BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-601

29 JUNE 2005

SCOTT AIR FORCE BASE Supplement

18 AUGUST 2006

Incorporating Change 1, 4 AUGUST 2011

Certified Current on 12 November 2013

Security

INDUSTRIAL SECURITY PROGRAM MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **Error! Hyperlink reference not valid.** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ USAF/XOS-F

Certified by: HQ USAF/XOS-FI (Brigadier General James M. Shamess)

Supersedes: AFI31-601, 22 November 2000

Pages: 37

(SCOTTAFB)

OPR: 375 SFS/SFA

Certified by: 375 SFS/CC (Capt Daniel T. Pempel)

Pages:3

This instruction implements Air Force Policy Directive (AFPD) 31-6, *Industrial Security*. It provides guidance for implementing the National Industrial Security Program. Use this instruction with DOD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, DOD 5220.22-R, *Industrial Security Regulation*, and DOD 5200.1-R, *Information Security Program Regulation* and changes thereto. Maintain and dispose of all records created as a result of processes prescribed in this instruction in accordance with the *WebRims Records Disposition Schedule.* HQ USAF/XOS-FI is delegated approval authority for revision of this AFI.

(SCOTTAFB) This supplement implements and extends the guidance of AFI 31-601, *Industrial Security Program Management*, 29 June 2005; provides a base-line requirement for managing the Industrial Security Program; applies to all 375th Airlift Wing-serviced Scott Air Force Base host and tenant units. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123 (will convert to AFMAN 33-

363), *Management of Records,* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/.** Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through the appropriate functional's chain of command.

SUMMARY OF CHANGES

This revision incorporates Interim Change 2005-1 and aligns this guidance with the revised Air Force Policy Directive (AFPD) 31-6, *Industrial Security*. Revisions include renumbering the chapters; updating office symbols and publication references; requiring the identification of government information and sensitive resources that require protection in classified contract documents; mandating the integration of on-base contractor operations into the installation information security program per AFPD 31-6; requiring the execution of a security agreement with contractors that perform contractual services on Air Force installations and require access to classified and gives installation commanders the discretionary authority to also require the execution of an security agreement with on-base contractors that require access to sensitive unclassified information or frequent "entry" to the installation; clarifying responsibilities and procedures for processing National Interest Determinations (NIDs); requiring a review of the DD Form 254, Contract Security Classification Specification, at two year intervals; requiring subcontractors that perform contractual services on Air Force installations to execute a Visitors Group Security Agreement (VGSA) when execution is required per this instruction; requiring contractors that use government information technology (IT) and automated information systems (AISs) to undergo a background investigation prior to IT usage; and eliminating the requirement to use the DD Form 696, Industrial Security Inspection Report. (NOTE: As used in this publication, the term "security review" is not synonymous nor does it negate the "security and policy review" requirement of AFI 35-101, *Public Affairs Policies and Procedures*. The term "sensitive unclassified information" refers to information identified in a classified contract that has been marked "For Official Use Only (FOUO)" per DOD 5200.1-R, Information Security Program, and is exempt from release under the Freedom of Information Act (FOIA)). A bar (|) indicates a revision from the previous edition. The entire text of the IC is at the last attachment.

(SCOTTAFB) This interim change updates the office of primary responsibility (OPR) and the following references: 375 SFS/CC to 375 AMW/IP; 375 Security Forces Squadron (375 SFS/CC) to Chief, Information Protection (375 AMW/IP); 375 AW to 375 AMW; physical security to Industrial Security; 375 SFS/SFO to 375 AMW/IPD; 375 SFS/SFA to 375 AMW/IP; and changes the approval authority signature block. Margin bar indicates newly revised material.

(SCOTTAFB) AFI 31-601, *Industrial Security Program Management*, is supplemented as follows: This supplement implements and extends guidance and provides a base-line requirement for managing the Industrial Security Program; applies to all 375th Air Mobility Wing-serviced Scott AFB host and tenant units. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/gcss-af61a/afrims/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's chain of command.

Chapter 1—GENERAL PROVISIONS AND REQUIREMENTS **5**

1.1. Policy. 5

1.2. Purpose. 5

1.3. Scope. 5

1.4. Submitting Interpretation and Waiver Requests. 5

1.5. Authority and Responsibilities. 5

1.6. Program Implementation and Administration. 6

1.7. Public Release of Information. 9

1.8. Reporting Requirements. 9

Chapter 2—SECURITY CLEARANCES **12**

2.1. Facility Security Clearances (FCLs). 12

2.2. Contractors with Foreign Ownership, Control or Influence (FOCI). 12

2.3. Contractor Personnel Security Clearances (PCLs). 13

2.4. Processing Trustworthiness Determinations. 14

2.5. Reciprocity. 14

Chapter 3—SECURITY TRAINING AND BRIEFINGS **15**

3.1. Security Training Requirements. 15

3.2. Security Briefing/Debriefing Requirements. 15

Chapter 4—SECURITY SPECIFICATIONS AND GUIDANCE **16**

4.1. Issuing Security Classification Guidance. 16

4.2. DD Form 254, Contract Security Classification Specifications. 16

4.3. Reviewing and Certifying the DD Form 254. 16

4.4. Distribution of the DD Form 254. 17

4.5. Visitor Group Security Agreement (VGSA). 17

Chapter 5—SAFEGUARDING **19**

5.1. Designation of On-Base Visitor Groups. 19

5.2. Integrated Visitor Group. 19

5.3. Cleared Facility. 19

5.4. Intermittent Visitors. 19

5.5. On-Base Contract Completion or Termination. 19

Chapter 6—OVERSIGHT REVIEWS AND REPORTING REQUIREMENTS 20

6.1. Conducting Industrial Security Reviews (SRs). 20

6.2. Conducting Information Security Program Reviews. 21

Chapter 7—VISITS AND MEETINGS 23

7.1. Installation Visitors. 23

7.2. Visitor Groups. 23

7.3. Contractor Visits to Air Force Installations. 23

7.4. Air Force Visits to Contractor Facilities. 23

Chapter 8—SUBCONTRACTING 24

8.1. Prime Contractor's Responsibilities. 24

8.2. Subcontractor Responsibilities. 24

Chapter 9—INFORMATION TECHNOLOGY (IT) AND AUTOMATED INFORMATED SYSTEM (AIS) SECURITY 25

9.1. Information Technology and Automated Information System Accreditation. 25

Chapter 10—SPECIAL REQUIREMENTS 26

10.1. Special Access Program. 26

10.2. Sensitive Compartmented Information. 26

Chapter 11—INTERNATIONAL SECURITY REQUIREMENTS 27

11.1. Procedures for Contractor Operations Overseas. 27

11.2. Disclosure of Information to Foreign Visitors/Interests. 27

11.3. Documentary Disclosure of Information to a Foreign Entity. 27

11.4. Foreign Visits. 27

Chapter 12—OTHER APPLICABLE SECURITY GUIDANCE 28

12.1. 28

12.2. Applicability of Other Security Program Requirements. 28

13.1. (Added-SCOTTAFB) Adopted Form: 28

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 29

Attachment 2—IC 2005-1 TO AFI 31-601, INDUSTRIAL SECURITY PROGRAM MANAGEMENT 33

Chapter 1

GENERAL PROVISIONS AND REQUIREMENTS

1.1. Policy. It is Air Force policy to identify in its classified contracts (DD Form 254, **Contract Security Classification Specification**) [DOD 5220.22-R] specific government information (regardless of classification, sensitivity, physical form, media or characteristics) and sensitive resources, which must be protected against compromise and or loss while entrusted to industry.

1.2. Purpose. This instruction implement Executive Order 12829, *National Industrial Security Program*, DOD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, and DOD 5220.22-R, *Industrial Security Regulation* (ISR) and AFPD 31-6, *Industrial Security*. It assigns functional responsibilities and establishes a system of review that identifies outdated, inappropriate and unnecessary contractual security requirements. It outlines and provides guidance for establishing on-base integrated contractor visitor groups.

1.3. Scope. The security policies, requirements and procedures identified in this instruction are applicable to Air Force personnel and on-base DOD contractors performing services under the terms of a properly executed contract and associated security agreement or similar document, as determined appropriate by the installation commander (IC).

1.4. Submitting Interpretation and Waiver Requests. Submit requests regarding the interpretation, clarification and/or waiving of requirements stipulated in Air Force Policy Directive (AFPD) 31-6, *Industrial Security* and this instruction through command Information Security Program Manager (ISPM) channels to HQ USAF/XOS-FI, 1340 Air Force Pentagon, Washington, D.C., 20330-1340.

1.5. Authority and Responsibilities.

1.5.1. The Secretary of Defense (SECDEF) is the Cognizant Security Agency (CSA) for the Department of Defense (DOD). The SECDEF has designated the Defense Security Service (DSS) as the Cognizant Security Office (CSO) for DOD. DSS oversees security for cleared contractor facilities located off-base and on-base when so requested by the installation commander, in writing.

1.5.2. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) is designated the Air Force Senior Security Official responsible for ensuring implementation of the Industrial Security Program.

1.5.3. Headquarters United States Air Force, Deputy Chief of Staff (DCS)/Air & Space Operations, Directorate of Strategic Security, Director of Security Forces and Force Protection, Information Security Division, (HQ USAF/XOS-FI) is responsible for industrial security policy development, interpretation, administration and program oversight.

1.5.4. The Assistant for Federal Acquisition Regulation (FAR) System, Deputy Assistant Secretary (Contracting), Assistant Secretary (Acquisition), (SAF/AQC) is responsible for formulating and interpreting contracting policy and issuing supplemental guidance to the FAR. The contracting office (CO) is responsible for coordinating contractual changes and modifications with Air Force contractors.

1.5.4.1. **(Added-SCOTTAFB)** Contracting Officers (CO) will notify the Industrial Security Manager anytime an active DD Form 254, *Contract Security Classification Specification, Department of Defense*, is amended. This action includes contract modifications, change of sensitivity level or contract extensions. All updated DD Forms 254 will be forwarded to the Chief, Information Protection (375 AMW/IP) for filing.

1.5.5. Headquarters United States Air Force, DCS/Air & Space Operations, Director of Intelligence, Surveillance and Reconnaissance (HQ USAF/XOI) is responsible for Sensitive Compartmented Information (SC) policy, when applicable to Air Force (AF) awarded contracts. Furthermore, AF/XOI is responsible for formulating policy and disseminating guidance pertaining to AFPD 10-11, *Operations Security (OPSEC)* requirements.

1.5.6. The Secretary of the Air Force, Warfighting Integration - Chief Information Officer, (SAF/XC), is responsible for formulating and oversee implementation of information technology (IT) security policy, and disseminating communications security (COMSEC) and emission security (EMSEC) guidance, when applicable to AF awarded contracts. SAF/XC also formulates and disseminates guidance pertaining to DOD Regulation 5400.7/AF Supplement, *Freedom of Information Act Program*. Referenced publication addresses the handling, marking and protection of sensitive unclassified and "For Official Use Only (FOUO)" information.

1.5.7. DELETED.

1.5.8. The Secretary of the Air Force, Office of Public Affairs, Security and Review Division (SAF/PAX), 1690 Air Force Pentagon, Washington DC 20330-1690, formulates policy and disseminates guidance pertaining to the clearance and release of information to the public, in any form.

1.5.9. The IC or designated designee is responsible for authorizing and/or granting DOD contractors access to the installation and for providing appropriate security supervision over the on-base contractor operation and its personnel.

1.6. Program Implementation and Administration.

1.6.1. The IC will:

1.6.1.1. Designate on-base contractor operations that require access to classified information as an intermittent visitor, visitor group, or cleared facility.

1.6.1.2. Execute a VGSA with all contractor operations located on Air Force installations that require or will have access to classified information. This provision may also be extended to include other contractors that perform contractual services on the installation and require or have access to sensitive unclassified information or those that require routine or infrequent "entry" to the installation in the performance of other types of contracts, services or maintenance.

1.6.1.3. Ensure NISPOM or equivalent security procedures are implemented for contractor operations supporting classified efforts within the confines of the installation.

1.6.1.4. Designate the installation ISPM (see AFI 31-401, Information Security Program Management) as the authority to perform industrial security program oversight for on-base contractor operations, unless unique or special operational circumstances warrant the use of the DSS.

1.6.1.4. **(SCOTTAFB)** The 375 AMW/IP is designated as the authority to perform industrial security program oversight for on-base contractor operations.

1.6.1.5. Ensure security reviews are conducted on those on-base contractor operations designated as a "cleared facility," when determined by the IC. In these instances, DSS must be notified that the Air Force will retain "security oversight" for the on-base contractor operations.

1.6.2. Air Force Activity (System, Program or Project Manager) will:

1.6.2.1. Initiate procurement requests and identify program unique security requirements in solicitations and contract documents.

1.6.2.2. Draft and incorporate program specific security classification guidance into the DD Form 254, **DOD Contract Security Classification Specification**.

1.6.2.2.1. **(Added-SCOTTAFB)** The Program Security Manager will maintain a copy of the current DD Form 254 to ensure all contractual access is not exceeded. All applicable DD Forms 254 will be reviewed and documented semiannually to ensure contract requirements are running according to prescribed deadlines.

1.6.2.3. Coordinate contractual security specifications with the contracting office and responsible security discipline, office of primary responsibility (OPR) or functional.

1.6.2.4. As a minimum, review and revise the classification/declassification security guidance every five years or as circumstances require.

1.6.2.5. Work in concert with the CO, ISPM, security program disciplines and/or functional OPRs to develop the VGSA.

1.6.3. Contracting Officers will:

1.6.3.1. Implement the NISPOM by incorporating specific security clauses into (classified/unclassified) contracts and solicitations as outlined in the Federal Acquisition Regulation (FAR) and supplementation thereto.

1.6.3.2. Negotiate all contractual agreements, modifications, changes and revisions with contractors.

1.6.3.3. Initiate and/or implement other actions as outlined in the FAR, DFARS, AFFARS, NISPOM and ISR relative to the administration of the industrial security program.

1.6.3.4. **(Added-SCOTTAFB)** The CO will ensure all completed DD Form 254s are forwarded to 375 AMW/IP immediately upon award of the contract. All units hosting a visitor group will maintain a copy of the DD Form 254 for accountability purposes and ease of contact.

1.6.4. The Defense Security Service (DSS) will accomplish the following tasks per DOD 5220.22-M, NISPOM and DOD 5220.22-R, ISR:

1.6.4.1. Administer the National Industrial Security Program (NISP) in accordance with national and DOD policy.

1.6.4.2. Establish and maintain a network of automated systems which provide real-time personnel security clearance (PCL) and facility security clearance (FCL) data on DOD contractors and their employees.

1.6.4.3. Assume industrial security program oversight responsibility for on-base cleared facilities at the request of the IC.

1.6.5. Information Security Program Manager (ISPM) will:

1.6.5.1. Oversee and administer the industrial security program on behalf of the IC.

1.6.5.2. Integrate on-base contractor operations into the installation Information Security Program in accordance with AFPD 31-6, para 7 and this instruction.

1.6.5.3. Review pre-award and/or draft solicitations, contract documents, security classification guides, and DD Form 254 to ensure appropriate security clauses and/or language is contained therein which address the protection of government information and sensitive resources.

1.6.5.3.1. **(SCOTTAFB)** As the Servicing Security Activity (SSA), the 375 AMW/IP will be invited and will attend all pre-contract/pre-construction briefings to facilitate the contract processes. 375 AMW/IP may be called upon to research technical data in regards to storage or classified handling procedures and will assist all units excluding United States Transportation Command, Headquarters Air Mobility Command and 126th Air Refueling Wing.

1.6.5.4. Serve as technical OPR for the development and preparation of the VGSA or other security agreements as determined necessary by the IC.

1.6.5.5. Maintain a folder on each on-base contractor for which a VGSA has been executed.

1.6.5.5. **(SCOTTAFB)** The 375 AMW/IP will maintain 6-part folders on each on-base contractor for which a Visitor Group Support Agreement (VGSA) has been executed. Folders will contain the DD Form 254, VGSA, contract point of contact information, visit requests, supporting documentation and any additional pertinent information. Program reviews and self-inspections will be maintained in the Information Security Program Folders for each applicable unit.

1.6.5.6. Conduct security oversight of an on-base designated “cleared facility” as determined by the IC. A designated on-base cleared facility operates under the security provisions and requirements of the NISPOM.

1.6.5.7. Ensure the contractor takes prompt corrective actions when security program deficiencies are identified and promptly report security violations and/or compromises.

1.6.5.8. Forward to DSS a copy of the security review and survey reports and other applicable documentation, which pertains to an on-base “cleared facility” per DOD 5220.22-M, DOD 5220.22-R, AFPD 31-6, and this instruction, if required.

1.6.5.9. Participate and/or provide input during the source selection process, incentive awards evaluation process, etc.

1.6.6. **(Added-SCOTTAFB)** Unit Security Managers (USM) whose unit hosts contractors with access to government Automated Information Systems (AIS) or classified information will maintain folders on these contracts. Additionally, any time the USM receives information or documentation regarding contractors meeting these criteria, they will notify the SSA within 3 duty days. Program reviews and self-inspections will be maintained in the Security Manager's Handbook.

1.6.6.1. **(Added-SCOTTAFB)** USMs whose unit hosts contractors with access to government AIS will maintain a Visitor Authorization Letter (VAL) or Joint Personnel Adjudication System (JPAS) person summary as proof that the contractor has the applicable background check before AIS access is granted. This documentation will be maintained in the Security Manager's Handbook as outlined in AFI 31-401_SCOTTAFBSUP1.

1.6.6.2. **(Added-SCOTTAFB)** USMs whose unit hosts contractors with access to their classified information and/or systems will maintain a separate folder containing the DD Form 254, VGSA, VAL (or JPAS person summary), contract point of contact information, visit requests, supporting documentation and any additional pertinent information.

1.7. Public Release of Information.

1.7.1. Contracting offices (COs) forward contractor's requests for public release of information relating to Air Force classified contracts or programs to the installation Public Affairs (PA) office. The PA office processes the request in accordance with AFI 35-101, *Public Affairs Policies and Procedures*, Chapter 15, Security and Policy Review and Chapter 18, News Media and Public Affairs.

1.7.1.1. Information requiring Air Force or DOD-level review will be forwarded by the entry-level 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. SAF/PAX forwards the requests, as required, to the Directorate for Freedom of Information and Security Review (DFOSIR), Washington Headquarters Service, Department of Defense, Pentagon, Washington DC 20301-1400.

1.7.2. When a contractor reports that classified information has appeared publicly, follow the guidelines in these documents: DOD 5200.1- R, *Information Security Program Regulation*; Air Force Policy Directive (AFPD) 31- 4, *Information Security*; and Air Force Instruction (AFI) 31- 401, *Information Security Program Management*

1.8. Reporting Requirements.

1.8.1. Reporting Adverse Information and Suspicious Contact Reporting.

1.8.1.1. On-base integrated visitor groups satisfy NISPOM adverse information and suspicious contacts reporting requirements by notifying or submitting the appropriate report or information to the ISPM through the AF activity they support. This reporting provision must be outlined in the visitor group security agreement (VGSA), when applicable. On-base designated "cleared facilities" make reports or submit information directly to the ISPM.

1.8.1.2. Upon receipt of information submitted per paragraph **1.8.1**, the ISPM will forward the report to the visitor group's Home Office Facility (HOF). Any subsequent or additional reporting required by the NISPOM to other federal agencies, e.g., CSA, CSO, Federal Bureau of Investigations (FBI), is thereafter the responsibility of the HOF.

1.8.1.3. The ISPM will retain a copy of the adverse information or suspicious contact report in the visitor group's files for 2 years.

1.8.1.4. The ISPM is responsible for notifying other AF activities, e.g., contracting office, Air Force Office of Special Investigations (AFOSI), when appropriate.

1.8.2. Reporting Security Violations.

1.8.2.1. A designated on-base "cleared facility" reports the loss, compromise, suspected compromise or other security violations pursuant to the NISPOM through the ISPM, who in-turn is responsible for notifying the CSO.

1.8.2.2. On-base integrated visitor groups report such incidents and/or information in accordance with AFI 31-401 to the ISPM via the AF activity security manager. This reporting requirement must be specified in the VGSA, if applicable. The commander of the AF activity being supported appoints an assigned federal employee (military or civilian) to conduct the preliminary inquiry in accordance with AFI 31-401, Chapter 9.

1.8.2.3. The CSO and ISPM report significant contractor security violations and compromises (resulting in actual loss or compromise) of classified information to the contracting officer.

1.8.3. **Reporting Espionage, Sabotage, and Subversive Activities.**

1.8.3.1. The ISPM reports espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media, involving cleared facilities or visitor groups located on Air Force installations to the servicing AFOSI. AFOSI coordinates with the FBI, as appropriate. The ISPM sends a report via secure communications (STU III or classified fax) with an information copy to each of the following activities:

1.8.3.1.1. Cognizant Security Office (CSO)

1.8.3.1.2. Functional Office of Primary Responsibility (OPR)

1.8.3.1.3. Headquarters United States Air Force, Information Security Division (HQ AF/XOS-FI)

1.8.3.1.4. Headquarters United States Air Force, Public Affairs (SAF/PA)

1.8.3.1.5. Appropriate Major Command (MAJCOM) Headquarters

1.8.3.2. Such a report should:

1.8.3.2.1. Identify the cleared facility or integrated visitor group involved.

1.8.3.2.2. Identify the contractor involved. Identify the person(s) involved, including the full name, date and place of birth, social security number, local address, present location, position with the contractor, security clearance (including past or present participation in any special access programs (SAPs), and a description of any plans or

action and any recommendations to suspend or revoke the individual's personnel security clearance (PCL).

1.8.3.2.3. Establish the known circumstances of the incident, including the identity of the classified material involved; any subsequent activities or circumstances (including whether and which news media know about the incident); and culpable individuals, where known.

1.8.3.2.4. Document when (time and date) the ISPM reported the incident to the AFOSI or when the CSO reported the incident to the FBI, if known.

1.8.3.2.5. Include a copy of any investigative reports.

1.8.3.2.6. Identify any changes in contractor procedures necessitated by the incident and any recommendations for change in the security program, which might prevent similar future violations.

1.8.4. The reporting requirement outlined in paragraph **1.8.3** is exempt from licensing with a report control symbol (RCS) IAW paragraph 2.11.1. of AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public and Interagency Air Force Information Collections*.

1.8.5. Reporting Loss, Compromise, and Possible Compromise.

1.8.5.1. ICs follow this instruction and perform actions as directed by DOD 5220.22-R, *Industrial Security Regulation*, to report the loss, compromise, or possible compromise of classified information for on-base contractor operations for which the Air Force has retained security oversight.

1.8.5.2. Contracting officers who learn of contractor loss, compromise, or possible compromise of classified information immediately notify the servicing ISPM and the Air Force functional office that has responsibility for the compromised information.

1.8.5.3. The original classification authority (OCA) or designated organization is responsible for determining whether a damage assessment is warranted and making any subsequent.

1.8.5.4. The OCA or designated organization notifies the Air Force activity, CSO, and/or the contractor of decisions to declassify, downgrade, or retain classification of the affected information. Do not give copies of damage assessment reports to the CSO or contractor operation.

1.8.5.5. Unless assistance is needed, do not notify the CSO of action begin taken to mitigate damage to national security.

1.8.5.6. Correspondence associated with or related to any such incidents should be handled between the CSO and/or ISPM and the affected Air Force activity direct.

1.8.5.7. When the seriousness of the incident warrants, the ISPM will provide a copy of the security incident investigation report to the CSO that has jurisdiction over the HOF.

Chapter 2

SECURITY CLEARANCES

2.1. Facility Security Clearances (FCLs).

2.1.1. Sponsoring FCLs. The contracting office (CO) is responsible for Facility Security Clearance (FCL) sponsorship. Defense Security Service is the authorizing agent for the FCL. DSS establishes and maintains all FCLs within the NISP. Also see DOD 5220.22-M, DOD 5200.2-R, *Personnel Security Program,* AFPD 31-5, *Personnel Security,* and AFI 31-501, *Personnel Security Program Management.*

2.1.1.1. To request an FCL sponsorship, write to the CSO with oversight responsibility for the sponsored facility.

2.1.1.2. Give the full name for the sponsored facility, its physical and mailing address, telephone number, and a specific point of contact at the facility, when known. Give the full name, job title, and direct-dial telephone number of the Air Force sponsor.

2.1.1.3. Establishing final FCLs through DSS may take several months. When circumstances do not permit such delays, sponsors may request an interim FCL through DSS.

2.1.2. Sponsoring Interim FCLs. DSS automatically processes all requests for Confidential and Secret FCLs for interim clearances when possible. However, Air Force sponsorship of interim Top Secret FCLs must be justified on a case-specific basis in accordance with DOD 5220.22-R. To request a Top Secret interim FCL, the CO prepares and routes sponsorships through command channels to the MAJCOM, FOA, or DRU commander for approval. Each request must include these items:

2.1.2.1. An explanation of why an interim Top Secret FCL would prevent a crucial delay in the award or performance of a classified contract.

2.1.2.2. A listing giving the legal name of the facility being sponsored, its complete street address, and the names and positions of people who are applying for interim Top Secret access authorization.

2.1.2.3. The address of the authorizing DSS.

2.1.3. Establishing FCLs. DSS establishes and maintains FCL for contractor operations participating in the NISP.

2.1.3.1. The ISPM with oversight responsibility for a cleared facility conducts required security reviews of the operation and assists the CSO, as necessary.

2.1.3.2. The ISPM also conducts surveys and/or administrative inquiries pertaining to an on-base cleared facility as requested by the CSO and ensures contractor compliance with DOD 5220.22- M, NISPOM.

2.1.3.3. Complete the survey by using the DD Form 374, **Facility Security Clearance Survey Data Sheet**, [DOD 5220.22-R], or an equivalent/acceptable automated format when conducting survey for an on-base cleared facility and forward a copy to the CSO.

2.2. Contractors with Foreign Ownership, Control or Influence (FOCI).

2.2.1. The CSO tells COs if a contractor performing on a classified contract has foreign ownership, control, or influence (FOCI) or whether it can be negated. Such influence might jeopardize the security of classified information held by the contractor.

2.2.2. To resolve a FOCI problem, the CSO may establish a facility clearance that limits the level and type of classified information to which a FOCI contractor has access. Such restrictions might affect ongoing, pending and future classified contracts with the contractor. The CO should discuss this impact with the ISPM and servicing Foreign Disclosure office.

2.2.3. The CO considers sponsoring a National Interest Determination (NID) after receiving written justification from the requesting program office or activity. This justification must address and explain how the FOCI contractor's product or service is crucial or is the sole available source to the AF. If applicable, the program or activity must also provide a written explanation when contract cancellation would cause unacceptable delays for mission-essential weapons systems in the field or for support organizations.

2.2.3.1. The requesting program office or activity is responsible for obtaining written release approval authority from the functional owner of the "proscribed information," prior to submitting the NID to the contracting office. The program office or activity contacts the OCA for Top Secret (TS), NSA for Communications Security (COMSEC), DCI for Sensitive Compartmented Information (SCI), and DOE for Restricted Data (RD) or Formerly Restricted Data (FRD) to obtain release approval. (**NOTE**: All release determination request (NID) involving/for SCI must be submitted to HQ USAF/XOIIS for review, coordination and processing).

2.2.3.2. The CO reviews, validates, and processes the NID and associated written approvals as follows:

2.2.3.2.1. Forward request for NID related to special access program (SAP) performance through the appropriate SAP and command channels to the Deputy for Security and Investigative Programs, Office of the Administrative Assistant (SAF/AAZ), 1720 Air Force Pentagon, Washington, D.C. 20330-1720 for approval.

2.2.3.2.2. Forward request for non-SAP NID through command ISPM channels to HQ USAF/XOS-FI for review and coordination. The NIDs are then be forwarded to SAF/AAZ for review and endorsement.

2.2.3.3. SAF/AA endorse the NID and forwards it to the Office of the Under Secretary of Defense for Counterintelligence and Security (OSD-USD/I), 5000 Defense Pentagon, Washington, D.C. 20301-3040, for final approval.

2.3. Contractor Personnel Security Clearances (PCLs).

2.3.1. The Defense Security Service grants and maintains contractor PCLs. DSS also terminates contractor PCLs when the contractor no longer needs them or when a contractor employee is terminated. Administrative termination of a PCL carries no adverse implications regarding the employee or the contractor.

2.3.2. The Directorate for Industrial Security Clearance Review, DOD Office of General Counsel, may suspend or revoke contractor PCLs following due process.

2.3.2.1. **(Added-SCOTTAFB)** 375 SFS/SFA will act as the liaison between contract individuals and the Air Force Central Adjudication Facility (AFCAF) when adverse

information is discovered during the course of security clearance background investigations. The 375 SFS/SFA does not handle Security Information Files for contractors; their company is forwarded the case from the AFCAF.

2.3.2.2. **(Added-SCOTTAFB)** Subjects of adverse investigations will provide all required information outlined in the suitability determination. All completed information will be routed through their servicing unit security manager or contract representative to 375 SFS/SFA for mailing.

2.3.2.3. **(Added-SCOTTAFB)** Subjects of suitability determinations will not contact 375 SFS/SFA or AFCAF on their own behalf. All coordination on suitability files will be exclusively routed through the servicing unit security manager.

2.3.3. DSS automatically processes all requests for Confidential or Secret PCLs for interim clearances, where possible.

2.3.4. When a contractor employee who is not cleared for access to Top Secret information needs such access to perform on an Air Force classified contract, the employing contractor may sponsor the individual for an interim Top Secret PCL.

2.3.4.1. The contractor should send requests to the CO who seeks concurrence of the system program office (SPO), system manager (SM), or program manager (PM).

2.3.4.2. The contractor's request should document clearly why the individual needs an interim PCL, why contract requirements may not be satisfied with another individual more suitably cleared, and what the potential adverse impact would be on contract performance if an interim PCL were not granted. The contracting officer will deny contractor requests that do not meet these criteria.

2.3.4.3. The CO routes the appropriate contractor's request for interim Top Secret PCLs to the MAJCOM, FOA, or DRU commander for approval.

2.3.4.4. The CO sends favorably endorsed requests to the contractor, who then includes the endorsement in the personnel security questionnaire package for transmission to DSS for action. The CO promptly returns denied requests.

2.4. Processing Trustworthiness Determinations.

2.4.1. When contractors require *unescorted entry to restricted areas*, *access to sensitive unclassified information*, *access to government automated information systems (AIS)* and/ or *sensitive equipment*, not involving access to classified information, the contractor's personnel security questionnaire is processed by the sponsoring Air Force activity per DOD 5200.2-R and AFI 31-501.

2.5. Reciprocity. The CO, ISPM, and other installation security disciplines offices of primary responsibility (OPRs) work together to resolve issues pertaining to reciprocity, as applicable to inspections, surveys, audits, security clearances, security reviews, etc. Elevate reciprocity issues to the next higher level of command when they can not be resolved locally.

Chapter 3

SECURITY TRAINING AND BRIEFINGS

3.1. Security Training Requirements.

3.1.1. Air Force classified solicitations and/or contracts [Statement of Objectives (SOO), Statement of Work (SOW), Request for Bid (RFB), Request for Quote (RFQ), VGSA, etc.] may stipulate contractor compliance with and participation in pertinent Air Force, command and installation security training programs when performance or services will occur on an Air Force installation.

3.1.2. When specified in an executed VGSA, AFI 31-401, *Information Security Program Management*, security training requirements satisfy the NISPOM training provision for on-base integrated visitor groups. Other Air Force functionals and/or security discipline OPRs may use this training provision for operational efficiency, however the specific requirements must be identified in the VGSA.

3.1.2.1. **(Added-SCOTTAFB)** Unit security managers must ensure that integrated visitor group personnel receive security education training when given to unit members as part of the unit security education training program. Training topics should be tailored to meet the needs and requirements of the work performed to support the classified contract. Security education training must be documented.

3.1.3. When an on-base contractor operation is designated as a cleared facility, the ISPM will provide the initial facility security officer (FSO) briefing in accordance with the NISPOM and CSO guidance.

3.1.4. Air Force unit security managers or security officers will provide information security program training (initial, refresher and annual) and other security awareness support to integrated visitor groups. The AF activity, working in concert with the ISPM, will incorporate language into the VGSA, which requires visitor group personnel to attend and/or receive information security training per DOD 5200.1-R and AFI 31-401, Chapter 8. Unit security managers will ensure integrated visitor group personnel are included in their security education program.

3.2. Security Briefing/Debriefing Requirements.

3.2.1. Management officials of the on-base cleared facility visitor groups are responsible for ensuring their employees receive all required security briefings and debriefings as mandated by the NISPOM.

3.2.2. For integrated visitor groups, DOD 5200.1-R and AFI 31-401 security training requirements are equivalent to and satisfy the training requirements of NISPOM, where appropriate. On-base contractor management officials are responsible for ensuring their personnel's attendance and satisfying NISPOM documentation requirements.

3.2.3. The ISPM will invite on-base cleared facility, Facility Security Officers (FSOs) and/or security representatives, to the installation's information security manager meetings.

Chapter 4

SECURITY SPECIFICATIONS AND GUIDANCE

4.1. Issuing Security Classification Guidance.

4.1.1. The AF program, project, activity and contracting office (CO) implements NISPOM, DOD 5200.1-R, and installation security requirements through contract documents. Only COs can sign, modify or negotiate changes to contracts.

4.1.2. When a contractor requires access to classified information, the AF program, project or activity prepares the required DD Forms 254, **DOD Contract Security Classification Specifications**. The contractor should use the security requirements in this form to accurately estimate the cost of security measures. More detailed security requirements are specified in the statement of work (SOW), statement of objectives (SOO), performance work statement (PWS), Visitor Group Security Agreement (VGSA), etc.

4.1.3. The responsible AF program, project, or activity will identify (by title, functional OPR, and approval date), the specific security classification guidance or guides (SCGs) applicable to the contract in Block #13 of the DD Form 254. The AF activity/program will provide copies of the SCG to the contractor prior to the contract commencing.

4.2. DD Form 254, Contract Security Classification Specifications.

4.2.1. The AF program, project or activity prepares a *draft* DD Form 254 for each classified contract. When drafting the DD Form 254s, the program, project or activity will consult with the CO, ISPM and other installation security discipline or functional OPRs affected under the terms of the solicitation/contract to ensure accuracy. Once drafted, the *draft* DD Form 254 is forwarded to the CO for processing. The contractor should use the security classification/declassification specifications and other contractual security requirements listed in the DD Form 254 to accurately estimate the cost of security.

4.2.2. The CO reviews and coordinates the *draft* DD Form 254 with all affected security disciplines and functionals, as appropriate. This action ensures that approved security guidance is being provided to the contractor. Once the review has been completed, the requesting AF entity/activity incorporates the necessary changes and prepares and forwards an *original* DD Form 254 to the CO for subsequent approval and signing.

4.2.3. Prior to signing the *original* DD Form 254, the CO will verify that all affected security disciplines and/or functional OPRs have reviewed and coordinated on the *draft* DD Form 254. This review and coordination action will be recorded/annotated in Block 13 (office symbol, date and initial's of reviewer) of the *draft* DD Form 254. The CO will file and maintain a copy of the annotated *draft* DD Form 254 in the respective contract file. When SAPs are involved, coordinate draft and original DD Form 254 with the office responsible for SAP security oversight. Keep DD Form 254 for collateral programs and SAPs unclassified, whenever possible.

4.3. Reviewing and Certifying the DD Form 254.

4.3.1. The ISPM reviews the *draft* and *original* DD Form 254 to ensure that the security classification guidance is accurate, approved and appropriate. However, the ISPM only

annotates Block 13 of the *draft* DD Form 254. Other security requirements are incorporated into the SOW, SOO, PWS, VGSA, etc.

4.3.1. **(SCOTTAFB)** Initial DD Forms 254 will be reviewed by 375 AMW/IPD (Industrial Security) and 375 AMW/IP for compliance with base policy and procedures.

4.3.2. The AF program, project or activity reviews the DD Form 254 and applicable security classification/declassification guidance at least once every five years or as required, to ensure accuracy and currency. When changes are necessary, the contract will be modified, if appropriate and revised guidance issued.

4.3.3. The CO certifies (signs) the DD Form 254, Block 16e. At the CO discretion, this authority may be delegated (in writing) as authorized by the Federal Acquisition Regulations (FAR) or supplementation thereto.

4.4. Distribution of the DD Form 254.

4.4.1. When DSS is relieved of security oversight responsibility for cleared facilities performing on SCI or SAP programs, furnish Headquarters DSS, 1340 Braddock Place, Alexandria VA 22314- 1651, a copy of the DD Form 254.

4.4.2. When a contractor's performance will be on Air Force installation, the AF program, project or activity must identify/specify all contract performance locations, if known, on the DD Form 254. When the contract is performed elsewhere, the CO will provide a copy of the signed DD Form 254 to that location's ISPM.

4.4.3. Procuring Contracting Officers (PCOs), their designated representatives, including Administrative Contracting Officers (ACOs), distribute DD Form 254.

4.5. Visitor Group Security Agreement (VGSA).

4.5.1. Execute a VGSA with all contractor operations located on Air Force installations that will require access to classified information. At the IC's discretion, the VGSA execution requirement may be extended to contractors performing on contracts that require access to sensitive unclassified information, sensitive resources or frequent "entry" to the installation.

4.5.2. The installation ISPM, security disciplines and functional OPRs work in concert with the AF program, project and/or activity to develop the Visitor Group Security Agreement (VGSA) requirements. The requirement to execute a VGSA is in addition to preparing the DD Form 254.

4.5.3. The VGSA must address those security requirements and/or procedures that are unique to the *installation* for which the contractor will be held contractually liable. VGSAs need only address those areas of security, safeguarding and/or protection that have not been covered elsewhere within the contract, DD Form 254, SOW, SOO, PWS, etc.

4.5.4. The ISPM is the technical OPR for development and preparation of the VGSA. For coordination purposes, the ISPM routes the VGSA to all *installation* security discipline OPRs and/or other agencies lending expertise to the contractual security requirements.

4.5.5. The ISPM signs the VGSA on behalf of the installation commander. The ISPM forwards a copy of the executed/signed VGSA to the contracting officer who awarded the contract or to the contracting officer's designated representative, when appropriate.

4.5.6. An authorized company official shall sign the VGSA. The CO will file a copy of the authorization with the contract.

Chapter 5

SAFEGUARDING

5.1. Designation of On-Base Visitor Groups. The IC works in concert with the Air Force activity, CO and ISPM to determine the designation of an on-base visitor group (cleared facility, integrated visitor group or intermittent visitor).

5.2. Integrated Visitor Group.

5.2.1. Integrated visitor groups operate in accordance with DOD 5200.1-R and supplemental guidance thereto. They handle, generate, process, and store classified information per AF guidance. The exception being, their "access" is limited to "need-to-know" contract-specific classified performance information.

5.2.2. The AF must stipulate the specific DOD 5200.1-R and supplemental guidance, which is applicable under the terms of the executed VGSA.

5.2.3. The guidance conveyed to on-base contractor operation via the VGSA is limited to the AF installation and the AF solicitation/contract which it was executed to support. All other NISPOM mandated security requirements not addressed or specifically exempted by the executed VGSA or other contracting document must be implemented by the contractor.

5.2.4. The VGSA must clearly reflect that the Air Force is accountable for and controls all classified information. Integrated contractor visitor groups are prohibited from establishing separate classified information controls. (NOTE: Integrated visitor group personnel *can not* be appointed as primary or alternate security managers for AF activities. However, they can be required (via the VGSA) to provide other security program support, under AF direction, such as, conducting end-of-day security checks, security training/briefings, etc.).

5.3. Cleared Facility. An on-base cleared facility operates under the security mandates and requirements of the NISPOM. See AFPD 31-6 for further guidance regarding their establishment.

5.4. Intermittent Visitors. Intermittent visitors may operate under the security requirements of the NISPOM or the installation security program. The IC makes this determination after considering the intermittent visitor's relationship and interface with the AF activity and/or installation.

5.5. On-Base Contract Completion or Termination. The program, project or AF activity will notify the ISPM in writing when the contractual services and/or performance has been completed or terminated.

5.5.1. **(Added-SCOTTAFB)** When feasible, a 90-day or immediate notification will be made to 375 SFS/SFA serving formal notice of the closure of an industrial/classified contract. Upon notification, the industrial security manager will schedule a final inspection of the area and provide a final report for the contract holder.

Chapter 6

OVERSIGHT REVIEWS AND REPORTING REQUIREMENTS

6.1. Conducting Industrial Security Reviews (SRs).

6.1.1. Industrial Security Reviews. The ISPM conduct security reviews (SRs) of on-base cleared facilities that performs classified work on Air Force installations. Such SRs evaluate the contractor's compliance with contract specific-security requirements and pertinent DOD and Air Force security instructions.

6.1.2. Scheduling Industrial Security Reviews. Conduct (SRs) of on-base cleared facilities per DOD 5220.22-M and DOD 5220.22-R. Unless conducting an unannounced security review on a cleared facility, provide contractor activity's management 30 days advanced written notification.

6.1.3. Performing Industrial Security Reviews. ISPMs coordinate with other Air Force security discipline OPRs such as; Operations Security (OPSEC), Computer Security (COMPUSEC) and Communications Security (COMSEC), to provide specialized expertise when necessary to complete a security review. The SR is complete when all security requirements imposed under the terms of the contract have been evaluated.

6.1.3.1. When SRs are conducted for cleared facilities, provide copies of completed SR report, with all related correspondence, to the CSO. Use DSS' automated format to document the results of the SR. Contact HQ USAF/XOS-FI to obtain a copy of the automated DSS format.

6.1.3.2. Facility security clearance (FCL) files must contain all key documentation prescribed by DOD 5220.22- R and the CSO, to include DD Form 254 and related contract security requirement documents.

6.1.4. Post- Industrial 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 should:

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

6.1.4.3. List any deficiencies requiring corrective action.

6.1.4.4. Within 30 days, request written confirmation on the 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).

6.1.4.5. The ISPM may extend the time for corrective action if required changes are significant and the contractor is making a conscientious effort to resolve problems expeditiously.

6.1.5. Unsatisfactory Industrial Security Reviews.

6.1.5.1. The ISPM assigns an on-base cleared facility an unsatisfactory SR rating:

6.1.5.1.1. To a cleared facility visitor groups if it fails to satisfactorily perform its contractual security responsibilities.

6.1.5.1.2. When major failures in the contractor's security program have resulted in or could reasonably be expected to result in the loss or compromise of classified information.

6.1.5.1.3. When the contractor is clearly responsible for the security problems cited during a security review.

6.1.5.1.4. The ISPM coordinates with the CSO and contracting officer when assigning an unsatisfactory SR rating for an on-base cleared facility.

6.1.5.1.5. The home office facility (HOF) for the cleared facility is ultimately responsible for meeting contract security requirements. When assigning an unsatisfactory SR rating, the ISPM notifies the HOF immediately through the contracting office and requests prompt and complete corrective action. If the HOF fails to take corrective action, its security clearance may be affected. The servicing security activity should notify the HOF's CSO if problems continue.

6.1.6. Invalidating the Facility Security Clearance (FCL).

6.1.6.1. The CSO notifies the contracting officers in writing when the FCL of a contractor under their jurisdiction is invalidated.

6.1.6.2. A contractor who fails to correct security deficiencies that subsequently results in invalidation may lose its FCL.

6.1.6.3. Although most contractors resolve invalidations promptly, contractors with foreign owned, controlled, or influence (FOCI) invalidations may have to wait for many months. Where FOCI is evident, the facility clearance may remain invalidated for more than a year while methods to resolve the FOCI are considered, approved, and implemented. The FCL is invalidated while DSS negotiates voting trusts, proxy agreements, or special agreements with foreign interests.

6.1.6.4. Document SR for an on-base cleared facility as required by the DOD 5220.22-M, DOD 5220.22-R, and CSO guidance. Keep copies of completed SR reports with pre-security review letter and completed post- review correspondence for 2 years from the date of the most recent SR.

6.1.6.5. Maintain copies of self-inspection reports or reviews for 2 years from date of the most recent self-inspection.

6.2. Conducting Information Security Program Reviews.

6.2.1. Information Security Program Reviews. On-base integrated visitor groups will be evaluated and conduct self-inspections collectively with the AF activity per DOD 5200.1-R and AFI 31-401, guidance. Integrated visitor groups will not be subjected to the SR requirements of the NISPOM. The installation prescribes the report for documenting program reviews.

6.2.2. Scheduling Information Security Program Reviews. Schedule program reviews per DOD 5200.1-R and AFI 31-401 guidance.

6.2.3. The AF activity is responsible for ensuring its integrated visitor group implement and comply with DOD 5200.1-R and AFI 31-401 requirements.

6.2.4. The ISPM, unit security manager and integrated visitor group establishes files and maintain the following documentation, as appropriate:

6.2.4.1. Signed copy of the DD Form 254 and any revisions.

6.2.4.2. Signed copy of the VGSA. (**NOTE**: Maintaining a copy of the VGSA is *optional* for the ISPM).

6.2.4.3. Current listing of the key on-base management officials or representatives.

6.2.4.4. Copy of the last annual program review.

6.2.4.5. Copies of last two self-inspections reports. The annual program review can be used to substitute for one of the self-inspections. (**NOTE**: The maintenance of self-inspection reports is optional for ISPMs).

6.2.4.6. DELETED.

6.2.5. For visitor groups, the ISPM briefs key Air Force and designated visitor group managers on the status of the unit's security program. Provide both parties a copy of the PR report and any other related assessment, survey or staff assistance visit (SAV) report. Do not furnish copies of these reports to the CSO.

6.2.5.1. When warranted, AF commanders notify the contractor's home office facility (HOF), in writing, through the contracting office of major security program deficiencies or non-compliance with the terms of the VGSA.

6.2.6. The ISPM will maintain files/records on each on-base integrated visitor group in accordance with paragraph **6.2.4**, this publication.

Chapter 7

VISITS AND MEETINGS

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

7.2. Visitor Groups. The IC designates contractors who require access to the installation in the performance of a government contract as intermittent visitors, integrated visitor groups, or cleared facilities.

7.3. Contractor Visits to Air Force Installations.

7.3.1. DOD contractors located on or visiting Air Force installations in support of a classified contract must comply with DOD 5220.22-M, Chapter 6, Section 1, visit requirements.

7.3.2. DELETED.

7.3.3. DELETED.

7.4. Air Force Visits to Contractor Facilities. Air Force personnel who require access to classified information while visiting non-DOD contractor facilities must comply with the visit request submission requirements of DOD 5200.1-R, DOD 5220.22-M, AFI 31-401 and/or the contractor location to be visited.

Chapter 8

SUBCONTRACTING

8.1. Prime Contractor's Responsibilities.

8.1.1. Prime contractors are responsible for ensuring their on-base subcontractors are knowledgeable of and comply with the applicable security requirements (NISPOM, installation, etc.) as identified in contracts and/or other contracting documents.

8.1.2. Prime contractors supporting classified efforts must include a provision in each on-base subcontract that requires subcontractors to contact the installation commander or designee and execute a VGSA prior to beginning on-base operations.

8.2. Subcontractor Responsibilities. On-base subcontractors must execute a separate and/or independent VGSA with the installation. (NOTE: As an alternative, when multiple subcontractor perform services in support of the same on-base classified contract and prime contractor, the execution of this VGSA, can be satisfied by the subcontractor acknowledging review and understanding of the security requirements identified in the prime contractor's executed VGSA. This being the case, executing and adding a signatory page *only* (attachment) to the prime's VGSA is acceptable).

Chapter 9

INFORMATION TECHNOLOGY (IT) AND AUTOMATED INFORMATED SYSTEM (AIS) SECURITY

9.1. Information Technology and Automated Information System Accreditation.

9.1.1. When industrial security program oversight is retained by the Air Force for on-base cleared facilities, the CO coordinates information technology (IT)/ automated information system (AIS) accreditation, Communications Security (COMSEC), and Emission Security (EMSEC) requirements with the responsible installation security discipline OPR, the ISPM and DSS, if appropriate.

9.1.2. Integrated visitor groups use approved Air Force IT/AIS and/or networks to process classified and sensitive unclassified information.

9.1.3. Contractor employees who require access to government IT/AIS under the terms of a government contract must be determined to be trustworthy by a designated government official prior to IT/AIS access being granted. Process all contractors IT/AIS access security background investigations in accordance with DOD 5200.2-R and AFI 31-501. This requirement must be specified in the basic solicitation and/or contract documents.

9.1.4. Contracts or solicitations (classified and unclassified) involving the use, operation, maintenance, etc., of IT/AIS will be routed through the installation Communications and Information (SC) activity for review and coordination.

Chapter 10

SPECIAL REQUIREMENTS

10.1. Special Access Program. For a carve-out contract, the Special Access Program (SAP) program manager assigns an Air Force element to perform security reviews and oversight. (Also see DOD 5220.22M-Sup 1, National Industrial Security Program Operating Manual (NISPOM) Supplement, and AFI 16-701, Special Access Programs.)

10.2. Sensitive Compartmented Information. Program managers for Air Force SAP and SCI programs may relieve the designated CSO and servicing security activity from security review and oversight responsibility for cleared facilities and/or visitor groups. Such relief normally will be limited to specific SAP and SCI information.

Chapter 11

INTERNATIONAL SECURITY REQUIREMENTS

11.1. Procedures for Contractor Operations Overseas. DOD policy does not allow an FCL to be issued for contractors located outside the US, Puerto Rico, or a United States possession or trust territory. Treat DOD contractor operations supporting the Air Force overseas as visitor groups.

11.2. Disclosure of Information to Foreign Visitors/Interests. Visits by foreigners to contractors performing on Air Force contracts (whether on or off base) that requires access to classified or controlled unclassified information will be processed through the Foreign Visits System IAW AFI 16-201. Approved visits will include disclosure authorization through the installation or servicing Air Force foreign disclosure office. Visits may be non-sponsored by the Air Force in which case the visit may take place but disclosure will be limited to information in the public domain or information covered by a valid export license issued by the Department of State IAW the Arms Export Control Act. Any disclosure of classified information must be on a government-to-government basis.

11.3. Documentary Disclosure of Information to a Foreign Entity. Contractors performing on Air Force contracts will submit request for documentary disclosure of classified or controlled unclassified information to the contracting officer. The contracting officer validates the need for disclosure and forwards the information to the installation or servicing foreign disclosure office which process the request IAW AFI 16-201

11.4. Foreign Visits. All visit requests submitted by or on behalf of a foreign visitor must be processed through the installation and/or MAJCOM foreign disclosure activity, at least 30 days in advance of the intended arrival date.

Chapter 12

OTHER APPLICABLE SECURITY GUIDANCE

12.1. Integrated visitor groups use existing Air Force security program related plans (Operations Security, Program Protection, Information Technology, etc.), procedures, operating instructions (OIs), 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.

12.2. Applicability of Other Security Program Requirements.

12.2.1. Coordinate security requirements, not stipulated in the NISPOM, with the responsible security discipline OPR and DSS, if applicable.

12.2.2. Functional specialists representing related security programs may accompany the ISPM or CSO representative during security reviews or when requested.

13.1. (Added-SCOTTAFB) Adopted Form: DD Form 254, *Contract Security Classification Specification, Department of Defense*.

NORMAN R. SEIP, Maj Gen, USAF
Acting DCS/Air & Space Operations

(SCOTTAFB)

*MICHAEL J. HORNITSCHEK, Colonel, USAF
*Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Executive Order 12829, *National Industrial Security Program,* 7 Jan 93

Executive Order 12958*, Classified National Security Information*, 20 Apr 95

DOD 5200.1-R, *Information Security Program*

DOD 5220.22-M, National *Industrial Security Program Operating Manual (NISPOM)*

DOD 5220.22-M-Sup 1, *National Industrial Security Operating Manual Supplement (NISPOMSUP*)

DOD 5220.22-R, *Industrial Security Regulation*

(Added-SCOTTAFB)

AFPD 10-11, *Operations Security*

AFPD 31-4, *Information Security*

AFPD 31-5, *Personnel Security Program Policy*

AFPD 31-6*, Industrial Security*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI 33-203, *Emission Security*

AFI 35-101 *Air Force Public Affairs Policies and Procedures*

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public and Interagency Air Force Information Collections*

AFH 31-602, *Industrial Security Program*

AFMAN 37-123, Management of Records

Abbreviations and Acronyms

ACO—Administrative Contracting Officer

(Added-SCOTTAFB) AFCAF—Air Force Central Adjudication Facility

AFH—Air Force Handbook

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

DSS-OCC—Defense Security Service - Operating Center Columbus

DOD—Department of Defense

DRU—Direct Reporting Unit

DSS—Defense Security Service

EMSEC—Emanation Security

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

(Added-SCOTTAFB) JPAS—Joint Personnel Adjudication System

MAJCOM—Major Command

NID—National Interest Determination

OPR—Office of Primary Responsibility

OPSEC—Operations Security

PCL—Personnel Security Clearance

PCO—Procuring Contracting Officer

PM—Program Manager

RFB—Request for Bid

RFP—Request for Proposal

RFQ—Request for Quote

SAF—Secretary of the Air Force

SAP—Special Access Program

SAV—Staff Assistance Visit

SCI—Sensitive Compartmented Information

(Added-SCOTTAFB) SFO—Physical Security

(Added-SCOTTAFB) SFS—Security Forces Squadron

SM—System Manager

(Added-SCOTTAFB) SPA—Information Security Program Manager

SPO—System Program Office

SOO—Statement of Objectives

SOW—Statement of Work

(Added-SCOTTAFB) SSA—Servicing Security Activity

(Added-SCOTTAFB) USM—Unit Security Manager

(Added-SCOTTAFB) VAL—Visitor Authorization Letter

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 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 ISPM has responsible, is DOD contractors on Air Force installation who have been designated as "visitor groups." When used, the language "Cognizant Security Office" (CSO), always refers to DSS or an entity thereof.

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

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

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 Air Force. The integrated visitor group is authorized to function in accordance with DOD 5200.1-R and AFI 31-401 per the VGSA. The Air Force 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 AF organization it supports.

Interim Facility Security Clearances (Interim FCL)—Interim FCL 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.

Intermittent Visitor—A contractor or company, cleared per the NISP or ISR, that require "entry" to an Air Force 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 ISPM 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 AFI. The IC assesses and evaluates the working relationship and interactions between the visitor group and AF activity to determining 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 an Air Force activity and a DOD contractor whereby the contractor commits to complying with, rendering or performing specific security tasks or functions for compensation. The VGSA attest to and certifies the existence of such an agreement, including applicable changes and amendments, attachments, supplements and exhibits.

Attachment 2

IC 2005-1 TO AFI 31-601, INDUSTRIAL SECURITY PROGRAM MANAGEMENT

29 JUNE 2005

This instruction implements Air Force Policy Directive (AFPD) 31-6, *Industrial Security*. It provides guidance for implementing the National Industrial Security Program. Use this instruction with DOD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, DOD 5220.22-R, *Industrial Security Regulation*, and DOD 5200.1-R, *Information Security ProgramRegulation* and changes thereto. Maintain and dispose of all records created as a result of processes prescribed in this instruction in accordance with the *WebRims Records Disposition Schedule.* HQ USAF/XOS-FI is delegated approval authority for revision of this AFI.

OPR: HQ USAF/XOS-F

Certification: HQ USAF/XOS-FI

SUMMARY OF REVISIONS

This revision incorporates Interim Change 2005-1 and aligns this guidance with the revised Air Force Policy Directive (AFPD) 31-6, *Industrial Security*. Revisions include renumbering the chapters; updating office symbols and publication references; requiring the identification of government information and sensitive resources that require protection in classified contract documents; mandating the integration of on-base contractor operations into the installation information security program per AFPD 31-6; requiring the execution of a security agreement with contractors that perform contractual services on Air Force installations and require access to classified and gives installation commanders the discretionary authority to also require the execution of an security agreement with on-base contractors that require access to sensitive unclassified information or frequent "entry" to the installation; clarifying responsibilities and procedures for processing National Interest Determinations (NIDs); requiring a review of the DD Form 254, Contract Security Classification Specification, at two year intervals; requiring subcontractors that perform contractual services on Air Force installations to execute a Visitors Group Security Agreement (VGSA) when execution is required per this instruction; requiring contractors that use government information technology (IT) and automated information systems (AISs) to undergo a background investigation prior to IT usage; and eliminating the requirement to use the DD Form 696, Industrial Security Inspection Report. (NOTE: As used in this publication, the term “security review” is not synonymous nor does it negate the “security and policy review” requirement of AFI 35-101, *Public Affairs Policies andProcedures*. The term "sensitive unclassified information" refers to information identified in a classified contract that has been marked "For Official Use Only (FOUO)" per DOD 5200.1-R, Information Security Program, and is exempt from release under the Freedom of Information Act (FOIA)). A bar (|) indicates a revision from the previous edition. The entire text of the IC is at the last attachment.

1.4. Submitting Interpretation and Waiver Requests. Submit requests regarding the interpretation, clarification and/or waiving of requirements stipulated in Air Force Policy Directive (AFPD) 31-6, *Industrial Security* and this instruction through command Information Security Program Manager (ISPM) channels to HQ USAF/XOS-FI, 1340 Air Force Pentagon, Washington, D.C., 20330-1340.

1.5.3. Headquarters United States Air Force, Deputy Chief of Staff (DCS)/Air & Space Operations, Directorate of Strategic Security, Director of Security Forces and Force Protection, Information Security Division, (HQ USAF/XOS-FI) is responsible for industrial security policy development, interpretation, administration and program oversight.

1.5.5. Headquarters United States Air Force, DCS/Air & Space Operations, Director of Intelligence, Surveillance and Reconnaissance (HQ USAF/XOI) is responsible for Sensitive Compartmented Information (SC) policy, when applicable to Air Force (AF) awarded contracts. Furthermore, AF/XOI is responsible for formulating policy and disseminating guidance pertaining to AFPD 10-11, *Operations Security (OPSEC)* requirements.

1.5.6. The Secretary of the Air Force, Warfighting Integration - Chief Information Officer, (SAF/XC), is responsible for formulating and oversee implementation of information technology (IT) security policy, and disseminating communications security (COMSEC) and emission security (EMSEC) guidance, when applicable to AF awarded contracts. SAF/XC also formulates and disseminates guidance pertaining to DOD Regulation 5400.7/AF Supplement, *Freedom of Information Act Program*. Referenced publication addresses the handling, marking and protection of sensitive unclassified and "For Official Use Only (FOUO)" information.

1.5.7. DELETED.

1.5.8. The Secretary of the Air Force, Office of Public Affairs, Security and Review Division (SAF/PAX), 1690 Air Force Pentagon, Washington DC 20330-1690, formulates policy and disseminates guidance pertaining to the clearance and release of information to the public, in any form.

1.6.2.4. As a minimum, review and revise the classification/declassification security guidance every five years or as circumstances require.

1.6.5.6. Conduct security oversight of an on-base designated "cleared facility" as determined by the IC. A designated on-base cleared facility operates under the security provisions and requirements of the NISPOM.

1.7.1.1. Information requiring Air Force or DOD-level review will be forwarded by the entry-level 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. SAF/PAX forwards the requests, as required, to the Directorate for Freedom of Information and Security Review (DFOSIR), Washington Headquarters Service, Department of Defense, Pentagon, Washington DC 20301-1400.

1.8.3.1.3. Headquarters United States Air Force, Information Security Division (HQ AF/XOS-FI)

1.8.5.7. When the seriousness of the incident warrants, the ISPM will provide a copy of the security incident investigation report to the CSO that has jurisdiction over the HOF.

2.1.1. Sponsoring FCLs. The contracting office (CO) is responsible for Facility Security Clearance (FCL) sponsorship. Defense Security Service is the authorizing agent for the FCL. DSS establishes and maintains all FCLs within the NISP. Also see DOD 5220.22-M, DOD 5200.2-R, *Personnel Security Program,* AFPD 31-5, *Personnel Security,* and AFI 31-501, *Personnel Security Program Management.*

2.1.1.3. Establishing final FCLs through DSS may take several months. When circumstances do not permit such delays, sponsors may request an interim FCL through DSS.

2.1.2. Sponsoring Interim FCLs. DSS automatically processes all requests for Confidential and Secret FCLs for interim clearances when possible. However, Air Force sponsorship of interim Top Secret FCLs must be justified on a case-specific basis in accordance with DOD 5220.22-R. To request a Top Secret interim FCL, the CO prepares and routes sponsorships through command channels to the MAJCOM, FOA, or DRU commander for approval. Each request must include these items:

2.1.3. Establishing FCLs. DSS establishes and maintains FCL for contractor operations participating in the NISP**.**

2.2.3.2.2. Forward request for non-SAP NID through command ISPM channels to HQ USAF/XOS-FI for review and coordination. The NIDs are then be forwarded to SAF/AAZ for review and endorsement.

2.2.3.3. SAF/AA endorse the NID and forwards it to the Office of the Under Secretary of Defense for Counterintelligence and Security (OSD-USD/I), 5000 Defense Pentagon, Washington, D.C. 20301-3040, for final approval.

2.3.1. The Defense Security Service grants and maintains contractor PCLs. DSS also terminates contractor PCLs when the contractor no longer needs them or when a contractor employee is terminated. Administrative termination of a PCL carries no adverse implications regarding the employee or the contractor.

2.3.4.4. The CO sends favorably endorsed requests to the contractor, who then includes the endorsement in the personnel security questionnaire package for transmission to DSS for action. The CO promptly returns denied requests.

4.2.1. The AF program, project or activity prepares a *draft* DD Form 254 for each classified contract. When drafting the DD Form 254s, the program, project or activity will consult with the CO, ISPM and other installation security discipline or functional OPRs affected under the terms of the solicitation/contract to ensure accuracy. Once drafted, the *draft* DD Form 254 is forwarded to the CO for processing. The contractor should use the security classification/declassification specifications and other contractual security requirements listed in the DD Form 254 to accurately estimate the cost of security.

4.2.2. The CO reviews and coordinates the *draft* DD Form 254 with all affected security disciplines and functionals, as appropriate. This action ensures that approved security guidance is being provided to the contractor. Once the review has been completed, the requesting AF entity/activity incorporates the necessary changes and prepares and forwards an *original* DD Form 254 to the CO for subsequent approval and signing.

4.2.3. Prior to signing the *original* DD Form 254, the CO will verify that all affected security disciplines and/or functional OPRs have reviewed and coordinated on the *draft* DD Form 254. This review and coordination action will be recorded/annotated in Block 13 (office symbol, date and initial's of reviewer) of the *draft* DD Form 254. The CO will file and maintain a copy of the annotated *draft* DD Form 254 in the respective contract file. When SAPs are involved, coordinate draft and original DD Form 254 with the office responsible for SAP security oversight. Keep DD Form 254 for collateral programs and SAPs unclassified, whenever possible.

4.3.1. The ISPM reviews the *draft* and *original* DD Form 254 to ensure that the security classification guidance is accurate, approved and appropriate. However, the ISPM only annotates Block 13 of the *draft* DD Form 254. Other security requirements are incorporated into the SOW, SOO, PWS, VGSA, etc.

4.3.2. The AF program, project or activity reviews the DD Form 254 and applicable security classification/declassification guidance at least once every five years or as required, to ensure accuracy and currency. When changes are necessary, the contract will be modified, if appropriate and revised guidance issued.

5.3. Cleared Facility. An on-base cleared facility operates under the security mandates and requirements of the NISPOM. See AFPD 31-6 for further guidance regarding their establishment.

6.1.3.1. When SRs are conducted for cleared facilities, provide copies of completed SR report, with all related correspondence, to the CSO. Use DSS' automated format to document the results of the SR. Contact HQ USAF/XOS-FI to obtain a copy of the automated DSS format.

6.2.4.6. DELETED.

7.3.2. DELETED.

7.3.3. DELETED.

7.4. Air Force Visits to Contractor Facilities. Air Force personnel who require access to classified information while visiting non-DOD contractor facilities must comply with the visit request submission requirements of DOD 5200.1-R, DOD 5220.22-M, AFI 31-401 and/or the contractor location to be visited.

Chapter 9 - INFORMATION TECHNOLOGY (IT) AND AUTOMATED INFORMATED SYSTEM (AIS) SECURITY

9.1. Information Technology and Automated Information System Accreditation.

9.1.1. When industrial security program oversight is retained by the Air Force for on-base cleared facilities, the CO coordinates information technology (IT)/ automated information system (AIS) accreditation, Communications Security (COMSEC), and Emission Security (EMSEC) requirements with the responsible installation security discipline OPR, the ISPM and DSS, if appropriate.

9.1.2. Integrated visitor groups use approved Air Force IT/AIS and/or networks to process classified and sensitive unclassified information.

9.1.3. Contractor employees who require access to government IT/AIS under the terms of a government contract must be determined to be trustworthy by a designated government official prior to IT/AIS access being granted. Process all contractors IT/AIS access security background investigations in accordance with DOD 5200.2-R and AFI 31-501. This requirement must be specified in the basic solicitation and/or contract documents.

9.1.4. Contracts or solicitations (classified and unclassified) involving the use, operation, maintenance, etc., of IT/AIS will be routed through the installation Communications and Information (SC) activity for review and coordination.

12.1. Integrated visitor groups use existing Air Force security program related plans (Operations Security, Program Protection, Information Technology, etc.), procedures, operating instructions (OIs), 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.