's delineate contractor responsibilities for reporting security violations? <u>Must have a "security violation reporting" statement in VGSA - if they have a VGSA package then you can assume this exists</u>				

Section 6: Unsatisfactory Review <i>(Applies to on-base Cleared Facility Only)</i>			SAT	UNSAT	N/A	REMARKS
6.1		The ISM assigned an unsatisfactory rating to 6.1.1, 6.1.2, or 6.1.3 <u>(If this has occurred, is there documentation to this effect? Otherwise it is N/A)</u>	--	--	--	--

Appendix E
FB Industrial Security Program Checklist

Section 6: Unsatisfactory Review <i>(Applies to on-base Cleared Facility Only)</i>			SAT	UNSAT	N/A	REMARKS
6.1.1	Critical	A cleared facility/visitor group fails to satisfactorily perform its contractual security responsibilities? <u>The ISM normally assigns an unsatisfactory Security Review rating.</u>				
6.1.2	Critical	Major failures in the contractor security program have resulted in or could reasonably be expected to result in the loss or compromise of classified information?				
6.1.3	Critical	The contractor is clearly responsible for the security problems cited during a periodic security review?				
6.2	Critical	Does the ISM have procedures for coordinating with the CSO and base-contracting officer when assigning an unsatisfactory security review rating/ security violation/compromise?				
6.3	Critical	When assigning an unsatisfactory rating, is the ISM notifying the HOF through the contracting office requesting prompt and complete corrective action?				

Section 7: Contracts			SAT	UNSAT	N/A	REMARKS
7.1	Critical	Does the ISM maintain a contract folder for each cleared facility or visitor group over which the installation commander has security cognizance? <u>Applies to VGSA only at FB</u>				
7.2	Critical	Do contracts written by installation contracting officers include the requirement to enter into a VGSA with the installation commander? (DoD 5220.22-R) <u>Check Block 8a of DD Form 254 for FB entry</u>				

Appendix E
FB Industrial Security Program Checklist

Section 7: Contracts			SAT	UNSAT	N/A	REMARKS
7.3	Critical	Does the ISM conduct security reviews for supported on-base cleared facilities IAW contract specific security requirements and DoD and DA security instructions.?				

Section 8: DD Form 254			SAT	UNSAT	N/A	REMARKS
8.1	Critical	Is the ISM reviewing draft DD Forms 254 and draft security classifications ensuring they are identified by title and date? <u>Does block 13 contain the ISM signature? - If prior to 2002 signature not required in Block 13</u>				
8.2	Non-Critical	When DSS is no longer responsible for security oversight of cleared facilities involved in SCI or SAPs, is a copy of DD Form 254 sent to HQ DSS?				
8.3	Non-Critical	Are all known contract performance locations specified on the DD Form 254 and are copies of applicable DD Forms 254 forwarded to the ISM at each performance location? <u>Check Block 8a, Contractor facilities must have blocks (a, b & c) filled in - Military facility only block (a)</u>				

Section 9: Reviewing and Certifying DD Form 254			SAT	UNSAT	N/A	REMARKS
9.1	Critical	Is the ISM reviewing the DD Form 254 to ensure the security classification guidance is accurate, approved, and appropriate? Check first paragraph in block 13 for statements referring to the NISPOM.				
9.2	Critical	Are DD Forms 254 coordinated through all security related OPRs (COMSEC, EMSEC, foreign disclosure, etc.)? <u>Spot check to see if a box in blocks 10 or 11 is checked that it is addressed on the DD 254 in block 13 or as an attachment</u>				

Appendix E
FB Industrial Security Program Checklist

Section 9: Reviewing and Certifying DD Form 254			SAT	UNSAT	N/A	REMARKS
9.3	Critical	Does the ISM ensure DD Forms 254 show that the required facility clearance is at an equivalent or higher level than access required for performance of contracts? <u>Block 1b cannot be a higher classification level than 1a</u>				
9.4	Critical	Are the DD Forms 254 certified by contracting officers? <u>Is the ISM's copy of the DD 254 signed in block 16e/a?</u>				
9.5	Critical	Is the ISM seeing that the program is reviewing all pertinent DD 254s and applicable security guides every two years? <u>IPRs review DD Form 254 for accuracy but applicability is subjective call</u>				

Section 10: Visits			SAT	UNSAT	N/A	REMARKS
10.1	Critical	Do DA personnel who require access to classified information while visiting contractor facilities comply with the provisions of DoD 5200.1-R and the National Industrial Security Program Operating Manual (NISPOM)? <u>Are visit requests being sent to contractor facilities? Don't need to see the actual visit request</u>				
10.2	Critical	Are visit authorization request procedures reviewed during security reviews of on-base contractor operations or included in host unit self-inspections? <u>This is accomplished thru the IPR - Spot check a few VALs to ensure complete.</u>				

Appendix E
FB Industrial Security Program Checklist

Section 10: Visits			SAT	UNSAT	N/A	REMARKS
10.3	Critical	Do contractor visit authorization letters (VAL) include the required information to include: 1) Name, address, telephone #, CAGE code, level of facility security clearance; 2) DOB/POB, citizenship; 3) Visitor(s)' clearance level; 4) POC being visited; 5) Date or period of visit; 6) Purpose? <u>(Can just be a listing of the contract number)</u> DoD 5220.22M) <u>Spot check</u>				

Section 11: Facility Clearance			SAT	UNSAT	N/A	REMARKS
11.1	Critical	When requesting an interim Top Secret Facility Clearance (FCL), do contracting officers prepare and route FCL sponsorships through command channels to the MACOM, FOA, or DRU commander for approval and do these requests include the following? <u>Do you have any new contractors that you are sponsoring?</u> <u>IF NO skip, If applicable, documentation is required</u>				
11.2	Non-Critical	An explanation why an interim Top Secret FCL would prevent a crucial delay in the award or performance of a classified contract? <u>If applicable, documentation is required</u>				
11.3	Non-Critical	A list giving the legal name of the facility seeking sponsorship, its complete street address, and the names and positions of people who are applying for interim Top Secret authorization? <u>If applicable, documentation is required</u>				

Appendix E
FB Industrial Security Program Checklist

Section 11: Facility Clearance			SAT	UNSAT	N/A	REMARKS
11.4	Non-Critical	The address of the authorizing DSS? <i>If applicable documentation is required</i>				
11.5	Non-Critical	Is the ISM conducting surveys and administrative inquiries of the FCL as requested by the CSO, and ensuring contractor compliance with the NISPOM? (Applies to clear facilities only)				
11.6	Non-Critical	Does the ISM complete the FCL survey and is a copy provided to the CSO? <i>Applies only to a cleared facility</i>				
11.7	Non-Critical	Is the CSO notifying contracting officers in writing when the FCL of a contractor is invalidated? <i>(If applicable, documentation is required)</i>				
11.8	Non-Critical	Are procedures in place to notify CSOs and program managers of possible invalidation or revocation of facility clearances as the result of Foreign Ownership Control or Influence (FOCI)?				
11.9	Non-Critical	Are on-site/on-base contractors following the NISPOM, DoD, and DA instructions when reporting the loss, compromise, and possible compromise of classified materials? <i>As contractor personnel on FB integrated into units, they must comply with using DA reporting procedures -covered in VGSA</i>				
11.10	Non-Critical	Does the installation commander follow the instructions by DoD 5220.22-R, <i>Industrial Security Regulation</i> , to report the loss, compromise, or possible compromise of classified information for on-base contractor operations for which DA has security oversight?				

Appendix E
FB Industrial Security Program Checklist

Section 11: Facility Clearance			SAT	UNSAT	N/A	REMARKS
11.11	Non-Critical	Are the DA activity, CSO and the contractor notified of decisions to declassify, downgrade, or retain the security classification of the affected material? <u>If applicable, documentation is required</u>				
11.12	Non-Critical	Does the ISM report cases of espionage or sabotage involving visitor groups or cleared facilities to the serving MI? <u>What would you do if you ran across this?</u>				
11.13	Non-Critical	If a contractor requests permission to submit a request to disclose classified information to a foreign interest, is the request forwarded through command channels <u>IAW DoD Directive 5230.11, Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations?</u> <u>Do your contractors coordinate through the Program Office for foreign release of information? If YES show foreign disclosure worksheet</u>				

Section 12: Integration/Training			SAT	UNSAT	N/A	REMARKS
12.1	Non-Critical	Are visitor groups included in the host activity's self-inspections? (FB Regulation 1-201) <u>Are contractor personnel available for interview during IPR?</u>				
12.2	Critical	Are procedures in place to ensure on-base contractors receive required security education, training and briefings? (DoD 5220.22-R); DoD 5220.22-M (NISPOM), chapter 3; and subparagraphs) <u>Training rosters</u>				

Appendix E
FB Industrial Security Program Checklist

Section 12: Integration/Training			SAT	UNSAT	N/A	REMARKS
12.3	Critical	Are individual security requirements and responsibilities concerning the Industrial Security Program included in security training for government personnel as appropriate? <u>Does training syllabus, newsletters, etc. include information /personnel/industrial security?</u>				

Section 13: Automated Information Systems (AIS)			SAT	UNSAT	N/A	REMARKS
13.1	Critical	Is automated information system (AIS) accreditation for on-base cleared facilities coordinated through the responsible installation OPRs (computer security, COMSEC, etc.) and the ISM?				
13.2	Critical	Do all contractor employees who require access to unclassified government information systems have the required personnel security investigations and trustworthiness determinations by an authorized government official? <u>Is there a DD Form 2875 System Authorization Access Requirements on record for each contractor with access to Gov't AIS?</u>				
13.3	Critical	Do contractors who require access to classified information systems have the necessary security clearances? <u>Check Visit Authorization Letter from contractor's home office</u>				

Appendix E
FB Industrial Security Program Checklist

Notes:

Items to check in DD Forms 254 review:

All DD 254s must be reviewed. The following points should be checked at a minimum:

1. Block 1: (b) can never be higher than (a)
2. Block 3a must have a date
3. If block 6a is filled in, so must be 6b & 6c
4. If block 7a is filled in, so must be 7b & 7c
5. If block 8a is filled in, so must be 8b & 8c if 8a is a commercial location
6. If block 8a is filled in with a military location, 8b and 8c are blank but a release statement of oversight responsibility by DSS must be included in block 13/14/15.
7. Some sort of security guidance is evident in block 13 (amplification may be found in attachments)
8. ISM signature block is signed (after 2002)
9. If coordinated thru IN, IN signature block is signed (after 2002)
10. Signature in Block 16

Notes:

List of all DD Forms 254 reviewed:

	<u>CONTRACT NUMBER</u>	<u>COMPANY NAME</u>
1		
2		
3		
4		
5		
6		
7		
8		
9		

Include additional page(s) as required

Appendix F
Industrial Security DD Forms 254 Guide

The DD Form 254 Guide for form preparation is available at
<http://www.dss.mil/training/pub.htm>