DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

AFI 16-1406_AFGM2019-01
24 October 2019

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/AA
1720 Air Force Pentagon
Washington, DC 2033-16655

SUBJECT: Air Force Guidance Memorandum, AFI 16-1406, *Air Force Industrial Security Program*

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum (AFGM) immediately changes AFI 16-1406, *Air Force Industrial Security Program*. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other publications, the information herein prevails in accordance with AFI 33-360, *Publications and Forms Management*. On August 3, 2017, a joint signature memorandum was released by the Secretary of the Air Force and Chief of Staff of the Air Force, Subject: Air Force Directive Publication Reduction. This AFGM provides changes aligned with Air Force leadership's intent to review existing publications, eliminate unnecessary publications, and revise publications where necessary to allow commanders to exercise good judgment and waive requirements to the lowest appropriate level. This AFGM removes the restriction on delegation of certification for the DD Form 254, *Department of Defense Contract Security Classification Specification*.

In addition, this AFGM requires the use of the DD Form 254 Instructions, *Instructions for Completing DD Form 254, Department of Defense Contract Security Classification Specification*, mandates the use of the Enterprise Protection Risk Management (EPRM) Tool to record and analyze key elements of program self-inspections, and clarifies and corrects minor administrative errors in previous versions of the AFI.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon incorporation by interim change to, or rewrite of AFI 16-1406, whichever is earlier**.**

ANTHONY P. REARDON
Administrative Assistant

Attachment

AFI16-1406_AFGM2019-01

1.6.2. (REVISED) Installation commanders categorize on-site contractors as visitor groups, intermittent visitors, or cleared facilities. **(T-0).** Visitor groups can:

1.6.2.1. (ADDED) Operate under day-to-day oversight of an Air Force activity. In these cases, the Commander/Director will integrate contractor employees into their Information Security Program. **(T-0).** These contractor employees typically sit in the same work-space as government employees where an Air Force official is responsible for the security requirements of the space. Contractors who operate as an integrated visitor group remain subject to this AFI and AFI 16-1404 and must provide an on-site security point of contact to the Information Protection Office.

1.6.2.2. (ADDED) Operate independently from an on-base Air Force activity. In these cases, the contractor employees operate independently from day-to-day oversight by Air Force employees and typically have a separately assigned space for which they are responsible as described in Memoranda of Agreement, Support Agreements, etc. Further, contractors are normally only categorized this way when their contract requires them to store classified information and they do so separately from other Air Force operations. Contractors who operate as an independent visitor group remain subject to this AFI and AFI 16-1404 and must provide an on-site security point of contact to the Information Protection Office. **(T-0).**

1.6.2.3. (ADDED) Contractors that cannot be categorized as cleared facilities or visitor groups will be categorized as intermittent visitors. **(T-0).** See paragraph 4.1. of this AFI for additional guidance.

1.6.3. (REVISED) Installation commanders who elect to request a facility clearance for an on-base contractor activity in lieu of processing the contractor as a visitor group or intermittent visitor shall follow the guidance in DoDM 5220.22, Volume 2, National *Industrial Security Program: Industrial Security Procedures for Government Activities,* paragraph 3.8. to request facility clearance establishment from the Defense Security Service (DSS). **(T-0).** The request shall identify whether the Air Force will retain oversight or whether DSS is requested to provide cleared facility oversight. **(T-0).** Provide a copy of the request and final determination through MAJCOM/DRU Information Protection channels to SAF/AAZ. **(T-1).**

1.6.3.1. (ADDED) When the installation commander has elected to retain security cognizance of on-base contractors as a cleared facility, the commander will ensure security oversight actions are performed in accordance with DoDM 5220.22, Volume 2. **(T-0).** The contractor's security posture will be evaluated based upon the standards in DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM).* **(T-0).** Security oversight actions include, but are not limited to: review of the contractor's Standard Practices and

Procedures and its implementation, conduct periodic inspections of the contractor's security controls and communicate any observations, process and review contractor security violations, and communicate with DSS regarding the security posture of the contractor facility.

1.6.3.2. (ADDED) When the installation commander retains security cognizance of on-base contractor facilities and the contract includes a requirement for one or more classified systems, the local Cybersecurity Squadron will support the installation, oversight, and maintenance of the classified system(s). **(T-1).**

1.6.4. (REVISED) DSS makes risk management determinations in consultation with and for the Air Force relating to contractor Foreign Ownership, Control, or Influence (FOCI) to include supporting the Air Force National Interest Determination (NID) process when needed. Close coordination between Information Protection Offices, Program Managers, Contracting Officers, and DSS is critical in ensuring identification of FOCI factors, maintenance of FOCI mitigation agreements, and oversight of facilities operating under FOCI.

1.6.5. (REVISED) The Contracting Officer awards or modifies contracts. Only the Contracting Officer can enter into, administer, or terminate a contract. If the Special Access Program (SAP) Program Security Officer and/or Sensitive Compartmented Information (SCI) Special Security Officer (SSO) require any modifications to a contract, they must coordinate their request with the Contracting Officer. **(T-0).** This does not negate the requirement to coordinate DD Forms 254 with the Information Protection office as identified in paragraph 3.1.1. of this AFI. **(T-1).** Once awarded or modified, the Contracting Officer, with assistance from the Program Manager, notifies the Activity Security Manager and the servicing Information Protection Office when a contract requires performance on a government installation and 1) access to classified information, and/or 2) Information Technology Level I/II access is required, and/or 3) when a security clearance is required to perform unclassified services in a facility requiring a security clearance for unescorted access. **(T-1).** Notifications shall be made as soon as possible, recommended not to exceed 30 days of award or modification. **(T-1).**

1.7. (REVISED) Other Roles and Responsibilities. The following are key stakeholders contributing to an effective AF industrial security posture:

Paragraph 2.4.1.1. (ADDED) For on-base cleared contractor facilities as described in Paragraph 1.6.3.1.of this AFI and in DoDM 5220.22, Volume 2, DSS retains their delegated role as the Cognizant Security Office. The Air Force provides oversight under the authority of the Cognizant Security Office when the Installation Commander requests to retain oversight of the on-base cleared facility. Installation Commanders must submit requests for waivers of security requirements of the NISPOM for on-base cleared contractor facilities through DSS to the Office of the Under Secretary of Defense for Intelligence, for decisions regarding contractor waiver requests. **(T-0).** The Installation Commander should include a recommendation regarding the waiver request in the

staffing package and provide a copy to the MAJCOM/DRU Information Protection Office.

2.4.3. (REVISED) Shall grant contractors (prime contractors and subcontractors) access to the installation IAW AFMAN 31-113, *Installation Perimeter Access Control*. **(T-1).**

2.4.4. (REVISED) Shall designate classified contractor operations (prime contractors and subcontractors) as cleared facilities, visitor groups or intermittent visitors. **(T-0).** The specific performance location(s) and identification of the organization with security oversight shall be identified on the DD Form 254. **(T-1).**

2.4.5. (REVISED) Will enter into security agreements with contractors (prime contractors and subcontractors) performing collateral duties, by signing Visitor Group Security Agreements (VGSA)." **(T-1).** Additional guidance regarding subcontractors is located at Paragraph 4.2.2.

2.5.3.2. (DELETED)

2.5.5. (REVISED) Review VGSAs and staff packages for approval. **(T-1).**

2.5.6. (REVISED) Serve as the authority to perform industrial security program oversight for contractor operations and coordinate with DSS when unique or special operational circumstances warrant and in all cases when the Air Force provides oversight of on-base cleared facilities. **(T-0).**

2.5.7. (REVISED) Coordinate with the MAJCOM/DRU Director, Information Protection; Contracting Officer; the contractor's Home Office Facility Security Officer (FSO); and DSS when assigning an unsatisfactory review rating for a cleared facility. **(T-0).**

2.5.9. (REVISED) Monitor program/project manager responses to contractor security violation notifications received from DSS. **(T-1).** Ensure responses include a review of the classification of the information, a recommendation for mitigation actions to be taken by the contractor, and whether or not the information will remain classified. **(T-0).** Ensure responses are provided to the cognizant DSS Field Office and a copy is provided to SAF/AAZ through Command Information Protection channels. **(T-0).** If a damage assessment is required, refer to DoDM 5200.01 Volume 3, Enclosure 6 and AFI 16-1404, Chapters 3 and 7 for additional guidance.

2.6.9. (REVISED) Administer the DSS contractor reported security violations process and ensure a copy of the returned response is provided by program/project managers to DSS and a copy is provided to SAF/AAZ through Command Information Protection channels. **(T-1).**

2.7. Contracting Officer Actions. (REVISED) In addition to requirements in this AFI; DoDM 5220.22, Volume 2; DoDM 5220.22 Volume 3, *National Industrial Security Program:*

Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI); and DTM 15-002, *Policy Guidance for the Processing of National Interest Determinations in Connection with FOCI*; submit NIDs in accordance with AFHB 16-1406. Contracting Officer responsibilities include the following:

2.7.3. (REVISED) Shall sign Block 17 of the DD Form 254 as the certifying official. **(T-0).** The Contracting Officer may delegate this responsibility to a knowledgeable individual familiar with the requirements of the contract. The delegate will normally be an individual from the office with the requirement (e.g. Program Manager, Program Security Officer, Contracting Officer's Representative, etc.). Delegation must be conducted in writing with copies maintained by the Contracting Officer and the delegate, be available for review during self-inspections and other oversight activities, and include the following: **(T-1).**

2.7.3.1. (ADDED) The Contracting Officer and the delegate must both sign the delegation letter to document the authority for delegation and the acceptance of responsibility. **(T-1).** Contracting Officers can terminate the delegation in writing at any time.

2.7.3.2. (ADDED) The Contracting Officer will ensure the delegation letter includes a statement that the delegate is knowledgeable of the requirements of the contract, has reviewed the DD Form 254 Instructions, *Instructions for Completing DD Form 254, Department of Defense Contract Security Classification Specification* and supplemental security guidance, and is aware of their responsibilities under the Federal Acquisition Regulation. **(T-1).**

2.7.3.3. (ADDED) The delegate must be a government employee (federal civilian or military member). **(T-0).** Contractor employees may not serve as certifiers of DD Forms 254 through delegated authority of the Contracting Officer.

2.7.3.4. (ADDED) The Contracting Officer retains the responsibility to incorporate the DD Form 254 into the contract with the solicitation, award, or contract modification in accordance with the Federal Acquisition Regulation, 4.403. **(T-0).**

3.1. (REVISED) The DD Form 254 communicates security requirements needed in the performance of a classified contract. For Request for Bid, Request for Proposal, and Request for Information see DFARS 204.403 and PGI 204.403 which include the responsibility for Contracting Officers to clarify security requirements to the contractor. When access to classified information is required prior to award of a contract, the DD Form 254 shall be completed in the same manner as a DD Form 254 at contract award. **(T-0).** Program/project managers or designees must prepare the DD Form 254 for prime contracts. **(T-1).** In the absence of exceptional circumstances that clearly support classification, the DD Form 254 will not be classified. If classified supplements are required as part of the security classification specification, the Contracting Officer must ensure they are identified in item 13 of the DD Form 254 and be furnished as an attachment or forwarded to the contractor by separate

correspondence. **(T-1).** The certifying official will sign the form in block 17. **(T-0).** The DD Form 254 Instructions may be referenced for detailed guidance on the correct preparation of the DD Form 254. The DD Form 254 can be located on the NISP Contract Classification System (NCCS) website accessible on the Procurement Integrated Enterprise Environment (PIEE) system at https://wawf.eb.mil. Information Protection Offices will provide NCCS hierarchy management and account provisioning support for those installation security offices with a reviewing role in the processing of the DD Form 254. **(T-3).** Acquisition and Contracting Offices will provide NCCS hierarchy management and account provisioning support for their workflow requirements. **(T-3).**

3.1.1. (REVISED) The servicing Information Protection Office must review and coordinate by annotating Block 13 with name, organization, office symbol, and digital signature. **(T-1).** When reviewing a DD Form 254 routed in hard copy, the office symbol, date and initials/signature of reviewer are the minimum items required. **(T-1).** NOTE: When reviewing the DD Form 254 in NCCS, this step is automated and may not conform exactly to these guidelines.

3.1.1.1. (ADDED) When Item 10(e) of the DD Form 254 is selected, the servicing Special Security Officer (or designee) must document coordination in Block 13. **(T-1).**

3.1.1.2. (ADDED) When Item 10(f) of the DD Form 254 is selected, the servicing Program Security Officer and/or Government SAP Security Officer (or designee), as appropriate, must document coordination in Block 13. **(T-1).**

3.2.1.2. (REVISED) Revised DD Forms 254 are issued when there is a change to the classification guidance or security requirements of the contract, including additional performance location(s) and the contractor's physical address change.

3.2.2. (REVISED) If blocks 10a, b, c, e(1), f are selected or Top Secret access is required, verify in the National Industrial Security System (or successor system) whether the company requires a NID. If the company does require a NID for access to proscribed information, verify a NID has been completed or ensure a NID is submitted in accordance with AFHB 16-1406.

3.2.3. (REVISED) Block 12 Public Release: Ensure "Through" block is marked and the following statement is included: "Contractor is to submit requests through the Contracting Officer for OPSEC Program Manager review and public release authorization. The Contracting Officer will provide contractor with written approval/disapproval. **(T-1).** Information requiring AF or DoD–level review will be reviewed by the unit's OPSEC Program Manager or Coordinator who will in-turn forward to the entry-level public affairs office through the AFIMSC Public Affairs Office to the Secretary of the Air Force, Office of Public Affairs, Security and Review Division (SAF/PAX), 1690 Air Force Pentagon, Washington DC 20330-1690." MAJCOM/DRUs will send information requiring AF or DoD-level review directly to SAF/PAX. **(T-0).**

3.2.4.2. (REVISED) Reviewers shall use this area to document coordination by annotating name, organization, office symbol, and digital signature. **(T-1).** When reviewing a DD Form 254 routed in hard copy, the office symbol, date and initials/signature of reviewer are the minimum items required. **(T-1).** NOTE: When reviewing the DD Form 254 in NCCS, this step is automated and may not conform exactly to these guidelines.

3.2.5. (REVISED) The Contracting Officer shall sign Block 17 Certification. **(T-0).** See Paragraph 2.7.3. for requirements when the Contracting Officer delegates certification authority for the DD Form 254.

3.2.6. (REVISED) Block 18 Required Distribution. If work is to be conducted at multiple locations or MAJCOMs, the Contracting Officer or designee shall ensure the DD Form 254 is distributed to the commanding officer or civilian equivalent (or designee) at the location of contract performance. **(T-1).**

4.2.4. (REVISED) Require that contractor employees who need access to government information technology (IT) systems, or otherwise occupy billets designated as national security positions as defined in Title 5 Code of Federal Regulations, Part 1400, *Designation of National Security Positions*, current edition, are determined to be trustworthy by the completion of a favorable personnel security investigation commensurate with assigned duties and adjudication by a designated government official prior to IT access being granted or assumption of sensitive duties. **(T-0).** Personnel security investigative requirements for access to IT systems are based on the level of access/privileges granted to the user (IT Level I, II or III). Privileged access is defined in DoD 8570.01-M, *Information Assurance Workforce Improvement Program,* Appendix 1, Definitions, AP1.22. Privileged Access and AFMAN 17-1301, *Computer Security*, Paragraph 4.2. The Government sponsor/security manager will submit contractor personnel security investigation requests (i.e., contractors who do not need access to classified information) for logical access to government IT systems, assignment to sensitive duties, or physical access to federal installations. **(T-0).**

5.3.4. (ADDED) In accordance with DoDM 5220.22, Volume 2, Paragraphs 2.7.h. and 8.4., Commanders shall report to DSS, Personnel Security Management Office for Industry (PSMO-I), and to the Department of Defense Consolidated Adjudications Facility (DoD CAF), any adverse or questionable information that comes to his or her attention, concerning a contractor employee who has been cleared, or is in the process of being cleared, for access to classified information, which may indicate that such access is not clearly consistent with the national interest. **(T-0).** Commanders shall also provide this notification to the servicing Information Protection Office. **(T-1).**

5.3.4.1. (ADDED) If the Commander can confirm that the Facility Security Officer notified DSS PSMO-I and the DoD CAF, additional notification is not required. **(T-3).**

5.3.4.2. (ADDED) Until such time as an automated solution is developed to provide simultaneous notification to DSS PSMO-I and the DoD CAF, Commanders are responsible for ensuring both notifications are accomplished. Commanders will provide initial notification to the servicing Information Protection Office who will further notify DSS PSMO-I and the DoD CAF. **(T-0).** The Information Protection Office will provide initial notification to DSS PSMO-I via their notification mailbox at **dss.ncr.dss-dvd.mbx.askvroc@mail.mil**. **(T-0).** Ensure initial notifications are sanitized such that they do not reveal protected information or encrypt the email when sending. **(T-0).** If sending a sanitized notification, DSS PSMO-I will follow-up the email with additional contact information where a complete report can be made. The Information Protection Office will provide notification to the DoD CAF through JPAS or successor system. **(T-0).** Notifications shall include relevant information in accordance with DoD 5200.02_AFMAN 16-1405, *Air Force Personnel Security Program*. **(T-0).** Notification procedures to the servicing Information Protection Office shall be developed locally. **(T-1).**

6.1.5.4. (ADDED) The industrial security specialist shall coordinate with DSS when a facility's security posture is less than Satisfactory. **(T-0).**

6.2. (REVISED) Self-Inspections and Self-Assessments for Visitor Groups. Wings and sponsoring AF activities will include contractor integrated visitor groups within their self-inspection and self-assessment programs. **(T-0).** Information Protection Offices and other security relevant program areas will evaluate independent visitor groups separate from its government sponsor. **(T-1).** Evaluation criteria will be based upon AFI 16-1404, Chapter 10, and the VGSA. Information Protection Offices and other security relevant program areas will evaluate independent visitor groups at a frequency based on risk management principles, not to exceed 24 months. **(T-3).** Contracting Officers will ensure a requirement for contractors to support these activities is included in appropriate contracts. **(T-0).**

6.2.1. (ADDED) Information Protection Offices shall utilize the Enterprise Protection Risk Management (EPRM) tool as the designated system for recording and aggregating key elements of self-inspections within their respective organizations as well as other organizations being supported through host tenant support agreements, memoranda of understanding or agreement, or supplements. **(T-1).** The EPRM tool will provide information to Commanders useful in the risk management decision process.

6.4. (REVISED) For installations with on-base cleared facilities where oversight is retained by the installation commander, the Information Protection Office must conduct close-out inspections when actions are being taken to negate the need for a facility clearance, e.g. contractual requirements no longer require access to classified information. **(T-0).** The Information Protection Office must also conduct close-out inspections for independent visitor groups. **(T-1).** The close-out inspection must occur prior to the administrative termination of the facility clearance and must include a thorough check of all areas and containers authorized for storage of classified material to ensure all classified items in the possession of the contractor facility are properly secured and returned to the government prior to facility clearance

termination. **(T-0).** The program office, requiring AF activity or Contracting Officer will notify the Wing industrial security specialist in writing 30 days prior to expected completion or termination of contract performance. **(T-0).**

8.1. (REVISED) Special Access Program (SAP). The Air Force assumes security cognizance of Special Access Program contracts where contractor performance takes place within a Special Access Program Facility. Program Security Officers and/or Government SAP Security Officers coordinate with the appropriate Contracting Officer and Program Manager to validate DD Forms 254 contain language indicating DSS and/or Air Force Information Protection Offices are "carved out" of program oversight and identify the Air Force Office of Special Investigations, Office of Special Projects (AFOSI/PJ) as having security and compliance inspection responsibility. **(T-0).** DSS will continue to serve as the Cognizant Security Office for the Facility Clearance, and for on base performance, the servicing Information Protection Office will provide oversight of any collateral performance outside a Special Access Program Facility but will provide no oversight of the space where SAP information is stored to include any non-SAP material stored in the space (e.g. collateral classified material, controlled unclassified information (CUI)). **(T-0).** For contracts with SAP access, a DD Form 254 may be certified only after endorsement by a Program Manager and Program Security Officer. **(T-0).** Contracting Officers may delegate the authority to certify a DD Form 254 with SAP requirements in accordance with this AFI (for additional SAP guidance, see AFI 16-701, *Management, Administration and Oversight of Special Access Programs).* Responsibility for oversight of SAP material and spaces in regards to contractor oversight resides with the cognizant Program Security Officer.

8.2. (REVISED) Sensitive Compartmented Information (SCI). Air Force contracts that include requirements for access to SCI typically "carve out" DSS and/or Air Force Information Protection Offices from oversight of the information as well as spaces where SCI is stored. DSS will continue to serve as the Cognizant Security Office for the Facility Clearance, and for on base performance, the servicing Information Protection Office will provide oversight of any collateral performance outside an SCI Facility but will provide no oversight of the space where SCI is stored to include any non-SCI material stored in the space (e.g. collateral classified material, CUI). **(T-0).** Responsibility for oversight of SCI material and spaces resides with the cognizant Special Security Officer.

9.2. (REVISED) Disclosure of Information to Foreign Visitors/Interests. Visits by foreign representatives to contractors performing on AF contracts (whether on or off base) which require access to classified military information (CMI) or CUI related to those contracts are processed in accordance with AFI 16-201, *AF Foreign Disclosure and Technology Transfer Program*. Requests to disclose CMI and CUI must be coordinated and approved by the servicing AF Foreign Disclosure Office with the appropriate delegated disclosure authority. **(T-0).** Refer to AFI 16-201 for further information.

Attachment 1 – Glossary of References and Supporting Information

References

(DELETED) DoD 5220.22-R, *Industrial Security Regulation*, December 4, 1985

(ADDED) DoDM 5220.22, Volume 2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, August 1, 2018

(ADDED) DoDM 5200.02_AFMAN 16-1405, Air Force Personnel Security Program, August 1, 2018

Terms

(ADDED) Integrated Visitor Group – A contractor whose contract performance is categorized by the installation commander as an integrated visitor group operates under day-to-day oversight of an Air Force activity. Contractor employees working as part of an integrated visitor group typically sit in the same work-space as government employees where an Air Force official is responsible for the security requirements of the space. These contractor employees are integrated into a Commander/Director's Information Security Program.

(ADDED) Independent Visitor Group – A contractor whose contract performance is categorized by the installation commander as an independent visitor group operates independently from an on-base Air Force activity. Contractor employees working as part of an independent visitor group operate independently from day-to-day oversight by Air Force employees and typically have a separately assigned space for which they are responsible as described in Memoranda of Agreement, Support Agreements, etc. Contractors are normally only categorized this way when their contract requires them to store classified information and they do so separately from other Air Force operations.

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 16-1406

25 AUGUST 2015

Incorporating Change 1, 30 JANUARY 2017

Operations Support

AIR FORCE INDUSTRIAL SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available at **www.e-Publishing.af.mil** for downloading or ordering on the e-Publishing website

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: SAF/AAZ

Certified by: SAF/AAZ
(Mr. David Lowy)

Supersedes: AFI31-601, June 29, 2005

Pages: 29

This publication implements the industrial security portion of the Security Enterprise defined in Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*. It provides guidance for implementing the National Industrial Security Program and is applicable to AF personnel, the Air National Guard, the Air Force Reserve, and DoD contractors performing under the terms of a properly executed contract and associated visitor group security agreement as determined appropriate by the serivicing installation commander. This may include access to Controlled Unclassified Information (CUI), and technical information as defined in DFARS clause 252.204-7012, *Safeguarding of Unclassified Controlled Technical Information*. Use this instruction with DoD 5220.22-R, *Industrial Security Regulation*, DoD 5220.22-M, *National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)*: *Volume* 3, and DoD 5200.01-M V1-4, *DoD Information Security Program* and if necessary, DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*. Ensure records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records* and disposed of IAW the Air Force Records Disposition Schedule (RDS) in the Air Force Records Information Management System (AFRIMS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented by MAJCOM but drafts must be reviewed by this publication's OPR prior to publishing. (T-1) The authorities

to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement.

SUMMARY OF CHANGES

This interim change to portions of AFI 16-1406, *Air Force Industrial Security Program* provides direction for processing all National Interest Determinations (NIDs of Collateral, Sensitive Compartmented Information (SCI), and Special Access Programs (SAP). Reference AFI 16-1406 NID Handbook for guidance in submitting NIDs**.**

Chapter 1

PROGRAM OVERVIEW AND ROLES AND RESPONSIBILITIES

1.1. AF Security Enterprise. AFPD 16-14 defines the Air Force Security Enterprise as the organizations, infrastructure, and measures (policies, processes, procedures, and products) in place to safeguard AF personnel, information, operations, resources, technologies, facilities, and assets against harm, loss, or hostile acts and influences. Information Protection is a subset of the Air Force Security Enterprise. Air Force Industrial Security is a core discipline within Information Protection.

1.2. Information Protection. Information Protection is a subset of the Air Force Security Enterprise. Information Protection consists of three core security disciplines (Personnel, Industrial, and Information Security) which support insider threat detection and mitigation efforts and are used to:

1.2.1. Determine military, civilian, and contractor personnel eligibility to access classified information (Personnel Security).

1.2.2. Ensure the protection of classified and CUI information released or disclosed to industry in connection with classified contracts (Industrial Security).

1.2.3. Protect classified information and CUI that, if subject to unauthorized disclosure, could reasonably be expected to cause damage to national security (Information Security).

1.3. Information Protection Oversight. These key positions direct, administer, and oversee management, functioning and effectiveness of the Information Protection Program.

1.3.1. The Senior Agency Official (SAF/AA) is the Secretary of the Air Force appointed authority responsible for the oversight of Information Protection.

1.3.2. The Security Program Executive (SPE) is appointed by the MAJCOM/DRU Commander in accordance with AFPD 16-14 and is responsible oversight of Information Protection for their MAJCOM/DRU.

1.3.3. Wing Commanders provide oversight of Information Protection by ensuring security controls, safeguards, and countermeasures are established through application of risk management principles, as appropriate, for their wings. (T-1) This may be delegated to the Wing/CV.

1.4. Information Protection Managers. These key positions develop guidance as necessary, and serve as principal advisors to the personnel identified in paragraph 1.3.

1.4.1. Director of Security, Special Program Oversight and Information Protection (SAF/AAZ) is responsible to the Senior Agency Official and addresses the equities within the functional portfolio related to Information Protection.

1.4.2. MAJCOM/DRU Director, Information Protection is responsible to the SPE and for integrating Information Protection into MAJCOM/DRU operations and provides oversight and direction to the security specialists and other personnel assigned to the MAJCOM/DRU Information Protection Directorate.

1.4.3. Chief, Information Protection is responsible for executing Information Protection on behalf of the Wing Commander and provides oversight and direction to commanders and directors at all levels and their security managers, and security specialists and other personnel assigned to the DRU/Wing Information Protection Office. (T-1)

1.4.4. Commanders and Directors ensure military and civilian personnel are properly cleared for access to classified information and CUI, integrate contractors into their existing security programs, and protect classified information and CUI under their authority to support Information Protection. (T-1)

1.5. Information Protection Implementation. The key security professionals below are responsible for implementing Information Protection core security disciplines (information, industrial, and personnel security):

1.5.1. Security Specialists are Office of Personnel Management (OPM) occupational series 0080, Security Administration, and are responsible for effecting Information Protection core security disciplines (Information, Personnel, Industrial Security) for a MAJCOM/DRU, or Wing.

1.5.2. Security Managers are principal advisors to commanders and directors. They implement the core security disciplines under the guidance and direction of the DRU/Wing Chief, Information Protection or one of the security specialists assigned to the Information Protection Office.

1.5.3. Military or civil service personnel assigned to the Information Protection Directorate or Office must meet the rank/grade requirements listed in DoD 5200.01-M, Volume 1, Enclosure 2, and complete training equivalent to information security specialists as prescribed in AFI 16-1404. (T-1)

1.6. Industrial Security . This core security discipline of Information Protection is designed to identify and protect classified national security information within DoD when that information is entrusted to industry. In most cases for the AF, "industry" consists of contractors that have been validated by DSS to have access to classified material. This AFI is used in conjunction with AFI 16-1404, Air Force *Information Security Program*. Within the AF industrial security program:

1.6.1. Identify in classified contracts using the DoD Contract Security Classification Specification (referred to as DD Form 254) procedures for protection of classified information/sensitive resources.

1.6.2. Categorize on-site contractors as Vistor Groups and integrate contractors into the organization's information security program in accordance with this AFI and AFI 16-1404.

1.6.3. When the installation commander has elected to retain security cognizance of contractors as a cleared facility, the commander will conduct security reviews in accordance with the NISPOM. (T-1) **NOTE:** Categorize DoD contractor operations supporting the AF overseas as visitor groups.

1.6.4. Defense Security Service (DSS) makes risk management determinations for the AF relating to contractor Foreign Ownership, Control, or Influence (FOCI) to include supporting the Air Force National Interest Determination (NID) process when needed.

1.6.5. The Contracting Officer (CO) award or modify contracts. Only the CO can enter into, administer or terminate a contract. If the Security Assistance Policy Coordinating Office

(SAPCO) and/or Special Security Officer require any modifications to a contract they must coordinate their request with the Contracting Officer. This does not negate the requirement to coordinate DD Forms 254 with the IP office as identified in **Chapter 3**. Once awarded or modified, the Contracting Officer, with assistance from the Program Manager notifies the Security Manager and the servicing IP Office when a contract requires performance on a Government installation and 1) access to classified information, and/or 2) IT Level I/II access is required, and/or 3) when a security clearance is required to perform unclassified services in a facility requiring a security clearance for unescorted access, as soon as possible, recommended not to exceed 30 days of award or modification.

1.7. Other Roles and Responsibilities. Is a key stakeholder contributing to an effective AF industrial security posture identified in AFI 16-1404.

1.7.1. The Deputy Assistant Secretary (Contracting), Assistant Secretary (Acquisition), (SAF/AQC) is responsible for formulating and interpreting Air Force contracting policy and issuing Air Force supplemental guidance to the Federal Acquisition Regulation (FAR).

1.7.2. Original Classification Authorities are responsible for conducting damage assessments in accordance with DODM 5200.01 Vol. 3, Encl. 6 and AFI 16-1404. (T-1)

Chapter 2

INDUSTRIAL SECURITY IMPLEMENTATION

2.1. Security Program Executives (SPE) . In addition to duties found in AFI 16-1404, provide oversight of industrial security program activites within their area of responsibility.

2.1.1. Approve program waivers and exceptions to policy and submit them to SAF/AA, when necessary.

2.1.2. Assess reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities or visitor groups and determine appropriate risk based countermeasures. AFOSI is the investigating agency concerning these reports or any other similar actions. Copies of the final reports will be submitted to SAF/AAZ.

2.2. MAJCOM/DRU Director, Information Protection . In addition to AFI 16-1404 responsibilities for Information Security, ensures Industrial Security Program implementation and provides oversight of subordinate Wings or organizations within their area of operations.

2.2.1. Assess program waivers and exceptions to policy and validate their accuracy prior to submission to the SPE for approval.

2.2.2. Provide the SPE risked-based countermeasure strategies concerning reported espionage, sabotage, subversive activies, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities and visitor groups located on or serviced by the command.

2.2.3. Develop industrial security data calls or responses when requested.

2.2.4. Ensure industrial security supplements and self-assessment checklists are coordinated with SAF/AAZ prior to publication and submission to the Management Internal Control Tool (MICT) database.

2.2.5. Notify SAF/AAZ of unsatisfactory Security Reviews of cleared facilities.

2.2.6. Report security violations and infraction metrics to SAF/AAZ when requested.

2.3. MAJCOM/DRU Industrial Security Specialist. Works closely with the MAJCOM/DRU Information Security Specialist to deliver a robust Industrial Security Program for the command.

2.3.1. Research program standards to validate program waivers and exceptions.

2.3.2. Participate in the development of risk based countermeasure strategies for reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities or visitor groups and determine appropriate risk based countermeasures.

2.3.3. Collect data to support industrial security data calls when requested.

2.3.4. Write and develop industrial security supplements and self-assessment checklists.

2.3.5. Notify the Director, Information Protection of unsatisfactory security reviews of cleared facilities.

2.3.6. Track unsatisfactory security reviews of cleared facilities until deficiencies are corrected or administrative action is taken on the Facility Security Clearance (FCL).

2.3.7. Collect, analyze and maintain metrics for security violations and infractions.

2.3.8. Process contractor reported security violations to SAF/AAZ. Upon receipt from SAF/AAZ, these are distributed to the appropriate Wing Information Protection Office.

2.3.8.1. Process copies of replies to DSS to SAF/AAZ.

2.3.9. Submit all Collateral, Sensitive Compartmented Information (SCI) and Special Access Programs (SAP) NIDs in accordance with AFHB 16-1406**.**

2.3.9.1. Refer Special Access Program (SAP) NID questions/submissions to MAJCOM SAP Management Office.

2.3.9.1. **(DELETE)**

2.4. Installation Commanders. In addition to responsibilities found in AFI 16-1404 for Wing Commanders and when the Installation Commander has elected to retain security cognizance for cleared facilities on an Air Force installation, the host –installation cybersecurity office (formerly information assurance) shall assist the servicing IP office by providing oversight in the contractor's system/networks that process/store Government information to ensure those system/networks are properly accredited and all DoD/AF information technology cybersecurity requirements are met.

2.4.1. Submit program waivers and exceptions to policy to the SPE through Information Protection channels. (T-1)

2.4.2. Provide reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities or visitor groups to the SPE, and determine risk based countermeasures to be enacted. (T-1)

2.4.3. Grant contractors (prime contractors and subcontractors) access to the installation IAW AFM 33-113, 33-113, *Installation Perimeter Access Control*.

2.4.4. Designate classified contractor operations as cleared facilities, visitor groups or intermittent visitors. Cleared facilities and visitor groups or intermittent visitors shall be identified as a specific performance location and security oversight on the DD Form 254. (T-1)

2.4.5. Enter into security agreements with contractors (prime contractors and subcontractors) preforming collateral duties, by signing Visitor Group Security Agreements (VGSA)." (T-1) For subcontractors see * 4.2.2. This may be delegated to the Chief, Information Protection. (T-1)

2.5. (Wing) Chief, Information Protection . In addition to responsibilities found in AFI 16-1404, this position should establish rapport with program or project managers and commanders/directors (hereinafter referred to as program/project managers) to ensure effective management of the industrial security program. When the Installation Commander has elected to retain security cognizance of industrial security activities ensure the following:

2.5.1. Analyze and submit program waiver and exception packages through Information Protection channels to appropriate approval authority. (T-1)

2.5.2. Brief the Installation Commander on reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities, visitor groups, or intermittent visitors and recommends appropriate risk based countermeasures. (T-1)

2.5.3. Make recommendations to the Installation Commander on restricting access to classified information when security reviews result in an unsatisfactory rating. (T-1)

2.5.3.1. If the cleared facility fails to take corrective actions, provide support information with recommendations (e.g., removal of facility clearance level). (T-1)

2.5.3.2. Notify the MAJCOM/DRU Director, Information Protection of facility rating. (T-1)

2.5.4. Develop staff packages to designate contractor operations as cleared facilities, visitor groups or intermittent visitors. This designation is determined by the visitor's relationship and interface with the AF activity and/or installation. (T-1)

2.5.5. Review VGSA and submit package to Installation Commander for signature unless this signature authority is delegated to the Chief of Information Protection. (T-1)

2.5.6. Serve as the authority to perform industrial security program oversight for contractor operations and coordinate with DSS when unique or special operational circumstances warrant. (T-1)

2.5.7. Coordinate with the MAJCOM/DRU Director, Information Protection, local contracting officer, and Home Office Facility (HOF) Facility Security Office (FSO) when assigning an unsatisfactory review rating for a cleared facility. (T-0)

2.5.8. Forward a copy of the security review and survey reports and other applicable documentation, pertaining to a "cleared facility" per DOD 5220.22-M, DOD 5220.22-R, and this instruction, as required to DSS. Forward a copy to the MAJCOM/DRU and SAF/AAZ through Information Protection channels when requested. (T-0)

2.5.9. Administer, and ensure a copy of the returned response is provided by program/project managers to SAF/AAZ through Information Protection channels concerning DSS reported contractor security violations.

2.5.10. Submit all (Collateral, SCI and SAP) NIDs in accordance with AFHB 16-1406.

2.6. (Wing) Industrial Security Specialist . Provide guidance to program/project managers (see para 2.5) to ensure security procedures (e.g., SCI, physical, OPSEC, SAP, etc.) are followed throughout the contracting process. Assist in determining the relationship and interface between the contractor and the Air Force to designate contractor activities as visitor group, cleared facility, or intermittent visitor. Work closely with the Wing Information Security Specialist to deliver a robust Industrial Security Program.

2.6.1. When the Installation Commander has elected to retain security cognizance of contractor cleared facilities:

2.6.1.1. Review and prepare program waivers and exceptions to policy and develop staff packages for the commander. (T-1)

2.6.1.2. Analyze reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities, visitor groups, or intermittent visitors and develop possible courses of action to mitigate risks. (T-1)

2.6.1.3. The servicing host-installation cybersecurity (formerly information assurance) official should accompany the industrial security specialist to review the contractor's system/networks that process classified or controlled unclassified information for compliance. Conduct industrial security reviews of cleared facilities in accordance with NISPOM. Collaborate with FSO to determine or monitor any necessary corrective actions.

2.6.1.4. Staff correspondence for unsatisfactory ratings of security reviews. (T-1)

2.6.2. Establish a process, if necessary, with the servicing CO to ensure Information Protection Office (IP) is notified 30 days prior to work performance start date, when contract performance is on the IP's installation and access to classified information is required. (T-1)

2.6.3. Participate in development of Visitor Group Security Agreements in accordance with **Chapter 4**, incorporating visitor groups into the serviced unit information security program. (T-1)

2.6.4. Review DD Form 254. Refer to **Chapter 3** for specific guidance. (T-1)

2.6.5. Track, maintain, and analyze contractor visitor group security violations and infraction metrics, report through Information Protection channels to SAF/AAZ upon request. Categorize these occurrences with the terms found in AFI 16-1404.

2.6.6. Report adverse information and suspicious contact, security violations, and espionage, sabotage, and subversive activties in accordance with **Chapter 5** of this AFI. (T-0)

2.6.7. Provide industrial security training for security managers as applicable.

2.6.8. Provide industrial security review data and derivative classification decisions for inclusion in Senior Agency Self-Inspection and Agency Security Classification Management Program Data reports for visitor groups. (T-0)

2.6.9. Administer the DSS contractor reported security violations process and ensure a copy of the returned response is provided by program/project managers to SAF/AAZ. (T-0)

2.6.10. Submit all (Collateral, SCI and SAP) NIDs in accordance with AFHB 16-1406**.**

2.6.11. Work closely with the host-installation cybersecurity office (formerly information assurance). The host-installation cybersecurity office will provide oversight to any approved contractor system/networks that process classified or controlled unclassified information to ensure those system/networks are properly accredited/authorized and all DoD/AF information technology cyber-security requirements are met. (T-0)

2.7. Contracting Officer Actions. In addition to requirements in this AFI, DoD 5220.22 Volume 3, *National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI*) and DTM 15-002, *Policy Guidance for the*

Processing of National Interest Determinations in Connection with FOCI. *Submit NIDs in accordance with AFHB 16-1406.

2.7.1. Notify the servicing Wing Information Protection Office:

2.7.1.1. Ensure contractor compliance IAW AFFARS Security Clause 5352.204-9000, Notification of Government Security Activity and Visitor Group Security Agreements, at Gov't and OCONUS place performance locations identified in the DD Form 254.

2.7.1.2. Submit all (Collateral, SCI and SAP) NIDs in accordance with AFHB 16-1406**.**

2.7.2. Ensure DD form 254 is distributed in accordance with **Chapter 3** of this AFI.(T-1)

2.7.3. Sign Block 16 of the DD Form 254 as the certifying official. (T-0)

2.7.4. Contact the GCA's servicing IP office for assistance immediately before obtaining mailing addresses and contact information for the individual IP offices at each contract performance location.

2.8. System, Program, Project Managers, Commanders/Directors. These positions are referred to as program/project managers in this AFI**.** These positions are key to identification of specific types of information required by the contractor and security classification guidance by completing the DD Form 254. Program/project managers also play a critical role in identifying companies with access to proscribed information. Submit all (Collateral, SCI and SAP) NIDs in accordance with AFHB 16-1406. In addition, program/project managers assist with the development of the VGSA, providing responses to security violations to DSS (and the Wing Information Protection office), and identifying and reporting changes that may affect a contracted company FCL.

2.8.1. A DD Form 254 will be included with the Request for Bid, Request for Proposal, and Request for Information to clarify security requirements for the final contract award. When access to classified information is required during the acquisition process, a DD Form 254 shall be completed in the same manner as a DD Form 254 for awarding a contract (Ref **Chapter 3**).

2.8.2. Notify the servicing Wing Information Protection office 30 days prior to contractor work beginning (i.e., work or classified information access; a contract with a DD Form 254) and assist with development of the VGSA. (T-1)

2.8.3. Process DSS reported security violation responses received from the servicing Wing Information Protection office to DSS and provide a copy to the wing. (T-0)

2.8.4. Changes that could affect the FCL include but are not limited to: indicators of FOCI, federal investigation resulting in FCL termination, termination of FCL by owners request, etc. (T-0)

Chapter 3

THE DD FORM 254

3.1. The DD Form 254 communicates security requirements needed in performance of a classified contract. For Request for Bid, Request for Proposal, and Request for Information see DFARS 204.403 and PGI 204.403 which includes responsibilities of Contracting Officers to clarify security requirements. When access to classified information is required prior to award of a contract, the DD Form 254 shall be completed in the same manner as a DD Form 254 at contract award. Program/project managers must complete the DD Form 254 for prime contracts. (T-1) The certifying official will sign the form in block 16. (T-0) The Defense Security Service website may be referenced for detailed guidance. The DD Form 254 can be located on the NISP Contract Classification System (NCCS) accessible on Wide Area Workflow (WAWF) at **https://wawf.eb.mil**.

3.1.1. Ensure servicing Wing Information Protection office reviews and coordinates by annotating Block 13 with office symbol, date and initials of reviewer (T-0).

3.1.2. Submit DD Form 254 to the servicing contracting office for certification. (T-0)

3.1.2.1. Ensure contracts:

3.1.2.1.1. Incorporate language and appropriate contract clauses for protection of critical information identified in the Operations Security program IAW AFI 10-701, **Chapter 8**. (T-0)

3.1.2.1.2. Incorporate language and appropriate contracts clauses for the protection to classified information. (T-0)

3.1.2.1.3. Incorporate language and appropriate contract clauses for protection of unclassified controlled technical information IAW DFARS Subpart 204.73. (T-0)

3.2. Completing the DD Form 254. Complete all blocks on the DD Form 254. (T-0) The following blocks require special attention:

3.2.1. Block 3 This Specification Is: verify the intended specification for the DD 254. (T-0)

3.2.1.1. Original date refers to the release date of the DD Form 254. This date will not change and will be annotated on subsequent revisions of the DD Form 254. (T-0)

3.2.1.2. Revised DD Form 254s are issued when there is a change to classification guidance or security requirements of the contract.

3.2.1.3. "Final' DD Form 254 is only used to authorize additional retention of classified materials beyond the terms of the contract.

3.2.2. If blocks 10a, b, c, e(1), f, or TS access is required, verify in ISFD that the company doesn't require a NID. If the company does require a NID for access to proscribe information, verify a NID has been completed in the ISFD or ensure the GCA submits a NID in accordance with AFHB 16-1406.

3.2.2.1. **(DELETED)**

3.2.2.2. **(DELETED)**

3.2.3. Block 12 Public Release: Ensure "Through" block is marked and the following statement is included: Information requiring AF or DoD–level review will be forwarded by the entry-level public affairs office through the MAJCOM/DRU Public Affairs Office to the Secretary of the Air Force, Office of Public Affairs, Security and Review Division (SAF/PAX), 1690 Air Force Pentagon, Washington DC 20330-1690. (T-0)

3.2.4. Block 13 Security Guidance:

3.2.4.1. Be specific on security guidance.

3.2.4.2. Use this area to show coordination of security officials by annotating contact information and initials. (T-1)

3.2.4.3. **(DELETED)**

3.2.4.4. The responsible Contracting Officer Representative or Program Manager will identify (by title, functional OPR, and approval date, to include letter changes), the specific security classification guidance or guides (SCG) applicable to the contract in block 13 of the DD Form 254. (T-1) If SCG's title is classified, the Program Manager is responsible for notifying the contractor. An addendum sheet may be added to list guides when insufficient space is not provided in Block 13.

3.2.5. Block 16 Certification, is signed by the contracting office. (T-0)

3.2.6. Block 17 Required Distribution. If work is to be conducted at multiple locations or MAJCOMS, ensure the DD Form 254 is distributed to the stakeholders.

3.2.7. **(DELETE)**

3.2.8. Submit all (Collateral, SCI and SAP) NIDs in accordance with AFHB 16-1406**.**

3.3. Distribution of DD Form 254. The CO will maintain a copy of the DD Form 254. (T-1) Distribution is made to:

3.3.1. Wing Information Protection Office for collateral information when contractor performance is on an AF installation.

3.3.2. When SAP is involved, coordinate the DD Form 254 in accordance with AFI 16-701, Management, Administration and Oversight of Special Access Programs. Keep DD Forms 254 unclassified whenever possible. (T-0)

3.3.3. AF/A2 for SCI. Keep DD Forms 254 unclassified whenever possible. (T-0)

3.3.4. DSS Headquarters, if DSS is relieved of security oversight responsibility. (T-0)

Chapter 4

VISITOR GROUPS AND AGREEMENTS

4.1. General. Installation commanders categorize contractors operating on the installation as cleared facility, visitor groups, or intermittent visitors. (T-0) Cleared facilities are discussed in **Chapter 5**. Contractor operations performing less than 90 days qualify as intermittent visitors Intermittent visitors may operate under the security requirements of the NISPOM or the installation security program. Generally, contractor operations in excess of 90 days are designated visitor groups. Visitor Group limits and actions while on the installation are codified in Visitor Group Secuity Agreements.

4.2. Development of the VGSA . The industrial security specialist will ensure VGSA:

4.2.1. Incorporates the visitor group into the AF Information Security Program. (T-1)

4.2.2. A separate or independent VGSA is developed for subcontractors when prime and subcontractors are not working at the same AF installation. If at the same location, a separate VGSA is not required; however, at a minimum, the subcontractor signs the prime contractor's VGSA. (T-0)

4.2.3. Prohibits Visitor Groups from establishing their own Information Technology (IT) systems/networks (Local Area Networks [LAN], Wide Area Network [WAN], Cellular phone/USB Modem as WAN, Wi-Fi as WAN, etc.) without the direct permission of governing communications and responsible information systems office. If permission is granted, the Government office approving the contractor system/network is responsible for providing oversight to the contractor's system/network to ensure the system/network is properly accredited/authorized and all DoD/AF information technology requirements are met. (T-0)

4.2.4. Require contractor employees who need access to government IT are determined to be trustworthy by the completion of a favorable personnel security investigation commensurate with assigned duties and by a designated government official prior to IT access being granted. (T-0) This is accomplished through the system authorization access request, DD Form 2875, process. Reference AFI 31-501 (or applicable revisions) for background investigation requirements.

4.2.5. Use existing AF security program related plans (Operations Security, Program Protection, Information Technology, etc.), procedures, operating instructions, and educational/training materials that meet the intent of and satisfy NISPOM requirements. Coordinate with other security discipline OPRs, when applicable, and incorporate authority for their usage in the VGSA or other appropriate contracting documents. (T-0)

4.2.6. Is coordinated with the security discipline OPRs (T-1)

4.2.7. Allows responsible security discipline OPR to accompany the industrial security specialist or CSO representative during security reviews or when requested. (T-0)

4.2.8. Subcontractors submit independent Visit Requests to the serviced organization via JPAS on their employees. (T-1)

Chapter 5

REPORTING REQUIREMENTS

5.1. Clearances. There are two types of clearances within the industrial security program. A Facility Security Clearance (FCL) is an administrative determination by Defense Security Service (DSS) that a company is eligible for access to classified information. The other clearance is Personnel Security Clearance (PCL)**.** A PCL is an administrative determination that a contractor is eligible for access to classified information. The FCL can be affected if adverse information results in the removal of a PCL, or change introducing FOCI indicators of those identified as key management personnel.

5.2. Requesting a FCL. Most companies bidding on a classified contract have an FCL. However, a company may be awarded a contract and not be in possession of an FCL. Should this occur, the contracting office initiate a request for an FCL. (T-0) A sample FCL request letter can be obtained from the Defense Security Service (DSS) website, Industrial Security page.

5.2.1. A company's FCL can be verified through the Industrial Security Facilities Database (ISFD) maintained by DSS. ISFD can verify the company's safeguarding capability, address, CAGE code, and if the company requires a NID for access to proscribed information.

5.2.1.1. To gain access to the ISFD complete the ISFD System Access Request form located on the DSS website, Information Systems ISFD web page.

5.2.1.2. It is U.S. policy to support foreign investment in the United States consistent with the protection of the national security. Foreign Ownership, Control, or Influence (FOCI) is a set of processes which may facilitate foreign investment in the US. These processes become necessary to make a determination by DSS that access to national defense information by companies impacted by FOCI is considered. SAP NID questions/submissions will be reported to the MAJCOM SAP Management Office. Submit all (Collateral, SCI and SAP) NIDs in accordance with AFHB 16-1406.

5.2.1.3. REVISED from 5.2.2.1. Program/project manager, contracting office, becoming aware of the sale of a contract or a company subject to FOCI must report this information to the servicing Wing Information Protection Office. (T-1)

5.2.1.4. REVISED from 5.2.2.2. Information Protection offices will relay this information to SAF/AAZ through IP channels. (T-1)

5.2.2.1. Program/project manager, contracting office, becoming aware of the sale of a contract or a company subject to FOCI must report this information to the servicing Wing Information Protection Office. (T-1)

5.2.2.2. Information Protection offices will relay this information to SAF/AAZ through IP channels. (T-1)

5.3. Reporting Adverse Information and Suspicious Contacts . Actions or behaviors which may cause question of an employees trustworthiness, reliability, or judgment concerning their access to classified information are considered Adverse Information. Personnel working with or near classified information are possible targets of persons our contry's adversaries or even those with a casual interest in national defense. Reporting suspicious contacts assist in safeguarding

critical defense information. Visitor Groups and cleared facilities report these occurrences to the Information Protection office. This reporting requirement will be specified in the VGSA. (T-0)

5.3.1. Identify the contractor employee(s) involved, include the company name (identify prime contractor, if a subcontractor), address, and CAGE Code, the contract number and delivery order, if applicable.

5.3.2. Cleared facilities report occurences to the Wing Information Protection Office. (T-1)

5.3.3. The Wing Information Protection Office will:

5.3.3.1. Notify other AF activities, e.g., contracting office, Air Force Office of Special Investigations (AFOSI), when appropriate. (T-1)

5.3.3.2. Report information to the visitor group's Home Office Facility (HOF) through the Contracting Officer. (T-1)

5.3.3.3. The servicing Wing Information Protection Office will retain a copy of any adverse information or suspicious contact reports in accordance with Air Force Records Management standards. (T-1)

5.3.3.4. HOF performs any subsequent or additional reporting required by the NISPOM.

5.4. Reporting Security Violations.

5.4.1. Reference AFI 16-1404 for inquiry/investigation/reporting requirements occurring on an installation. Identify the contractor employee(s) involved, include the company name (identify prime contractor, if a subcontractor), address, and CAGE Code, the contract number and delivery order, if applicable. Visitor groups will report violations through their unit to the Wing Information Protection Office. Cleared facilities report directly to the Wing Information Protection Office. The Wing Information Protection Office reports security violations to the HOF for cleared facilities. When contractors cause security incidents on AF installations, Wing Information Protection Office (IP) will notify the contractor's Facility Security Officer (FSO) and Contracting Officer. (T-1)

5.4.2. Program/project managers will respond to the DSS requirements and provide the Wing Information Protection Office a copy of the response. (T-0) Original Classification Authorities are responsible for conducting damage assessments. See DoDM 5200.01, Vol 3, Enclosure 6.

5.4.2.1. These are cases of external Security Violation processing. The AF receives notice of security violations occurring at an industry concerning information an AF program or project manager uses is at risk or has been compromised. Specifc instructions are provided for each occurrence.

5.5. Reporting Espionage, Sabotage, and Subversive Activities. Suspicious activities may extend beyond the AF and endanger the defense industrial framework of our nation and its governing principles. When this occurs external government investigative agencies may need to be notified.

5.5.1. To expedite notifications, Visitor Groups and cleared facilities report these incidents directly to both the Wing Information Protection Office and AFOSI. The report should identify:

5.5.1.1. The Visitor Group or cleared facility.

5.5.1.2. All person(s) involved to include full name, date and place of birth, social security number, local address, present location, position within the company, and security clearance. Adhere to Personal Identity Information guidelines.

5.5.1.3. Any past or present participation in special access programs (SAPs).

5.5.1.4. Facts of the incident (who, what, when, where, why, and how).

5.5.1.5. Level of classified information involved and description (document, material, equipment, etc.,).

5.5.1.6. Whether news media know about the incident and if so which one(s).

5.5.1.7. Culpable individuals, if known.

5.5.1.8. Changes in contractor procedures necessitated by the incident and any recommendations for change in the security program, which may prevent similar violations.

5.5.2. Protect and mark reports containing personal identifiable information or any other exemption under the Freedom of Information Act (FOIA) as For Official Use Only (FOUO) in accordance with DoD 5200.01, Volume 4. (T-0)

5.5.3. The Wing Information Protection Office will ensure that the MAJCOM/DRU is notified. Include the servicing Public Affairs for incidents of information released to the media. (T-1)

5.5.3.1. Include a copy of any reports. (T-1)

5.5.3.2. Describe of any plans or action to safeguard and any recommendations to suspend or revoke an individual's personnel security clearance (PCL). (T-1)

5.5.4. AFOSI notifies external investigative agencies as required.

5.6. Invalidation of FCL. Invalidation of FCL renders a contractor ineligible to bid on new classified contracts or receive new classified material. If a Visitor Group or cleared facility loses their FCL the Wing Information Protection Office:

5.6.1. Notify SAF/AAZ through Information Protection channels. (T-0)

5.6.2. Instruct the contractor to return the classified material in its possession, unless otherwise directed. (T-0)

5.7. A company may encounter growth or other situations which present foreign ownership, control, or influence (FOCI) indicators. While not exclusive to program/project managers, they are in a position to observe and learn of information and conditions that may surface FOCI and play a critical reporting role that may result in a NID. Submit all (Collateral, SCI and SAP) NIDs in accordance with AFHB 16-1406**.**

5.7.1. **(DELETE)**

5.7.1.1. **(DELETE)**

5.7.1.1.1. **(DELETE)**

5.7.1.1.2. Top Secret access is required in the performance of the contract or any of the contract's supporting documentation. (T-0)

5.7.1.2. Identify the FOCI condition(s). FOCI applies if the company is:

5.7.1.2.1. **(DELETE)**

5.7.1.2.2. **(DELETE)**

5.7.1.2.2.1. **(DELETE)**

5.7.1.2.3. **(DELETE)**

5.7.1.3. Notify the Servicing Information Protection Office or the appropriate Special Security Office (SSO) or MAJCOM SAP Management Office for further guidance on NIDs (Collateral, SCI and SAP) processing respectively. (T-0)

Chapter 6

OVERSIGHT REVIEWS

6.1. Conducting Security Reviews (SRs) at Cleared Facilities: (NOTE: As used in this publication the term "security review" is not synonymous with nor does it negate the "security and policy review" requirement of AFI 35-101, *Air Force Public Affairs Policies and Procedures*.)

6.1.1. The Wing Industrial Security Specialist will conduct annual security reviews of cleared facilities that perform classified work on AF installations when the Installation Commander retains oversight responsibilities. (T-1)

6.1.2. Scheduling Security Review. Provide contractor activity management 30 days advanced written notification. (T-0)

6.1.3. Industrial security specialist coordinates with other AF security discipline OPRs; Operations Security (OPSEC), Computer Security (COMPUSEC), and Communications Security (COMSEC), etc., to provide specialized expertise when necessary to complete a security review. The servicing host-installation Cyber-security (formerly information assurance) official will participate in security reviews of cleared facilities when the cleared facility has systems/networks that process classified or controlled unclassified information. (T-0) The security review is complete when all security requirements imposed under the terms of the contract have been evaluated.

6.1.4. Post-Security Review Requirements.

6.1.4.1. Send a letter/report to senior management officials of the cleared facility within 10 days of completing the security review. The letter will:

6.1.4.2. Confirm the assessment of the contractor security program as discussed during the exit interview. (T-0)

6.1.4.3. List any deficiencies requiring corrective action. (T-0)

6.1.4.4. , Request written confirmation be provided within 30 days of the deficiencies, remedy, and status of any open major discrepancy (condition which resulted in or could reasonably be expected to result in the loss or compromise of classified information). (T-0)

6.1.5. Unsatisfactory Security Review.

6.1.5.1. The industrial security specialist assigns a cleared facility an unsatisfactory security review rating:

6.1.5.1.1. If the cleared facility fails to satisfactorily perform contractual security responsibilities. (T-0)

6.1.5.1.2. When major failures in the contractor security program have resulted in or could reasonably be expected to result in loss or compromise of classified information. (T-0)

6.1.5.1.3. When the contractor is clearly responsible for the security problems cited during a security review. (T-0)

6.1.5.2. The industrial security specialist coordinates with the contracting officer when assigning an unsatisfactory security review rating for a cleared facility. (T-0)

6.1.5.3. The HOF for the cleared facility is ultimately responsible for meeting contract security requirements.

6.1.5.3.1. When assigning an unsatisfactory security review rating, the industrial security specialist notifies the HOF immediately through the contracting office and requests prompt and complete corrective action.

6.1.5.3.2. Industrial security specialists notify HOF if problems continue. (T-1)

6.2. Self-Inspections and Self-assessments for Visitor Groups. Wings and sponsoring AF activities will include contractor visitor groups within their self-inspection and self-assessment programs; see AFI 16-1404. (T-1)

6.3. Security Discipline Assessment/Inspection Reciprocity. The CO, industrial security specialist, and other Wing (or installation security discipline offices) of primary responsibility (OPRs) work together to resolve issues pertaining to reciprocity, as applicable to assessments, surveys, audits, security clearances, security reviews, etc.

6.4. The program office, requiring AF activity or CO will notify the Wing industrial security specialist in writing within 30 days of when contract performance has been completed or terminated in order to schedule a close-out inspection. (T-0). Reference DoD 5220.22-R, * C4.3 for more information on close-out inspections."

Chapter 7

VISITS AND MEETINGS

7.1. Installation Visitors. The installation commander is the authority responsible for granting contractors access to the installation, regardless of which DoD agency, military service component, or activity awarded the contract.

7.2. Contractor Visits to AF Installations. DoD contractors located on or visiting AF installations in support of a classified contract must comply with DoD 5220.22-M, **Chapter 6**, Section 1, visit requirements. (T-0).

7.2.1. Verify the information/accesses are authorized via the DD Form 254 on the contract for which the information is being released to fulfill the contract. (T-0)

7.2.2. In the case of a subcontractor, review the subcontract DD Form 254. The Joint Personnel Adjudication System (JPAS) is the system of record for confirming classified access eligibility for DoD employees and all contractor personnel. (T-0)

7.3. AF Visits to Contractor Facilities. AF personnel who require access to classified information while visiting commercial contractor facilities must comply with the visit request submission requirements of DoD 5200.01, V1-4 and AFI 16-1404, DoD 5220.22-M, and/or the contractor location to be visited. (T-0).

Chapter 8

SPECIAL REQUIREMENTS

8.1. Special Access Program. The AF assumes cognizance (instead of DSS for oversight responsibility) of Special Access Program contracts. Program Security Officers (PSO) coordinate with the appropriate contracting officer (CO) and program manager (PM) to validate DD Forms 254 contain language indicating DSS is "carved out" of program oversight and identifies AF Office of Special Investigations, Office of Special Projects (AFOSI/PJ) as having security and compliance inspection responsibility in accordance with the NISP and AF authorities (T-0). In these cases, a DD Form 254 may be completed only after endorsement by a PM and PSO. (T-0) COs may not delegate the authority to approve a SAP DD 254 (for specific SAP guidance also see DoD 5220.22M-Sup 1, NISPOM Supplement, NISP, AFPD 16-7 and AFI 16-701, *Management Administration Oversight* of *Special Access Programs)*. Non-SAP classified material and CUI kept within a SAPF does not fall within the assessment (or self-assessment) purview of the industrial security specialist. Responsibility for such material rests with the applicable PSO (T-0).

8.2. Sensitive Compartmented Information. Program managers for SCI may relieve DSS and AF from security review and oversight responsibility for cleared facilities and/or visitor groups. This relief is normally limited to specific SCI information. Non-SCI classified material and CUI kept within a SCIF does not fall within the assessment purview of the Information Protection office. Responsibility for such material rests with the applicable SSO.

8.3. Other Access Considerations . The CO will engage program managers to validate a DD Form 254 requires access and adherence to other programs (e.g., Personnel Reliability Program (PRP), Restricted Data (RD), Critical Nuclear Weapons Design Information (CNWDI), Nuclear Command and Control Extremely Sensitive Information (NC2 ESI) and NATO. (T-0)

8.4. NATO . AF organizations will:

8.4.1. Ensure contracts requiring access to NATO classified materials is included on a DD Form 254 when applicable. (T-0) A NATO briefing will be completed prior to granting access to the Secure Internet Protocol Router Network (SIPRNet). Refer to AFI 16-1404 for granting personnel access to NATO information. (T-1)

8.4.1.1. Integrate their visitor group contractors into the servicing NATO control point security program. (T-0)

8.4.1.2. If NATO approved computer network or standalone system access is required, annotate the need on the DD Form 254. (T-0)

8.4.1.3. Ensure NATO access for employees are approved by the contractor company, to include providing initial briefings and debriefings. (T-0) This should be clearly stated in either the contract Statement of Work (SOW), DD Form 254, or VGSA.

8.4.1.4. Instructions and responsibilities for the protection of NATO material will be clearly stated in the DD Form 254 or VGSA. (T-0)

8.5. Controlled Unclassified Information (CUI):

8.5.1. Ensure local policies for awarding contracts and VGSA, include the requirement for security training and education in all contracts that require or will have access to classified or CUI. (T-0) See DoD 5200.1-M, Volume 4.

8.5.2. CUI will be marked in accordance with DoD 5200.01, Volume 4. (T-0)

8.5.3. NATO and material identified as foreign government information are not CUI.

Chapter 9

INTERNATIONAL SECURITY REQUIREMENTS

9.1. Categorizing Contractor Operations Overseas. DoD policy does not allow an FCL to be issued for contractors located outside the US, Puerto Rico, or a US possession or trust territory. Treat DoD contractor operations supporting the AF overseas as visitor groups.

9.2. Disclosure of Information to Foreign Visitors/Interests. Visits by foreigners to contractors performing on AF contracts (whether on or off base) which require access to classified or controlled unclassified information will be processed according to AFI 16-201, AF Foreign Disclosure and Technology Transfer Program. (T-1) Requests to disclose classified, controlled unclassified, and other types of information must be coordinated and approved by the servicing AF foreign disclosure office with the appropriate delegated disclosure authority. (T-1) Refer to AFI 16-201 for further information.

9.3. Documentary Disclosure of Information to a Foreign Entity. Contractors performing on AF contracts will submit requests for disclosure of classified or controlled unclassified information to the contracting officer. (T-1) The contracting officer will validate the need for disclosure and forward the request for information to the servicing AF foreign disclosure office with appropriate delegated disclosure authority. (T-0) The servicing AF foreign disclosure office will process the request in accordance with AFI 16-201. (T-1)

9.4. Foreign Visits. All visit requests to Visitor Groups or a Cleared Facility submitted by or on behalf of a foreign government must be processed through the installation and/or MAJCOM or DRU foreign disclosure activity, at least 30 days in advance of the intended arrival date. (T-1)

PATRICIA J. ZARODKIEWICZ
Administrative Assistant

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 33-360, *Publications and Forms Management*, 25 September 2014

AFPD 16-14, *Security Enterprise Governance,* July 24, 2014

DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM),* February 28, 2006

DoD 5220.22-R, *Industrial Security Regulation,* December 4, 1985

DoDM 5220.22-V3, *National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)*: 17 Apr 14

DoDM 5200.01-V1, *DoD Information Security Program,* February 24, 2012

DoDM 5200.01-V2, *DoD Information Security Program,* February 24, 2012

DoDM 5200.01-V3, *DoD Information Security Program,* February 24, 2012

DoD Manual 5200.01-V4, *DoD Information Security Program,* February 24, 2012

United States Security Authority for NATO Affairs (USSAN) 1-07, April 5, 2007

DFARS clause 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, December 16, 2014

AFMAN 33-363, *Management of Records*, March 1, 2008

AFI 31-401, *Information Security Program Management,* November 1, 2005

AFI 16-1404, *The Air Force Information Security Program,* 29 May 2015

AFI 35-101, *Air Force Public Affairs Policies and Procedures,* August 18, 2010

Subpart 204.404-70, *Defense Federal Acquisition Regulation Supplement* (DFARS),

August 17, 1998 as amended

DoD 5200.2-R, Personnel Security Program, December 6, 1986

Federal Acquisition Regulation Part 4, 4.1303, 52.204-9 Personal Identity Verification of Contractor Personnel, OMB Guidance M-05-24, August 5, 2005

AFI 33-115, *Air Force Information Technology (IT) Service Management*, September 16, 2014

The Joint Air Force - Army - Navy (JAFAN) 6/0, Special Access Program Security Manual,

Revision 1, 29 May 2008

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program,* July 23, 2014

AFMAN 31-113, *Installation Perimeter Access Control*, 2 February 2015

Prescribed Forms

None

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

DD Form 254, Department of Defense Contract Security Classification Specification

Abbreviations and Acronyms

ACO—Administrative Contracting Officer

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AIS—Automated Information System

CO—Contracting Office

COMSEC—Communications Security (COMSEC)

CSO—Cognizant Security Office

CUI—Controlled Unclassified Information

DOD—Department of Defense

DOE—Department of Energy

DRU—Direct Reporting Unit

DSS—Defense Security Service

FAR—Federal Acquisition Regulation

FBI—Federal Bureau of Investigations

FCL—Facility Security Clearance

FOA—Field Operating Agency

FOCI—Foreign Ownership, Control, or Influence

HOF—Home Office Facility

IT—Information Technology

JPAS—Joint Personnel Adjudication System

ISS—Industrial Security Specialist

NID—National Interest Determination

NISPOM—National Industrial Security Program Operating Manual

OPR—Office of Primary Responsibility

OPSEC—Operations Security

PCL—Personnel Security Clearance

PCO—Procuring Contracting Officer

PSO—Program Security Officer

PM—Program Manager

SAF—Secretary of the Air Force

SAP—Special Access Program

SAV—Staff Assistance Visit

SCI—Sensitive Compartmented Information

SOO—Statement of Objectives

SOW—Statement of Work

VGSA—Visitor Group Security Agreement

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 Agency (CSA).—Executive Branch Agencies authorized to establish an industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. Industry. These agencies are DoD, DHS, DOE, CIA, and NRC.

Cognizant Security Office—The designated Department of Defense (DoD) agency responsible for industrial security program administration. The Secretary of Defense (SedDef) has designated the Defense Security Service (DSS) to perform this function. The DSS Director has further delegated this responsibility downward within the agency. DSS Regional Directors provide industrial security administration for contractor facilities located within their respective geographic area. One exception for which AF has responsibility is DoD contractors on AF installations designated as "visitor groups."

Functional Office of Primary Responsibility (OPR)—Functional OPR examples are a SAF directorate, A-Staff, or squadron that manages a security discipline and its associated proscribed or collateral information/material/equipment. Examples are A/2 or local SSO office for SCI; SAF-CIO, A/6, or communications squadron for COMSEC; etc.

Industrial Security—the element of the security enterprise to ensure the safeguarding of

classified information when in the possession of U.S. industrial organizations, educational institutions, and organizations or facilities used by contractors.

Industrial Security Specialist—This AF position administers the industrial security program most commonly located on a Wing staff at an installation. The industrial Security Specialist is responsible for overseeing contractor security programs and/or operations through an executed (signed by both parties) VGSA.

Installation—An installation is an area in which the AF holds a real property interest or real property over which the AF has jurisdiction by agreement with a state or foreign government or by right of occupation. The term installation also includes all off-base or detached installations under the jurisdiction of the commander of the primary installation.

Intermittent Visitor—A contractor or company, cleared per the National Industrial Secutiy Program (NISP) or Industrial Security Regulation, that require "entry" to an AF 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 does not usually 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.

National Industrial Security Program Operating Manual (NISPOM)—DoD 5220.22-M establishes the standard procedures and requirements for all government contractors, with regards to classified information.

National Interest Determination—a determination that contractor access to proscribed information is consistent with the national security interests of the United States.

Proscribed Information—Proscribed information is Top Secret (TS); Communications Security (COMSEC) material, excluding controlled cryptographic items when unkeyed and utilized with unclassified keys; Restricted Data (RD); Special Access Program (SAP); and sensitive compartmented information (SCI).

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

Visitor Group—Any contractor operation, cleared per the NISP or Industrial Security Regulation that requires access to classified information (excluding a cleared facility). A contractor on an installation less than 90 days is categorized as an Intermittent Visitor and does not rquire a VGSA. The Installation Commander determines the categorization of the contractor operation based on the interaction with the serviced unit.

Visitor Group Security Agreement—The VGSA is installation and Wing specific and traces its existence to installation commander authority for allowing personnel to access a military installation; a documented and legally binding contractual agreement between an AF and a DoD contractor whereby the contractor commits to complying with, rendering, or performing specific security tasks or functions for compensation. The VGSA is different from, and in addition to the DD Form 441, **Department of Defense Security Agreement**, and DD Form 254, **DoD Contract Security Classification Specifications,** which are required.