BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE HANDBOOK 31-602

1 FEBRUARY 1997

Security

INDUSTRIAL SECURITY PROGRAM

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ USAF/SPI (Mr Danny Green)

Certified by: HQ USAF/SP
(Brig Gen R. A. Coleman)
Pages: 91
Distribution: F

This handbook provides information and "how-to-guidance" for establishing and maintaining an effective Air Force Industrial Security Program. In addition, it provides helpful information on "best business practices" and "lessons learned." Recommend it be used in conjunction with Air Force Policy Directive 31-6**,** *Industrial Security*, Air Force Instruction 31-601, *Industrial Security Program Management*, DoD 5220-22-M, *National Industrial Security Program Operating Manual (NISPOM)* , and DoD 5220-22-R, *Industrial Security Regulation*. **Guidance offered by this handbook is suggestive, not directive in nature**. Forward inquiries, recommendations, and inputs to improve this handbook through command channels to HQ USAF/SPI, 1340 Air Force Pentagon, Washington D.C. 20330-1340.

Chapter 1

PROGRAM AUTHORITY, SCOPE, AND ADMINISTRATION

1.1. Introduction

1.1.1. Executive Order 12829 establishes the *National Industrial Security Program (NISP).* DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM),* DoD 5220.22-R, *Industrial Security Regulation (ISR),* and DoD 5220.22-M-Sup 1, *National Industrial Security Program Operating Manual Supplement (NISPOMSUP),* implement NISP requirements. The NISPOM establishes uniform security policies, practices, and procedures to ensure the proper safeguarding of classified information throughout industry.

1.1.2. The NISPOM implements applicable Federal statutes, executive orders, and national directives.

1.1.3. The NISPOM prescribes requirements, restrictions and other safeguards that are necessary to prevent the unauthorized disclosure of classified information and to control authorized disclosure of classified information by US Government Executive Branch Departments and Agencies to their contractors. The NISPOM replaces DoD 5220.22-M, *Defense Industrial Security Manual for Safeguarding Classified Information***,** January 1991.

1.1.4. The NISPOMSUP prescribes special security measures to ensure the integrity of Special Access Programs (SAPs), Restricted Data (RD), and Sensitive Compartmented Information (SCI), and imposes supplemental controls to those security requirements prescribed in the NISPOM.

1.1.5. Air Force Policy Directive (AFPD) 31-6, *Industrial Security*, implements E.O. 12829, *National Industrial Security Program*, DoD 5220.22-M, *National Industrial Security Program Operating Manual*, and DoD 5220.22-R, *Industrial Security Regulation*. Air Force Instruction (AFI) 31-601, *Industrial Security Program Management*, provides broad guidance necessary to implement the NISP, NISPOM and ISR uniformly, and this handbook addresses general "how to," "lessons learned," and "best business" practices.

1.2. Scope:

1.2.1. The NISPOM applies to all executive branch departments and agencies and to all DoD cleared contractor facilities located within the United States, its territories and possessions.

1.2.2. The NISPOM shall be used by DoD contractors to safeguard classified information released during all phases of the contracting, licensing, and grant process, including bidding, negotiation, award, performance, and termination.

1.2.3. The NISPOM also applies to classified information not released under a contract, license, certificate or grant, and to foreign government information furnished to DoD contractors that requires protection in the interest of national security.

1.2.4. The NISPOM prescribes **"baseline"** security standards for safeguarding collateral classified information. Imposing protection requirements more stringent than those prescribed by the NISPOM on contractor operations designated as "cleared facilities" is not authorized, nor will waivers or exceptions be granted. This provision does not apply to on-base contractors operating under the terms of a government/ contractor negotiated Visitor Group Security Agreement (VGSA).

1.2.5. The NISP encompasses all security disciplines, i.e., personnel, information, computer, physical, operations security (OPSEC), communications security (COMSEC), and emission security (EMSEC), to include international and special access program protection requirements.

1.3. Administration and Oversight:

1.3.1. The National Security Council (NSC) is responsible for providing overall policy for the NISP.

1.3.2. The Secretary of Defense (SECDEF) serves as the NISP "Executive Agent," and is responsible for overall program administration.

1.3.3. The Director, Information Security Oversight Office (ISOO), is responsible for implementing and monitoring the NISP and for issuing implementing direction that shall be binding in all federal agencies.

1.3.4. The Department of Defense (DoD), the Department of Energy (DoE), the Defense Nuclear Regulatory Commission (NRC), and the Central Intelligence Agency (CIA) jointly share NISPOM security cognizance and oversight responsibilities. These agencies have the authority to further delegate "security administration" type responsibilities internally or externally to another agency which will serve as that agency's "Cognizant Security Office" (CSO).

1.3.5. The Defense Investigative Service (DIS) is DoD's designated CSO and is responsible for overseeing implementation of NISPOM requirements for all off-base AF classified contracts.

1.3.6. The Air Force Chief of Security Police (HQ USAF/SP) has been delegated responsibility for formulating industrial security policy and providing broad program guidance and oversight.

1.3.7. The Air Force Chief of Security Police, Information Security Division (AF/SPI), is the Air Force focal point for policy development and program oversight of the AF Industrial Security Program.

1.3.8. At major command (MAJCOM) and installation level, security police units or a designated equivalent, manages, provides guidance, and oversees implementation of the installation's industrial security program.

1.3.9. The Assistant Chief of Staff for Intelligence, Plans, Policy, and Evaluation Directorate, HQ USAF/INX, is responsible for management of the Sensitive Compartmented Information (SCI) security program.

1.3.10. The Deputy Chief of Staff, Communications and Information, Director, Architectures and Technology (HQ USAF/SCT), is responsible for the information protection, communications security (COMSEC), computer security (COMPUSEC), and emission security (EMSEC) programs (formerly TEMPEST), as outlined in AFPD 33-2, *Information Protection*.

1.3.11. The Director of Plans, HQ USAF/XOX, is responsible for the Operations Security Program (OPSEC).

1.3.12. The Assistant Secretary (Contracting), SAF/AQC, is responsible for contracting policy and implementation.

Chapter 2

GENERAL PROGRAM RESPONSIBILITIES AND FUNCTIONS

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

2.1.1. The system, program, or project manager responsibilities are, but not limited to:

2.1.1.1. Initiating procurement requests and identifying and incorporating program unique industrial security requirements into contract documents.

2.1.1.2. Drafting and incorporating program specific security classification guidance into the DD Form 254, **DoD Contract Security Classification Specifications.**

2.1.1.3. Discussing contract and security requirements with the contracting office and responsible installation security discipline OPRs.

2.1.1.4. Reviewing, revising and modifying security classification guidance, as appropriate.

2.2. Contracting Officer Responsibilities:

2.2.1. MAJCOM and field level contracting offices implement the NISPOM by incorporating specific security clauses into classified contract documents as outlined in the Federal Acquisition Regulations (FAR), as supplemented by DoD and Air Force guidance.

2.2.2. The contracting officer negotiates all contractual agreements, modifications, changes, revisions, and is responsible for ensuring NISPOM implementation and contractor compliance.

2.2.3. The contracting officer coordinates all security requirements associated with classified contracts with the SSA and other installation security discipline OPRs or agencies, such as those responsible for computer security, emission security, foreign disclosure, information management, operations security, public affairs, etc.

2.2.4. Additional contracting officer responsibilities include, but are not limited to:

2.2.4.1. Incorporating any special security requirements into a contract, in addition to those identified in the NISPOM.

2.2.4.2. Initiating requests for Facility Clearance (FCL) action.

2.2.4.3. Authorizing release of classified information by contractors at seminars, meetings, and symposiums when authorization is required.

2.2.4.4. Authorizing retention of classified material by contractor.

2.2.4.5. Authorizing contractors to visit government activities and/or facilities in support of a specific classified work effort.

2.2.4.6. Reviewing and signing DD Form 254 and resolving security classification problems.

2.2.4.7. Advising the Cognizant Security Office (CSO) and Defense Technical Information Center (DTIC) upon completion or termination of classified contract.

2.2.4.8. Delegating specific responsibilities via letter, directive, supplement, memorandum of understanding (MOU), memorandum of agreement (MOA), to other government or AF activities, as appropriate, in support of NISPOM implementation.

2.3. Installation Commander Responsibilities:

2.3.1. Installation commanders derive their authority to control access (grant, limit, or deny) to the installation under Title 5, U.S.C., Title 10 U.S.C. 2.3.4.

2.3.2. The installation commander may deny a contractor employee access to the installation for cause. This action is considered separate and distinct from any PCL action. It is prudent, when making a recommendation to the commander or sending correspondence to a contractor or a contractor employee regarding the revocation of base access privileges, to avoid any reference to the individual's PCL, its status, or how it may be impacted.

2.3.3. The installation commander establishes and designates on-base contractor operations as cleared facilities, visitor groups, and/or intermittent visitors per authority of DoD 5220.22-R, *Industrial Security Regulation*, AFPD 31-6, *Industrial Security*, and AFI 31-601, *Industrial Security Program Management.*

2.3.4. DoD 5220.22-M**,** *National Industrial Security Program Operating Manual (NISPOM),* recognizes the installation commander's authority to establish installation security program requirements equivalent to NISPOM baseline security standards for contractors operating within the confines of the installation.

2.3.5. The installation commander designates an activity to perform industrial security program oversight for individual on-base contractor operations (Defense Investigative Service (DIS) or Servicing Security Activity (SSA). In most instances, this responsibility is entrusted to the installation security police or an equivalent on-base security activity.

2.3.6. The installation commander determines the frequency of security reviews for on-base contractors designated as visitor groups per AFI 31-601 guidance, to include approving the security review report format.

2.3.7. The installation commander authorizes the appropriate agency (CSO or SSA) to conduct security reviews for on-base contractors designated as cleared facilities in accordance with NISPOM requirements and in concert with the CSO.

2.3.8. The installation commander may designate other government or AF activities via letter, directive, supplement, MOA, MOU, etc., to perform specific duties in support of NISPOM implementation.

2.4. Defense Investigative Service (DIS) Responsibilities:

2.4.1. DIS has been designated by the Secretary of Defense (SECDEF) as the Cognizant Security Office (CSO) for the Department of Defense (DoD), including the military service components. DIS administers the National Industrial Security Program (NISP) in accordance with national and DoD policy. This responsibility extends to all cleared facility operations, regardless of their geographically location (on or off-base), except as specified in the NISPOMSUP. ***NOTE:*** As used in this handbook, the acronym "CSO" encompasses all DIS entities, i.e., headquarters, regional or field offices, centers and representatives.

2.4.2. DIS has three primary missions relevant to the National Industrial Security Program (NISP): (1) conducting personnel clearances (PCLs) investigations for contractors, (2) granting facility clearances (FCLs), and (3) providing industrial security program oversight for cleared facilities. This

agency is configured into a number of geographical regions, with each regional headquarters being responsible for those cleared contractor facilities falling within their respective jurisdiction.

2.4.3. DIS establishes and maintains a network of automated systems which provides real-time PCL/FCL data pertaining to contractor employees and facilities, to include intermittent visitors and/or visitor groups, although on-base oversight responsibility normally rests with the SSA. DIS's Personnel Investigative Center, Central Verification Activity (PIC-CVA), Baltimore MD, monitors, updates, and provides a PCL and FCL verification service.

2.4.4. DIS assumes industrial security program oversight responsibility for on-base cleared facilities at the request of the installation commander.

2.4.5. Only DIS has the authority to issue or terminate a contractor's PCL or FCL.

2.4.6. The CSO is responsible for and available to provide technical and quality control guidance to those SSAs having oversight responsibility for on-base cleared facilities.

2.4.7. The CSO is responsible for interpreting contractor submitted inquiries regarding NISPOM security requirements.

2.4.8. The CSO conducts security reviews for DoD contractor operations (cleared facilities) located off the installation and on occasions may be authorized to conduct security reviews for on-base cleared facilities, when determined appropriate by the installation commander.

2.5. Servicing Security Activity (SSA) Responsibilities:

2.5.1. At base level, the National Industrial Security Program is implemented by the installation commander via the contracting officer through a designated security activity, usually the installation security police unit or an equivalent security activity, and thereafter termed the "Servicing Security Activity" (SSA).

2.5.2. The designated SSA implements the industrial security program for the installation. This activity provides technical expertise, advice, and assistance to the installation commander, AF activities, contracting office, and other base entities regarding NISPOM requirements and their applicability. The SSA may be staffed by security police personnel or Department of the Air Force Civilian (DAFCs) security specialists, or a combination thereof.

2.5.3. The SSA may be responsible for other installation functions commonly associated with Security Police Administrations (SPA), i.e., information and personnel security, reports and analysis, and pass and registration, resources protection and crime prevention. Regardless of SSA's organizational home, its industrial security program responsibility remains unchanged.

2.5.4. The SSA provides industrial security program guidance and oversight for all visitor groups under the authority of the installation commander. This authority may extend to on-base cleared facilities, when determined appropriate by the installation commander.

2.5.5. The SSA coordinates and resolves contract security performance issues or problems via the contracting office for visitor groups. For on-base cleared facilities, the SSA consults with the CSO and contracting office when problems arise concerning contract security performance.

2.5.6. The SSA interacts closely (installation security focal point) with the Communications and Information, Intelligence, Public Affairs, Operations Security, International Affairs, and contracting activity to ensure appropriate and approved security measures and/or safeguards are implemented to

prevent the unauthorized disclosure or loss of classified or sensitive unclassified information. Base agencies identified below can provide expertise in the following areas:

2.5.6.1. Communications Unit - Information Protection (COMSEC, COMPUSEC, EMSEC, For Official Use Only (FOUO), and Privacy Act issues).

2.5.6.2. Intelligence Activity - SCI related matters, threat data, and counterintelligence.

2.5.6.3. International Affairs Activity - disclosure of U.S. classified information to foreign entities.

2.5.6.4. Public Affairs Activity - guidance on disclosure and/or release of USAF information to the general public.

2.5.6.5. Plans & Operations Activity - guidance on identifying operational weaknesses and suggested countermeasures to defend against intelligence collection efforts.

2.5.7. The SSA discusses and coordinates security performance issues with the contracting office, and when appropriate, the CSO. This same principle applies equally to contract modifications or revisions.

2.5.8. SSAs designated security oversight responsibilities for on-base cleared facilities, performs duties (surveys, security reviews, form completion or submission, etc.) per DoD 5220.22-R, in concert with the CSO.

2.5.9. Although not responsible for all security requirements identified in DD Form 254, the SSA is regarded by installation activities, acquisition community, and contracting office as the installation focal point for security guidance. Most security issues will be directed to the SSA for guidance or resolution. Security issues outside the scope of the SSA's responsibility should be immediately referred to the appropriate installation security discipline OPR.

2.6. DoD Contractor's Responsibilities:

2.6.1. Contractors participating in the National Industrial Security Program (NISP) execute a DD Form 441, **Department of Defense Security Agreement**, as an eligibility prerequisite. The DD Form 441, which is contractually imposed by Federal Acquisition Regulation (FAR) clause 52.204-2, Security Requirements, requires the contractor to establish and implement applicable portions of DoD 5220.22-M., *National Industrial Security Program Operating Manual (NISPOM).*

2.6.2. Under the terms of the DD Form 441, the contractor agrees to establish and comply with the applicable provisions of the NISPOM. Execution of the DD Form 441 gives DoD the authority to conduct periodic security reviews to verify compliance with the terms of the agreement and specific contract security requirements.

2.6.3. The DD Form 441 may be terminated by either the government or the contractor. However, termination of the security agreement is usually done by the government when a contractor is no longer active in the NISP, or no longer eligible for continued performance in the program, or has demonstrated an unwillingness to comply with the requirements of the agreement or pertinent security requirements.

2.6.4. The contractor's baseline source of industrial security guidance is the NISPOM which addresses the general security requirements contractually imposed on the contractor by the federal government. However, additional security requirements may be imposed by the Air Force at govern-

ment expense, provided they are consistent with DoD policy and are clearly identified in contracting documents.

2.6.5. The contractor's responsibilities are defined by the terms of a negotiated contract. The DD Form 254, **DoD Contract Security Classification Specification**, DD Form 441, **Department of Defense Security Agreement**, Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Standards (PWS), and/or Visitor Group Security Agreement (VGSA) identify those specific security requirements applicable to the contractor's performance.

2.6.6. Contractors are not subject to most Air Force policies or instructions, unless their compliance is mandated under the terms of a negotiated contractual agreement.

2.6.7. Contractors performing on a classified contract are required to sponsor those employees and consultants that require access to classified information. In addition, they are required to report any adverse information that may impact any cleared individual's eligibility to maintain a PCL to the CSO.

Chapter 3

TYPES OF DOD CONTRACTOR OPERATIONS

3.1. Cleared Facilities:

3.1.1. A cleared facility is a non-government owned or 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 access to classified information of a certain category (Confidential, Secret, or Top Secret).

3.1.2. On-base cleared facilities are established at the discretion of the installation commander, who decides whether the installation SSA or the CSO will have security oversight and responsibility for these designated contractor facilities.

3.1.3. Cleared facilities comply with and are subject to the requirements of the NISPOM, regardless of geographic location or responsible oversight agency.

3.1.4. The SSA oversee on-base cleared facility operations IAW DoD 5220.22-R, AFPD 31-6, and AFI 31-601 guidance.

3.1.5. On-base cleared facilities receive, store, dispatch, and process classified information under the provisions of the NISPOM, the exception being when and where unique operating conditions or circumstances dictates otherwise.

3.2. Visitor Groups:

3.2.1. A visitor group is a contractor operation located on an Air Force installation that requires access to classified information. It operates under the direct control of the Air Force. It differs from a cleared facility by its close interaction and/or working relationship with an Air Force organization. Normally, the visitor group operation is integrated into and directly supports the organization's mission. However, unlike a cleared facility, the visitor group does not have the capability to handle, process, or store classified information independent of the Air Force activity. It differs from an intermittent visitor primarily because of its long-term presence on an installation.

3.2.2. Visitor groups are established at the discretion of the installation commander under the authority of DoD 5220.22-R, AFPD 31-6 and AFI 31-601 to satisfy unique AF operational requirements. They are neither intermittent visitors nor cleared facilities. Typically, they are contractor operations which maintain a long-term presence on an Air Force installation and that have a very interactive relationship with the AF activity it is supporting. Technically, visitor groups function as extensions of the AF activity, operating under installation security program guidance and/or the AF activity's unit security operating instructions (OIs), or both. (See Figure 3.1).

3.2.3. Visitor groups may be authorized to operate in accordance with DoD 5200.1-R, *Information Security Program Regulation*, or the host installation security program. When so authorized, the specific security requirements applicable to the visitor group must be identified and clearly specified in the **Visitor Group Security Agreement (VGSA).** 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.

3.2.4. The VGSA outlines safeguarding requirements for both classified and sensitive unclassified information to be disclosed under the terms of the contract.

3.2.5. Visitor groups operating per DoD 5200.1-R/AFI 31-401 are not allowed to generate, receive, or store classified information independent of the AF activity. However, this is not the case for visitor groups operating under NISPOM guidance nor may it be the case for visitor groups operating under installation security program requirements.

3.2.6. Visitor groups, authorized to operate under the provisions of DoD 5200.1-R or installation security program, may function and operate under AF security program procedures, provided the AF maintains **control** of all classified information and the visitor group's access is limited to contract-specific information. ***NOTE:*** As used in this paragraph, "**control**" means stored in an AF owned security container, processed on AF owned equipment, transmitted via AF control requirements, and occurs at a location or facility over which the AF has jurisdiction.

3.2.7. Visitor group establishment is limited to areas or property over which the AF exercises jurisdiction. This includes auxiliary and detached installations.

3.2.8. Security program oversight responsibility for visitor groups rests with the designated SSA under the authority of the installation commander.

3.3. Intermittent Visitors:

3.3.1. The intermittent visitor can best be described as a cleared DoD contractor who may visit an AF installation on an infrequent basis for brief periods of time on a scheduled or on-call basis to perform contractual services or duties which requires access to classified information.

3.3.2. Typical intermittent visitors include, but are not limited to, telephone maintenance technicians, reproduction equipment and computer technicians, etc. Normally, the CSO provides industrial security program oversight for these types of visitors via their off-base home office facility (HOF).

3.3.3. The intermittent visitor's presence on a installation normally does not exceed 90 consecutive days.

Figure 3.1. Sample Unit Operating Instruction (OI).

(INSERT ORGANIZATION DESIGNATION) Operating Instruction 31-401

(INSERT UNIT DESIGNATION) (INSERT DAY, MONTH, YEAR)

INSERT INSTALLATION NAME & LOCATION)

Security

HANDLING, PROCESSING AND SAFEGUARDING CLASSIFIED HOLDINGS

PURPOSE: This operating instruction (OI) establishes procedures for the proper handling, processing, and safeguarding of classified material entrusted to or under the jurisdiction of the (INSERT UNIT/ OFFICE DESIGNATION). This OI is applicable to all government personnel (military and DoD civilians) assigned or attached, and those DoD contractors authorized under the terms of a signed Visitor Group Security Agreement (VGSA) to perform contract services under DoD 5200.1-R/AFI 31-401. Furthermore, it supplements DoD 5200.1-R, DoD 5220.22-M, DoD 5220.22-R, AFI 31-401, AFI 31-601, and other applicable security directives.

1.1. Responsibility:

1.1.1. Each person (government and DoD contractor) has a moral and legal obligation to protect classified material to ensure compliance with these procedures and to report any deviations.

1.1.2. The (INSERT COMMANDER OR AGENCY CHIEF DESIGNATION, AS APPROPRIATE) will appoint (in writing) a government official (primary) and at least one government or contractor official (alternate) to serve in the following information security program capacities. (*NOTE:* All primary security program officials required per DoD 5200.1-R/AFI 31-401 and this OI, must be government employees, i.e., unit security manager, safe custodians, etc.). The commander or agency chief will:

1.1.2.1. Appoint a unit security manager (USM) and at least one alternate. The USM will establish a security program as outlined in DoD 5200.1-R, AFI 31-401, and supplemental guidance thereto, to include overseeing and/or performing all associated duties and/or functions. The USM and/or alternate will also ensure government/contractor compliance with the applicable portions of DoD 5220.22-M, when and where appropriate.

1.1.2.2. Appoint Office Security Managers (OSMs), government or DoD contractor, as determined appropriate to assist the USM with security program implementation and management.

1.1.2.3. Appoint safe custodians (primary and at least one alternate for each security container).

1.1.2.4. Designate government official(s) to authorize reproduction of classified.

1.1.2.5. Designate government official(s) to conduct Foreign Travel Briefings.

1.1.2.6. Designate personnel (government and/or DoD contractor) to handcarry or escort classified material outside of duty location.

1.1.2.7. Appoint official(s) government and/or DoD contractor, to conduct the semiannual security inspections.

1.1.2.8. Appoint a government official to serve as primary Computer System Security Officer (CSSO) and at least one alternate (government or contractor).

1.1.2.9. Appoint government inquiry official(s) to investigate security incidents, when they occur.

2.1. References:

2.1.1. AFPD 31-4, *Information Security*

2.1.2. AFI 31-401, *Managing the Information Security Program*

2.1.3. AFI 31-501, *Personnel Security Program Management*

2.1.4. AFH 31-502, *Personnel Security Program Handbook*

2.1.5. AFPD 31-6, *Industrial Security*

2.1.6. AFI 31-601, *Industrial Security Program Management*

2.1.7. AFPD 33-2, *Information Protection*

3.1. Access:

3.1.1. Classified information will only be released to individuals (government or contractor) who possess a valid personnel security clearance equal to or greater than the information being disclosed (verify via ASCAS roster or visit authorization letter (VAL) with individual's organization or company), possess a valid need-to-know or required in performance of official duties, and have accomplished the SF 312, Classified Information Nondisclosure Agreement.

3.1.2. For government personnel, the requester's supervisor, USM or servicing security activity (SSA) or equivalent office can verify these elements for personnel requiring access. In addition, official government orders (PCS or TDY) may also be used to verify security clearance eligibility.

3.1.3. DoD contractors must be preannounced and approved by the (INSERT COMMANDER/AGENCY CHIEF OR DESIGNATED REPRESENTATIVE, AS APPROPRIATE) prior to access being granted. Verify visit authorization letter (VAL) authenticity by contacting the individual's home office Facility

Security Manager (FSO) or equivalent company representative, a government USM, or if applicable, the (INSERT DESIGNATION OF SERVICING SECURITY ACTIVITY) for on-base military, DoD civilian and/or contractors.

3.1.4. For DoD contractors, incoming VALs must be on company letterhead or stationary and signed by a company official other than the visitor(s). For additional information on visitor access refer to DoD 5200.1-R, DoD 5220.22-M or the installation's information security program supplement.

4.1. Safekeeping and Storage:

4.1.1. Classified material will be stored in GSA approved security containers (INSERT CONTAINER NUMBERS AND LOCATIONS). Classified material will be under the constant observation of an authorized individual (government or contractor) or secured in an approved security containers at all times. Emergency storage containers are (INSERT DESIGNATED EMERGENCY STORAGE FACILITY BY ACTIVITY DESIGNATION AND LOCATION).

4.1.2. High value items susceptible to theft will not be stored in security containers with classified material.

4.1.3. Classified cover sheets (AF Form 144, Top Secret Access Record and Cover Sheet, and SF Forms 704 and 705) will be attached to any classified document removed from a container, to include when the classified documents are handcarried outside the designated work area. (The cover sheet requirement does not apply to classified documents being entered into the Base Information Transfer System (BITS).

4.2. Custodian Responsibilities:

4.2.1. The primary and alternate safe custodian will be listed in the 1st & 2nd block of item #10 on the SF 700, Security Container Information, and will be responsible for:

4.2.2.1. Providing protection and controlling and/or accounting for all documents/material entered into the container.

4.2.2.2. Establishing and maintaining document suspense/receipt and destruction files as required.

4.2.2.3. Preparing and posting all required container documentation, such as, SF 700, Security Container Information, SF 701, Activity Security Checklist, SF 702, Security Container Check Sheet, and AFTO 36, Maintenance Record for Security Type Equipment.

4.2.2.4. Ensuring security container combination changes are made and preventative maintenance is performed by authorized personnel when required.

4.2.2.5. Ensuring combinations are protected and only distributed as dictated by agency needs.

4.2.2.6. Overseeing the continuous purging of administrative file systems containing classified information and the annual clean-out on (INSERT DESIGNATED CLEAN-OUT MONTH & DATE) of each year.

4.3. End-of-Day Security Checks: At the end of each duty day a complete check of all areas where classified is stored, handled, or processed will be accomplished. In addition, the clean desk policy will be in effect in these areas.

4.4. Administrative Requirements:

4.4.1. SF Form 702 will be posted on all classified security containers and annotated each time the container is opened and as a minimum annotated during the end-of-day security check. The notation "NOT OPENED" or a "line through the appropriate space" will be recorded at the end of each duty day, to include weekends and holidays, when duties are performed in the area. This notation is required regardless of container access.

4.4.2. SF Form 701 will be posted at or near the primary entrance/exit point to each room or area where classified material is stored, handled, processed, or destroyed. Additional areas/equipment to be checked will be added to the SF 701 in the space provided.

4.4.3. An end-of-day security check schedule will be published and posted by the USM, in conjunction with the SF 701, designating specific (by dates or time periods) government and DoD contractor personnel to conduct the end-of-day security check(s).

4.4.4. The reverse side of the SF 701 will be annotated any time the scheduled end-of-day security checker cannot personally accomplish the required check. The notation will identify (by name) a substitute who will complete the check. The USM is not responsible for arranging for substitute checkers. However, all schedule changes must be coordinated with the USM.

4.4.5. Use the reverse side of the SF 701 to report any problems or events requiring annotation or follow-up, i.e., desk top cluttered, container open and being used when end-of-day security check conducted, etc.

4.5. Security Check Requirements:

4.5.1. During the end-of-day security check the designated individual will inspect all equipment and areas, such as, desk tops, copier, computers and peripheral, STU IIIs, etc., where classified is handled, stored, processed, or destroyed as annotated on SF 701.

4.5.2. The individual will spin the dial on the security container(s) at least four (4) times in one direction and then attempt to gain access.

4.5.3. Keys to STU III telephone devices will be secured the end of the duty day. STU III keys may be secured in the same area as the STU III device if a GSA approved security container is used. If not it must be secured (locked desk or filing cabinet) in an area away from the STU III device.

5.1. Packaging and Transmission of Classified (Hard Copy Document/ Material):

5.1.1. Packaging and transmission requirements for classified dispatched via U.S. mail, BITS and TMO:

5.1.2. Classified document/material will be enclosed in two opaque sealed envelopes or similar wrapping, size permitting. If size prohibits the aforementioned security measures, then the classified material must be enclosed in two opaque sealed containers, such as boxes or heavy wrapping. If the classified material is an internal component of a packageable item or equipment, then the outer shell or body may serve as the inner enclosure, provided no classified information is revealed.

5.1.3. Any material used for packing must be of such strength and durability as to provide security and protection while in transit and to facilitate the detection of tampering. The wrappings must also conceal all classified characteristics. Always examine packages/containers bearing classified material for sign of tampering. If such signs are evident notify the USM immediately for additional guidance and actions.

5.1.4. Classified written information will be folded or packed in such a manner that the text will not be in direct contact with the inner envelope or container. Mailing of written materials of different classifications in a single package should be avoided.

5.1.5. For additional information and instructions on modes of transmission and packaging requirements review DoD 5200.1-R and AFI 31-401.

5.1.6. For policy on the electronic transmission of classified material review AFPD 33-2, *Information Protection.*

6.1. Handcarrying Classified On/Off Base:

6.1.1. All personnel escorting or hand-carrying classified material outside their work area must have prior approval (verbal/written) for such actions. Handcarrying and escorting requirements are as follows:

6.1.2. Classified documents will have a cover sheet and be placed in an envelope, folder, or other concealing container.

6.1.3. Verbal approval is sufficient when handcarrying between buildings or areas controlled by the escort's commander or agency chief. Written approval is required when the individual passes through check points controlled by security police or contract guards.

6.1.4. Written authorizations must specify the following: date, name of escort, issuing organization/unit, purpose, and telephone number of issuing activity for verification purposes.

6.1.5. The USM ensures that the following measures are adhered to:

6.1.5.1. Written authorizations are controlled.

6.1.5.2. Written authorizations are reaccomplished every five years.

6.1.5.3. Other courier requirements (see DoD 5200.1-R and AFI 31-401).

7.1. Destruction of Classified:

7.1.1. The classified destruction equipment (shredder) for the (INSERT UNIT/OFFICE DESIGNATION), is located (BUILDING AND ROOM NUMBER). Classified material (waste) will be destroyed in accordance with DoD 5200.1-R and AFI 31-401. At (INSERT NAME OF INSTALLATION) classified paper type materials (waste) will be destroyed by (INSERT DESTRUCTION METHOD).

7.1.2. Microfiche, computer diskettes and magnetic tapes will be transported to (INSERT DESIGNATED OFFICE/UNIT DESIGNATION, BUILDING AND ROOM NUMBER) for destruction. To schedule use of destruction equipment or facility contact (INSERT DESIGNATED ACTIVITY, NAME OF POINT OF CONTACT AND TELEPHONE). Other destruction requirements are as follows:

7.1.2.1. Two cleared personnel to witness the destruction of SECRET classified material.

7.1.2.2. One cleared person may destroy CONFIDENTIAL classified material.

7.1.2.3. When a shredder is used, check the in/out functional areas to ensure that no classified material remains intact. Run at least two sheets of unclassified paper/material through the shredder to ensure it is clear of all classified.

7.1.2.4. Check the immediate area around the shredder to ensure that no classified remains.

7.1.2.5. If transporting classified waste outside of the (INSERT UNIT/OFFICE DESIGNATION) for destruction, place waste in a sealed bag or box (tape or staple container) to ensure that no classified waste is accidentally lost while in transport.

7.1.2.6. Review AFI 33-202 for instructions on the degaussing, declassification and destruction of electronic/magnetic media or products.

7.1.2.7. Document and record classified destruction in accordance with DoD 5200.1-R and AFI 31-401.

8.1. Reproduction of Classified:

8.1.1. Only those government official(s) designated/appointed (LIST OFFICIALS BY POSITION TITLE) by the (INSERT COMMANDER/AGENCY CHIEF, AS APPROPRIATE) may approve the reproduction of SECRET and below classified documents.

8.1.2. The location of the only approved reproduction equipment (copier) for the (INSERT UNIT/ OFFICE DESIGNATION, BUILDING AND ROOM NUMBER).

8.1.3. The reproduction of classified material will be strictly controlled and any reproduction limitations enforced. Additional reproduction requirements are as follows:

8.1.4. Reproduction approval authority will annotate the file copy to reflect the number of copies made and distribution/recipients.

8.1.5. Maintain constant surveillance and control over reproduction equipment and areas where all such equipment is located (approved equipment only).

8.1.6. Ensure approved reproduction equipment is cleared after classified reproduction in accordance with instructions as outlined on the Air Force Visual Aid (AFVA).

8.1.7. Review DoD 5200.1-R and AFI 31-401 for additional requirements or limitations.

8.2. Equipment Control:

8.2.1. Post AFVAs, as appropriate.

8.2.2. Approved reproduction equipment will be placed in an area where constant surveillance can be maintained by individuals responsible for enforcing rules against unauthorized use. It the reproduction of classified material is required, two appropriately cleared persons must accomplish the reproduction process.

8.2.3. The reproduction approval official will initial and indicate the number of authorized copies on the original document. The requester will file the appropriately annotated original document.

9.1. Receiving Classified:

9.1.1. (INSERT DESIGNATED BITS PICKUP/ DELIVERY LOCATIONS, ROOM NUMBER) has been designated as the (INSERT UNIT/OFFICE DESIGNATION) central receiving office for BITS distribution. Administrative support personnel assigned duties at this location will:

9.1.1.1. Have a SECRET clearance.

9.1.1.2. Be authorized by the (INSERT COMMANDER/ AGENCY CHIEF, AS APPROPRIATE) to receipt sign for incoming mail.

9.1.1.3. Deliver hand-to-hand any classified material received.

9.1.1.4. Safeguard (GSA approved classified container or personal custody), all certified, registered mail, to include first class mail stamped/marked, DO NOT FORWARD.

9.1.2. The intended receiver will:

9.1.2.1. Sign and return receipt to sender immediately.

9.1.2.2. Review document for content and marking requirements prior to entering the document(s) into the classified file system. The receiver is also responsible for contacting the USM regarding procedures for initiating challenges for improper or unnecessary classifications and/or markings. Review DoD 5200.1-R and AFI 31-601 for instructions outlining challenge procedures. The USM is responsible for notifying (INSERT SSA DESIGNATION) whenever a challenge is initiated.

10.1. Review of Automated Security Clearance Approval System (ASCAS) Roster and Visit Authorization Letters (VALs):

10.1.1. The USM will conduct a monthly review of the unit ASCAS roster and update it as required in accordance with AFI 31-501, this also includes a review of VALs on file, if applicable.

10.1.2. The USM will monitor government periodic reinvestigations (PR) requirements and will direct any questions to the (INSERT SSA DESIGNATION). The identified government person (individual required to submit SF 85P, Questionnaire for Public Trust Position, or SF 86, Questionnaire for National Security Position, is responsible for contacting the USM upon notification of an upcoming/ pending PR and for completing and submitting all required investigative paperwork.

10.1.3. The USM will be responsible for preparing the AF Form 2583, Request For Personnel Security Action, and providing guidance and assistance in the preparation of the Standard Form 85P or 86, as appropriate.

10.1.4. The USM review complete investigation package and initials it prior to submitting it to (INSERT SSA DESIGNATION). The USM will maintain on file a copy of each open investigation package until a final clearance is granted and the ASCAS roster reflects this update.

10.1.5. For additional guidance on Personnel Security Program requirements, see AFI 31-501 and AFH 31-502.

11.1. Security Education and Training:

11.1.1. The USM will develop and publish an Annual Security Education Training Plan for the (INSERT UNIT DESIGNATION). Once published the USM, division, branch chief, supervisor or a designee will be responsible of conducting or ensuring all personnel (government and contractor) receive security training as outlined in the annual training plan. The USM will be responsible for gathering educational material, audiovisual aids and monitoring training accomplishment. The annual training plan will be developed in accordance with DoD 5200.1-R and AFI 31-401.

11.1.2. Personnel designated to administer or conduct security training may modify the training material to meet the specific audience training needs.

11.2.1. As a minimum, the unit's annual security education training plan must meets the following requirements:

11.2.1.1. Schedule training by calendar quarter.

11.2.1.2. Identify specific subjects and topics to be presented.

11.2.1.3. Identify personnel to make presentations.

11.2.1.4. Monitor training accomplishment.

11.2.1.5. Document training as required.

12.1. Processing Classified Information on Information Systems:

12.1.1. Classified Information will only be processed on an information system as approved by the Designated Approving Authority (DAA). This approval will be obtained by the Computer System Security Officer (CSSO) in accordance with AFI 33-202, *The Computer Security (COMPUSEC) Program.* The designated person(s) will process classified information in accordance with the DAA approved security plan.

13.1. Security Incidents and Violations:

13.1.1. Any person who has knowledge of the loss or possible compromise of classified information will immediately report such facts to the USM, immediate supervisor, commander or agency chief who is responsible for reporting the incident to (INSERT DESIGNATION OF SSA) within 24 hours of discovery.

13.1.2. The person discovering the security violation is responsible for protecting the classified until the responsible custodian or other such official regains proper custody.

13.1.3. The USM will advise the commander or agency chief of inquiry or investigative requirements as outlined in DoD 5200.1-R and AFI 31-401. The appointed government inquiry Official will be relieved of all other duties until the preliminary inquiry is completed.

14.1. NATO Classified Requirements and Safeguards:

14.1.1. NATO Access Requirements are as follows:

14.1.2. The USM will maintain a listing of all personnel authorized access to NATO classified information, to include each individual's level of clearance. Personnel who no longer require access to NATO classified information will be debriefed via AF Form 2587, Security Termination Statement.

14.1.3. Access to NATO classified information will be based on the individual possessing the required equivalent U.S. security clearance, (see USSAN 1-69, *United States Security Authority for NATO*), need-to-know (NTK) or required in the performance of official duties, NATO briefed, and execution of NDA. The NTK will be determined by the person having possession and control of the material involved.

14.1.4. Before granting an individual access to NATO confidential or above, the individual must be given an initial NATO security briefing.

14.1.5. Rebriefings are not required unless the person has access to ATOMAL information (any level). This security briefing will be annotated in the "Remarks" section of AF Form 2583, Request for Personnel Security Action.

14.2. NATO Safeguarding Requirements:

14.2.1. At (INSERT UNIT/OFFICE DESIGNATION), NATO classified documents will be stored in classified security container (INSERT CONTAINER NUMBER).

14.2.2. NATO classified information, CONFIDENTIAL or above, will be protected the same as prescribed for the storage of U.S. material of an equivalent classification (see USSAN 1-69 for U.S./NATO classification equivalent).

14.2.3. NATO classified documents may be stored in the same classified security container as non-NATO material, however they must be separated by a file divider. NATO documents marked "RESTRICTED" will also be stored in a GSA approved security container, they will not be stored in locked file cabinets, desks or other similar containers.

14.2.4. U.S. safeguarding, marking, transmission, access, dissemination, and accountability requirements apply equally to NATO classified material, with few exceptions. Review USSAN 1-69 for detailed guidance and additional requirements.

15.1. STU III Security:

15.1.1. STU III users will comply with procedures and instructions as outlined in AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type 1*, when using and to protect STU III equipment. STU III will remain in the non-secure mode unless required for classified/ sensitive information transmission.

15.1.2. Each authorized STU III user will be responsible for the security of their assigned keying device and/or code. Keys or codes will not be passed between authorized users.

15.1.3. Report key or equipment loss immediately to the organizations/units telephone control officer and the USM.

15.1.4. STU III equipment will be rekeyed and inventoried IAW AFI 33-209 and supplements thereto.

16.1. Foreign Travel Briefings/Reporting:

16.1.1. The (INSERT DUTY POSITION) is designated as Foreign Travel Briefer for (INSERT UNIT/ OFFICE DESIGNATION). Cleared (possess a security clearance) government and contractor personnel will report their planned non-official foreign travel and any inappropriate contacts, regardless of the individual's nationality, to the Foreign Travel Briefer or USM. Inappropriate contacts, include but are not limited to: attempts to obtain to classified and/or sensitive information, or when exploitation attempts by an unauthorized individual is made.

16.1.2. Prior to traveling abroad (unofficial travel), all cleared persons must contact the designated foreign travel briefer and receive a briefing as outlined in DoD 5200.2-R, *Personnel Security Program*.

16.1.3. Upon return, the traveler will contact the foreign travel briefer for a debriefing. Any suspicious activity or encounters will be immediately reported to the servicing AFOSI detachment/office. The USM will maintain and dispose of foreign travel records in accordance with AFMAN 37-139.

17.1. Special Security File Establishment:

17.1.1. Supervisors, co-workers, and USM will immediately notify the (INSERT COMMANDER/ AGENCY CHIEF, AS APPROPRIATE) when unfavorable information is revealed which could have a direct impact upon an individual's security clearance eligibility.

17.1.2. The (INSERT COMMANDER OR AGENCY CHIEF DESIGNATION, AS APPROPRIATE) will review, evaluate, and consider situation and take any necessary action in accordance with DoD 5200.2-R and AFI 31-501. If additional guidance is required, contact the (INSERT DESIGNATION OF SERVICING SECURITY ACTIVITY) for assistance.

18.1. Emergency Protection of Classified:

18.1.1. In case of fire, natural disaster, or civil disturbance, when time permits, classified material will be secured in any available GSA approved security container within the immediate work area. Personnel will not risk injury or the loss of life to secure classified material.

18.1.2. If the emergency is such, that classified material can not be secured, the holder of all such material will secure it on their person and evacuate the effected area immediately. The holder will secure the classified material until the emergency is terminated or take action to have it temporarily secured in an approved security container. Immediately following the emergency, personnel will return to their work areas and check for any insecure classified information.

18.1.3. Under no circumstances will the classified material be transported to the holder's private living quarters. (INSERT DESIGNATED EMERGENCY STORAGE LOCATION BY ORGANIZATION

AND BLDG. NUMBER) may be used for the temporary storage of classified material, if so dictated by the emergency at hand.

19.1. Semiannual Security Inspections:

19.1.1. The USM will ensure that semiannual security inspections are scheduled and conducted at the required six month intervals, to include, being responsible for keeping the (INSERT COMMANDER/ AGENCY CHIEF, AS APPROPRIATE) appraised of approaching inspection due dates, inspecting official appointment requirements, semiannual inspection results and corrective actions proposed or taken.

19.1.2. The USM will provide the inspecting official with the appropriate directives, self-inspection checklists and any required guidance or assistance, to include, reviewing the semiannual inspection report findings and notifying the (INSERT COMMANDER/AGENCY CHIEF, AS APPROPRIATE) and (INSERT DESIGNATION OF SERVICING SECURITY ACTIVITY) of any serious or major discrepancies.

20. Areas Not Covered In this Operating Instruction: For procedures or instructions not covered in this OI contact the USM or (INSERT DESIGNATION OF SERVICING SECURITY ACTIVITY).

(INSERT SIGNATURE BLOCK OF

COMMANDER/AGENCY, AS APPROPRIATE)

Chapter 4

FACILITY AND PERSONNEL SECURITY CLEARANCES AND SUITABILITY DETERMINATION INVESTIGATIONS

4.1. Facility Security Clearance (FCL) Requirements:

4.1.1. The Defense Industrial Security Clearance Office (DISCO) is responsible for the establishment, maintenance, and termination of all contractor FCLs or PCLs. DISCO also issues interim SECRET and CONFIDENTIAL FCLs, when possible and where practical. This activity is located in Columbus, Ohio. Address inquiries or correspondence as indicated below:

4.1.1.1. For verification of contractor personnel security clearance (PCL) status:

DISCO

Attn: S0834

P.O. Box 2499

Columbus, Ohio 43216-5006

Telephonic Inquiries: (614) 692-2265

Telefax: (614) 692-3663

4.1.1.2. For verification of facility clearance (FCL) status:

Personnel Investigation Center (PIC)

Central Verification Activity (CVA)

P.O Box 46060

Baltimore, MD 21240-6060

Telephonic Inquiries: (410) 865-2720/21

Telefax: (410) 865-2749

Internet Address: http://www.dis.mil.

4.1.2. All contractors requiring access to classified information require an FCL.

4.1.3. An FCL is an administrative determination that a company or firm is eligible for access to classified information. FCL eligibility is determined by the contractor's demonstrated reliability, integrity, stability, and mandated ownership prerequisite. ***Note: The existence of an FCL should not be interpreted to infer that a contractor is physically able to protect classified information. A contractor's safeguarding capability is an additional issue that requires a separate determination.***

4.2. Personnel Security Clearance (PCL) Requirements:

4.2.1. DISCO issues PCLs and maintains records for all contractor personnel performing on a classified contracts within the National Industrial Security Program (NISP).

4.2.2. PCLs for all cleared contractor employees are retained on file at the contractor's home office facility (HOF) or the specific cleared facility . The contractor HOF notifies the AF activity of all

employees requiring access to classified information (contract specific) and the status of their respective PCL via VAL.

4.2.3. The HOF should be tasked to forward a copy of the VAL to all contract performance locations identified in the contract per the AF's guidance or instructions provided in the VGSA or other contracting documents.

4.2.4. The VAL is completed and signed by the HOF's FSO and serves as means of verifying and confirming the employee's PCL status. The exception being when unique on-base conditions or circumstances warrants otherwise, i.e. special access program (SAP), etc.

4.3. Suitability Determination Background Investigations Requirements

4.3.1. Contractor personnel performing on DoD contracts as a visitor group or cleared facility, on or off -base, who are assigned duties using sensitive unclassified automated information systems (AISs) designated as ADP-I, ADP-II or ADP- III must be the subject of an investigation to determine the individual's suitability to occupy the position. ***NOTE:*** The background investigation requirement is not applicable when the contractor employee has a valid PCL on file with DIS.

4.3.1.1. The SF Form 85P, **Questionnaire for Public Trust Position,** is completed and submitted to: DIS Personnel Investigation Center (PIC), P.O. Box 28989, Baltimore MD 21240-8989, for the appropriate scope and type of background investigation to be conducted. See AFI 31-501.

4.3.1.2. Once completed, DIS PIC returns the results of the investigation to the AF CAF who, in-turn, returns the investigation to the requesting activity, who makes the suitability determination. ***NOTE:*** Investigations conducted to determine contractor employee's suitability are not adjudicated by AF or DIS.

4.3.1.3. For additional guidance see DoD 5200.2-R, *Personnel Security Program*.

Chapter 5

VISIT NOTIFICATION REQUIREMENTS

5.1. Pre-Announcement Notifications:

5.1.1. A VAL commonly referred to as a "visit request" is a formal pre-visit announcement or notification to a government activity or contractor's operation notifying that agency to expect the arrival of an official visitor in support of a specific contract or program.

5.1.2. Whether generated by a government activity or contractor agency, the VAL or equivalent document should contain the contractor's name, address, telephone number, assigned CAGE Code, if applicable, level of FCL, and name, date, and place of birth, citizenship, and certification of the intending employee visitor's security clearance. In addition, also include: purpose of visit, party to be visited, and anticipated date and time of arrival and departure.

5.2. Processing Requirements:

5.2.1. Provide the agency or location to be visited sufficient advanced notification to verify the need for the visit, other pertinent data, and ample time to approve or disapprove the request.

5.2.2. A VAL is required to be processed for any visit during which classified information will be discussed or disclosed, except when government representatives, serving in an official capacities as inspectors, investigators or auditors, visit contractor facilities.

5.2.3. Incoming contractor generated VALs may be verified (PCL status confirmed) by the AF activity, who approves or disapproves the visit, prior to disclosing or releasing any classified information. The AF activity publishes procedures for processing incoming VALs, to include designating VAL verification officials, if appropriate and VAL repositories (AF activity, SSA, contracting, etc.).

5.2.4. In addition to mailing, VALs may be verbally coordinated or FAXed to the agency to be visited. A written VAL must be submitted to confirm visits coordinated telephonically.

5.2.5. Forward hard-copy visit requests directly to the agency to be visited or as directed otherwise.

5.2.6. Contractor VALs submitted in support of a "classified" work effort may be accepted as being valid for a period of up to 12 months or for the duration of the contract, when authorized and approved by the AF activity.

Chapter 6

SECURITY REVIEW REQUIREMENTS

6.1. Conducting Security Reviews for Cleared Facilities:

6.1.1. The installation commander designates either the SSA or CSO to conduct security reviews for on-base cleared facilities. SSAs designated security oversight responsibilities for cleared facilities perform duties (security reviews, surveys, form completion, etc.) per guidance of the DIS cognizant security activity. When and/or if required, complete either a hard-copy or automated DD Form 696, **Industrial Security Inspection Report.** (See Figure 6.1.)

6.1.1.1. The SSA coordinates security reviews with other installation security discipline OPRs (OPSEC, COMSEC, COMPUSEC, EMSEC, etc.) to ensure all aspects of the contract security requirements are addressed during the security review.

6.1.1.2. Normally, letters of review are sent by the SSA directly to the contractor. However, the SSA formally communicates the results of unsatisfactory security review results to the contractor through the contracting office.

6.1.2. Security Review Scheduling . Cleared facilities are scheduled for security reviews periodically, consistent with risk management principles, but no more than once every 12 months unless special circumstances exist.

6.1.3. Notification of Pending Security Review . Cleared facilities are normally given advanced written notice, unless an unannounced security review is to be conducted. Unannounced security reviews must be justified (unsatisfactory security review rating, major deficiencies, etc.) and have SSA commander or equivalent official approval.

6.1.4. The Role of the SSA:

6.1.4.1. The SSA confirms compliance with security requirements, identifies weaknesses in the contractor's security program, and recommends appropriate corrective action.

6.1.4.2. The intent of the security review is to provide evidence of compliance and/or incidental noncompliance with contract security requirements. This process identifies both program strengths and weaknesses and assists the SSA in determining appropriate corrective actions.

6.1.5. Pre-Security Review Planning:

6.1.5.1. The SSA discusses and coordinates plans (in advance) with the on-base contractor's facility security officer (FSO) or representative prior to conducting a security review. Pre-security review planning considerations may include:

6.1.5.1.1. Reviewing last security review records.

6.1.5.1.2. Reviewing security violation reports since last security review.

6.1.5.1.3. Reviewing DD Form 254, Statement of Work, Visitor Group Security Agreement (VGSA), etc.

6.1.5.1.4. Reviewing other correspondence, as applicable.

6.1.5.2. The SSA evaluates data and information compiled during the pre-security review to make plans for conducting the formal security review.

6.1.6. Security Review Inbrief

6.1.6.1. Whenever possible, schedule a meeting via the FSO with the contractor's senior on-base management officials prior to the beginning of the formal security review.

6.1.6.2. The in-brief is a short explanation of the purpose and intent of the security review. It also provides an opportunity for informal SSA and contractor interaction.

6.1.7. Security Review Techniques

6.1.7.1. Be knowledgeable of security standards and the specific security requirements applicable to the contract. Apply sound judgment to problem areas, don't get wrapped up in technicalities and use common sense.

6.1.7.2. Follow plan articulated during the pre-security review.

6.1.8. Conducting Unannounced Security Reviews

6.1.8.1. Unannounced security reviews are conducted for cause (unsatisfactory rating, major deficiency, etc.) to confirm that appropriate corrective actions have been initiated, taken, or implemented which properly protect classified information.

6.1.8.2. Whenever possible, conduct unannounced security reviews during time periods when company management and/or key personnel are available to answer questions, participate and/or interact with SSA personnel.

6.1.9. The Exit Briefing

6.1.9.1. Brief the on-base contractor's senior management officials and FSO or security representative at the conclusion of the security review, providing accurate feedback on their overall security posture.

6.1.9.2. Make only generic reference to minor administrative issues. Stress the positive aspects of the contractor's security program and give personal recognition, when appropriate.

6.1.10. Unsatisfactory Security Reviews

6.1.10.1. Normally, an unsatisfactory rating is given when the results of the security review demonstrates the contractor's inability or unwillingness to properly safeguard classified information or repeated failure to correct major deficiencies.

6.1.10.2. Promptly coordinate the results of security reviews rated as "unsatisfactory" with the contracting office and CSO.

6.1.10.3. An unsatisfactory rating may be justification for FCL revocation. The SSA may make such a recommendation to the CSO via the contracting office, depending upon the severity of the situation or problem.

6.1.10.4. Suspension of the cleared facility's safeguarding capability is also an option available, pending resolution of the security deficiency.

6.1.10.5. Notifying the cleared facility of adverse revocation/ suspension actions is the responsibility of the contracting office.

6.2. Conducting Security Reviews for Visitor Groups:

6.2.1. Security reviews are **not** conducted for visitor groups operating under DoD 5200.1-R/AFI 31-401**,** *Managing The Information Security Program*.

6.2.2. Visitor groups designated to operate under DoD 5200.1-R/AFI 31-401 are evaluated in accordance with installation information security program requirements, and the sponsoring AF activity's security operating instructions (OIs).

6.3. Conducting NISPOM Equivalent Security Reviews for Visitor Groups:

6.3.1. When determined appropriate by the installation commander, NISPOM equivalent security reviews may be conducted for visitor groups operating under the auspices of the installation security program.

6.3.2. Conduct NISPOM equivalent security reviews as outlined in the installation security program supplement and VGSA. Normally, a combination of DoD 5220.22-M, DoD 5200.1-R, and installation security program specific requirements are reviewed when conducting this type of security review.

Figure 6.1. Instructions for Completion of DD Form 696, Industrial Security Inspection Report.

1. Executing DD Form 696. The DD Form 696 is undergoing revisions. In addition, an automated version of the form will soon be made available. Instructions listed below are applicable to the most current (hardcopy) version and are provided as recommendations for completing the form. Use of the DD Form 696 is mandatory for cleared facilities and the CSO will provide the SSA guidance on its completion and submission. AFI 31-601 makes its use optional for on-base visitor groups. However, data fields on the form are not intended for visitor groups. Suggested completion instructions are offered.

a. **Item 1. Date Prepared**. Date entered as numbers, year first, then month, then day. For example: September 14, 1993 is entered as 930914.

b. **Item 2. Facility**. Enter complete data.

c. **Item 2b. Address**. List physical address.

d. **Item 2c. CAGE Code**. Data field does not apply to visitor groups. Also known as a Federal Supply Code Number (FSCN). They are established and maintained by the Defense Logistics Supply Center, Battle Creek, MI for other reasons. They are used by the CSO to identify individual cleared facilities. Each cleared facility has a separate CAGE code. They are not issued to visitor groups. The CSO advises the SSA when temporary or final codes are issued for cleared facilities.

e. **Item 3. Home Office**. Identify the facility which executed the DD Form 441 which drives cleared facility or visitor group status for the operation. There may be an intermediary cleared division providing management and security oversight for the cleared facility or visitor group. This is known as a Principal Management Facility (PMF), but PMFs are not always home offices. Do not list the PMF in this data

field. However, since PMFs provide primary management oversight for the cleared facility or visitor group, when applicable, they may be referenced in the remarks section.

f. **Item 4. Parent Holding Company**. This data field may be left blank.

g. **Item 5. Facility Security Supervisor**. Identify by name and telephone number of the on-base contractor employee specified by company management to ensure contractor compliance with security requirements.

h. **Item 6. Facility Clearance**. Data field is intended for cleared facilities.

i. **Item 6a. Level**. For cleared facilities, the highest level of classified access permitted by the cleared facility. For visitor groups, the highest level of classified access authorized for site performance.

j. **Item 6b. Type**. Not applicable for visitor groups.

k. **Item 6c. Type of Foreign Interest Resolution**. Might apply to either cleared facilities or visitor groups. If the HOFs FCL has been established based on one of the formula FOCI resolutions noted, check the appropriate box. If the FCL of the HOF has been established based on a Special Security Agreement (SSA), classified access restrictions will also apply to cleared facilities or visitor groups on-base. The CSO can provide guidance on this subject.

l. **Item 6d. Clearance Date**. Applies only to cleared facilities. It may be left blank for visitor groups.

m. **Item 6e**. Applies only to cleared facilities. The CSO categorizes cleared facilities by degree of complexity, using a weighted point system. Each cleared facility is categorized, from "A" through "E," with "A" being the most complex and difficult to inspect. The CSO provides categorization instructions to the SSA and the SSA computes the category and reports the information to the CSO.

n. **Item 6f. Security Review Frequency**. Cleared facilities are inspected in accordance with DOD policy. Pursuant to AFI 31-601, the frequency of security reviews for on-base cleared facilities is determined by the installation commander.

o. **Item 7. Type of Business.** Brief description of the nature of the contractor's work on site. For example: "Computer hardware services."

p. **Item 8. Dates of Inspection**. List data numerically by year, month and date. Project next inspection for end of scheduled month. Do not project unscheduled inspection on the report.

q. **Item 9. Time Expended**. The CSO accounts for time expended as "TRIP" time, to report time spent on "T" for travel, "R" for presurvey research, to include time spent discussing the action with the contracting office and/or the CSO, "SR" security review, the actual time spent at the contractor site, and "P" for time expended in post survey actions, to include time needed to prepare the survey report and time

spent immediately following the survey to coordinate with the contractor and ensure prompt submission of required documentation. Trip time must be reported for cleared facilities, and may be required for visitor groups, if directed by the command. For cleared facilities, the CSO normally requests that data be reported to the nearest half hour.

r. **Item 10. Total Number of Employees**. Self explanatory.

s. **Item 11. Number of US Employees Cleared**. Employees may not be cleared at a level higher than that of the FCL. For visitor groups, employees may not be afforded classified access higher than the stated level of the contract.

t. **Item 12. Number of Non-US Citizens**. Self explanatory.

u. **Item 13. Number of Non-US Citizens With Limited Access Authorizations (LAAs).** Self explanatory.

v. **Item 14. Access to Classified Material Since Last Security Review**. Items 14d, e, and f do not apply to on -base cleared facilities. Item 14b does not normally apply to on-base cleared facilities, but is intended to address HOFs who send intermittent visitors to customers. Item 14g refers to Special Access Programs for which the CSO (or the SSA) has been relieved of security review duties. If the CSO or SSA representatives encounters a suspected SAP during the course of the security review, document available information on it in the remarks section of the DD Form 696 and refer the matter through command channels to SAF/AAZ for confirmation.

w. **Item 15. Inspection**. Report the nature and results of the security review by checking the appropriate boxes.

x. **Item 15a. Scope**. Partial security reviews are only authorized to confirm compliance with corrective action following an unsatisfactory security review rating.

y. **Item 15b. Rating Assigned**. Coordinate with the contracting officer and CSO before assigning an unsatisfactory security review rating to a cleared facility. Coordinate with the contracting officer and home office before assigning an unsatisfactory rating to a visitor group, when applicable.

z. **Item 15c. Results**. "NO DEF" means no deficiencies were cited during the security review. "COS" means "Corrected On the Spot." It reflects that minor deficiencies were noted but corrected promptly during the security review. "LOR" means "Letter of Requirements" and indicates that minor deficiencies were noted that were not corrected during the security review and are specified in the security review results letter. "MAJOR" reports serious incidents or conditions at the cleared facility or visitor group, if applicable, resulting in the probable loss or compromise of classified information and/or systematic failures of the company's security program which could result in loss or compromise of classified information. MAJOR deficiencies may result in the assignment of an unsatisfactory security review rating.

aa. **Item 16. Elements of Security Review and Ratings Assigned**. This form was intended to address cleared facility scenarios. Data fields do not always relate to visitor group scenarios. Annotate the blocks that apply to the cleared facility or visitor group. For example, block "A," "Facility Clearance," applies to all cleared facilities, but does not apply to visitor groups. Reflect "S" or "U" for a cleared facility and "N/A" for a visitor group . Block "B," "Access Authorizations," may apply to cleared facilities **and** visitor groups. Block "K," "Classified Storage," does not apply to visitor groups, but might apply to cleared facilities.

bb. **Item 17. Safeguarding Ability**. Applies to cleared facilities only.

cc. **Item 18. Approved Storage Facilities**. Applies to cleared facilities only. Unless contract language clearly specifies otherwise, the terms "Restricted Area" and "Closed Area" will refer to terms defined by the NISPOM.

dd. **Item 19. Other DOD Programs**. Blocks 19a and b refer to programs monitored by the CSO which are not addressed by the SSA.

ee. **Item 20. Number of Uncleared Locations With Cleared Personnel**. This data field is intended to address cleared PMFs. It has no meaning for on-base cleared facilities or visitor groups. Reflect "N/A" for this item.

ff. **Item 21. ISR Number**. Annotate this data field "N/A." This data field normally does not apply to SSA specialist performing surveys. It is intended to identify CSO representatives.

gg. **Item 22. Remarks**. Report any and all information of special interest relating to the cleared facility or visitor group security review.

hh. **Item 23. Security Specialists**. Self-explanatory.

ii. **Item 24. Reviewing Official**. Self-explanatory.

Chapter 7

FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE (FOCI)

7.1. FOCI Overview and Impact

7.1.1. Federal legislation restricts the dissemination of critical technologies, classified and unclassified, to foreign interests. Foreign ownership of critical US companies has been addressed by DoD policy for decades. Establishment and continuance of a company's FCL is predicated, in part, on the facility's ability to demonstrate its freedom from **inappropriate** FOCI. FOCI can pose problems for contractors and disrupt the Air Force mission. However, close interaction between the SSA, CSO, Contracting Officer, and foreign disclosure authorities offer ready solutions to most FOCI problems.

7.1.1.1. DoD policy directs that, when elements of major FOCI are evident, the company's FCL be invalidated by the CSO. Contracting officers are notified of the action by the CSO.

7.1.1.2. An invalidation is a very serious condition which threatens FCL revocation. Invalidation signals to the contracting officer that the FCL may be revoked in the near future if a satisfactory resolution of the FOCI problem is not found.

7.1.1.3. Revocation of the FCL affects the status of currently issued classified contracts. When notified by the CSO that an FCL has been invalidated for FOCI, contracting officers and program managers should review and plan for possible alternatives. The CSO addresses and resolves FOCI.

7.2. DOD FOCI Policy:

7.2.1. DoD FOCI policy is stated in DoD 5220.22-R, *Industrial Security Regulation (ISR).*

7.2.1.1. Contractors report FOCI by executing and submitting to the DIS a Certificate Pertaining to Foreign Interests (DD Form 441s) with complete explanatory information.

7.2.1.2. The HOF executes the DD Form 441S, **Certificate Pertaining to Foreign Interest**, for cleared facilities located on the installation, when applicable.

7.2.1.3. DIS monitors a company's ongoing involvement with foreign interests and notifies the Air Force contracting office when influence from foreign interests becomes serious. Invalidation of the FCL is considered only when major FOCI elements are reported.

7.3. Resolution of FOCI Issues. DIS resolves FOCI issues by completely neutralizing the foreign influence (via changes in voting trust or proxy agreement) or modifying the FCL (via reciprocal FCL or FCL based on special security agreement), when appropriate.

7.4. FOCI Special Security Agreements:

7.4.1. Special Security Agreements are negotiated arrangements between DoD, the acquiring foreign interest and the acquired US company. They are the basis for establishment of special FCLs with negotiated classified access restrictions.

7.4.2. Special Security Agreements permit foreign ownership and operation of a US company. The influence of the foreign interest is neutralized by agreements with the foreign interest and the estab-

lishment of internal administrative procedures within the acquired US company intended to deter and detect instances of noncompliance with those agreements.

7.4.3. DOD policy considers Special Security Agreements to be fully acceptable methods to neutralize the influence of the foreign interest. Companies cleared based on Special Security Agreement are considered to be US owned and operated for purposes of bidding on Air Force classified contracts.

7.4.4. A user agency may justify and request a company be cleared under a Special Security Agreement to isolate FOCI. This justification for such Special Security Agreement is called a National Interest Determination (NID).

7.4.4.1. The NID is a agency level risk analysis, determination, and acceptance used to justify the need for an Special Security Agreement. ASD(C3I) approve the establishment of a Special Security Agreement.

7.4.4.2. Contracting officers sponsor NIDs when the foreign interest refuses to accept the more traditional FOCI solutions, when an alternative action will result in an unacceptable delay, or when the prospective contractor is the sole source.

7.4.4.3. NID sponsorships are submitted through command channels to HQ USAF/SPI. NID sponsorships involving Special Access Program information are submitted through SAP command channels to SAF/AAZ for consideration. NIDs are transmitted by the Administrative Assistant to the Secretary of the Air Force, SAF/AA, to ASD(C3I).

7.4.4.4. NID sponsorships include:

7.4.4.4.1. Complete identification of the facility and the nature of the foreign involvement.

7.4.4.4.2. Identification of current and pending classified contracts with the company.

7.4.4.4.3. Explanation of the company's products and/or services and why they are critical to the Air Force mission. If sole source, so state.

7.4.4.4.4. Identification of the negative impact to the Air Force mission if the company's products/services were no longer available.

7.4.4.4.5. Description of efforts taken to discover or develop alternate sources of supply to reduce Air Force dependency on a foreign owned supplier and why they were ineffective.

7.4.4.4.6. If possible, explain the planned efforts to discover or develop alternate sources of supply in the future.

7.4.4.4.7. NIDs are reviewed periodically by the sponsoring activity and vacated when no longer necessary.

Chapter 8

INDUSTRIAL SECURITY PROGRAM REPORTS AND RECORDS

8.1. Industrial Security Program Reports:

8.1.1. The SSA prepares industrial security program related reports in accordance with DoD policy, AFI 31-401, AFI 31-601, and/or installation security program, as applicable. The facility's designation (cleared facility or visitor group) will normally determine reporting requirements. Most reports are submitted by the SSA as follows:

8.1.1.1. For cleared facilities, send cleared facility's management a notification letter in advance of pending security reviews and a subsequent letter noting the results following such security reviews. Advanced notification is not required for conducting unannounced no-notice security reviews for cleared facilities. For visitor groups operating in accordance with installation security program requirements, send a notification letter to the visitor groups' on-base management and AF activity, if appropriate. Security reviews are **not** conducted for visitor groups operating strictly under AFI 31-401.

8.1.1.2. Comply with CSO requests for reports and other administrative actions relating to cleared facilities. The following reports are sent to the CSO:

8.1.1.2.1. Reports of cleared facilities security violations or compromises of classified material. For visitor groups operating under AFI 31-401, report **only** compromises to the CSO via the

contracting office, and process all other security violations in accordance with AFI 31-401, unless the severity of the violation warrants CSO notification.

8.1.1.2.2. Copies of administrative inquiries conducted into those incidents of violations/compromises, with identification of employee culpability, where known.

8.1.1.2.3. Decision to downgrade or declassify information as a result of such contractor determined security violations.

8.1.1.2.4. Adverse information developed by the AF or disclosed by the contractor, relating to an employee of a cleared facility or visitor group, which is reportable pursuant to NISPOM requirements.

8.1.1.2.5. Forms and reports essential to the establishment and maintenance of the FCL, to include DD Forms 374, DD Forms 441, DD Forms 696, and correspondence relating to security reviews.

8.1.1.2.6. Forms, reports, or other documentation prepared in connection with visitor groups are not sent to the CSO, unless mandated by the severity of the situation.

8.2. Establishment of Industrial Security File Folders:

8.2.1. Each SSA establishes and maintains industrial security files in accordance with ISR, MAJCOM, and, when applicable, local direction. The following recommendations are offered to help SSAs maintain such records in a uniform fashion.

8.2.1.1. Contract Documents and DD Form(s) 254, **DoD Contract Security Classification Specification**. Current DD Forms 254, along with pertinent security requirements portions of contract documents are retained for all current and pending classified procurements for cleared facilities and visitor groups. Destroy official records in accordance with AFMAN 37-139.

8.2.1.2. DD Form 374, **DoD Facility Security Clearance Survey Data Sheet**. This form documents facility structure, ownership and history. The purpose of the survey is to determine that the contractor is capable of properly safeguarding classified information for precontract negotiations, and that the contractor is fully cognizant of the responsibilities involved in safeguarding classified information. It is a prerequisite to granting the FCL. It is used for cleared facilities and may be used for visitor groups, if and/or when appropriate.

Partial survey reports are permitted, not more than one DD Form 374 may be retained on file. As a general rule, a complete history of ownership, address and name changes is evident in the DD Form 374s. It is unimportant whether this history is reported in one complete DD Form 374 or several partial DD Forms 374. Maintain your record copy of DD Form 374 in accordance with AFMAN 37-139. (See Figure 8.1.)

8.2.1.3. DD Form 441, **DoD Security Agreement**. Each cleared facility retains a copy of the HOF DD Form 441 on file. The SSA also retains a copy. This does not apply to visitor groups.

8.2.1.4. DD Form 441-1, **Appendage to Department of Defense Security Agreement**. Each cleared facility has a DD Form 441-1 on file. Normally, the DD Form 441-1 is executed by the HOF on behalf of the on-base branch or division. However, the HOF may delegate authority to the division to execute the form locally. It is countersigned by the CSO or SSA, when so authorized. If the form is executed locally by the division, it is submitted to the CSO for certification. The SSA does not countersign the DD Form 441-1. The DD Form 441-1 is reexecuted to reflect changes in name or address. Only the most current DD Form 441-1 is retained on file by the cleared facility or the SSA. DD Forms 441-1 are not executed by or on behalf of visitor groups.

8.2.1.5. DD Form 441S, **Certificate Pertaining to Foreign Interests**. This form is executed by the HOF for on-base cleared facilities and visitor groups. It is submitted by the home office directly to the CSO. Copies are not retained in file for on base cleared facilities or visitor groups. The SSA is familiar with this form and its purpose pursuant to its obligation to support the acquisition community.

8.2.1.6. DD Form 696, **Industrial Security Inspection Report**. In conformance with DoD policy the DD Form 696 is used to document security reviews of cleared facilities. It may also be used to document security reviews of visitor groups when so mandated by the installation security program. Furnish copies of security review reports, to include security review letters of results, to the CSO following security reviews conducted each cleared facility. Security review reports for visitor groups, when applicable, are **not** sent to DIS. Maintain your record copy of DD Forms 696 in accordance with AFMAN 37-139.

8.2.1.7. DISCO Form 562, **Personnel Security Clearance Change Notification**. This is a multiple usage form used within the NISP to report changes in PCL status. The FSO of the cleared facility can demonstrate compliance with pertinent reporting requirements by maintaining copies of this form until the SSA has had an opportunity to review them. Normally, they are not executed by visitor groups, but by their home office. They are not retained in the facility files.

8.2.1.8. SF 312, **Classified Nondisclosure Agreement (NDA)**. For both cleared facility and visitor group employees, once executed, the DD Form 312 is forwarded to the CSA or it's designee (DISCO). The SSA may confirm the existence of a properly executed SF 312s for cleared on-base contractor personnel by contacting the designated repository. SSAs are not required to retain file copies of contractor executed DD Forms 312.

8.2.1.9. Classified Visit Authorization Letters (VALs). On/off base cleared facility and visitor group HOF's send VALs to the designated on-base activity or facility on behalf of their cleared employees. VALs may be sent to the contracting officer, SSA, or directly to the AF activity to be visited. Procedures should be established and implemented to facilitate the immediate processing and coordination of in-coming VALs and to afford classified access only to those authorized. VALs are retained on file at the designated location (contracting office, SSA or AF activity) and are disposed of in accordance with AFMAN 37-139.

8.2.1.10. General correspondence between the cleared facility, visitor group HOF, AF activity, CSO, and/or SSA is retained as long as needed.

8.3. Records Maintenance Requirements. The SSA maintains records relating to each cleared facility and visitor group serviced by the SSA. The CSO may request the SSA provide copies of reports and other records required for cleared facilities. With some exceptions, similar records may also be maintained for visitor groups, if determined appropriate by the installation commander.

Figure 8.1. Instructions for Completing DD Form 374, Facility Security Clearance Survey.

8.1. Executing DD Form 374: Execution of the DD Form 374 or equivalent automated media is mandatory for cleared facilities. Its use and execution may also be mandated for those visitor groups operating under the installation security programs. ***NOTE*:** Visitor groups falling under the preview of AFI 31-401 are exempt from this requirement. Complete DD Form 374 as follows:

a. **Part 1. Industrial Security Representative. Item 1. Credential Number**. Enter "N/A." This data field does not apply to Air Force personnel performing such surveys. It is intended to identify the DIS Industrial Security Representative performing the survey.

b. **Item 2. Name**. Self explanatory.

c. **Item 3. Signature**. Self explanatory.

d. **Item 4. Office Symbol**. The SSA organizational symbol is listed here.

e. **Item 5. Time Expended.** The CSO accounts for time expended as "TRIP" time, to report time spent on "T" for travel, "R" for presurvey research, to include time spent discussing the action with the contracting office and/or the CSO, "SR" for security review, the actual time spent at the contractor site, and "P" for time expended in post survey actions, to include time needed to prepare the survey report and time spent immediately following the survey to coordinate with the contractor and ensure prompt submis-

sion of required documentation. TRIP time must be reported for cleared facilities. Normally, this requirement is not applicable to visitor groups, unless directed by the MAJCOM or installation mandates.

f. **Item 6. Requesting User Agency/Contractor Address**. Identify the contracting office which has sponsored the cleared facility or visitor group.

g. **Item 7. Telephone Number**. For FCLs try to list a commercial direct dial number (DDN). The CSO may not have access to DSN circuits.

h. **Part II. Facility In Process. Item 8. Facility Identifying Information**. Submission of precise data is important. Coordination with the contracting officer helps to ensure that data reported on this form is consistent with information reported by the contractor elsewhere on contract documentation.

i. **Item 8a. Exact Legal Name**. Once again, precise data is important. For example, "The Boeing Company" is a proper corporate name. "Boeing" is not.

j. **Item 8b. "DBA/AKA/TA".** This refers to a company's marketing name, when different from the legal name in item 8a. "DBA" stands for "Doing Business As." "AKA" stands for "Also Known As." "TA" stands for "Trading As." The abbreviations are interchangeable for our purposes. Company documentation will usually list the legal name and then the trading name. For example, James T. Kirk, dba "Horizons Unlimited."

k. **Item 8c. Physical Location/Address**. Identify the physical address of the cleared facility or visitor group.

l. **Item 8d. Mailing Address**. Used normally to report the classified mailing address when different from the physical address. For cleared facilities, this is usually a post office box. For visitor groups, only the base classified mailing address may be listed, since visitor groups do not receive classified material independently.

m. **Item 8e. CAGE Code.** Also known as a Federal Supply Code Number (FSCN). They are established and maintained by the Defense Logistics Supply Center, Battle Creek, MI. They are used by the CSO to identify individual cleared facilities. Each cleared facility has a separate CAGE code. They are not issued for visitor groups. The CSO advises the SSA when temporary or final CAGE codes are issued for cleared facilities.

n. **Item 8f. Clearance Level Required**. For cleared facilities, list the highest sponsored level of facility security clearance necessary for contract performance. For visitor groups, list the highest level of classified access necessary for on base performance.

o. **Item 8g. Safeguarding Level Required**. Applies to cleared facilities only. Level of safeguarding cannot be higher than that of the cleared facility. For visitor groups, list "N/A."

p. **Item 8h. Safeguarding Approved.** A "Yes" answer is reflected only when the SSA has confirmed the existence of satisfactory security storage hardware and implementing procedures, to include supplemental security controls, to ensure that the cleared facility can protect adequately classified material entrusted to it. Safeguarding may not be certified prior to establishment of the cleared facility. For visitor groups, this data field may be left blank.

q. **Item 8i. Number of employees**. Self explanatory.

r. **Item 8j. Type of Business**. Identify briefly the nature of work to be provided by the contractor. For example: "Operates BITS."

s. **Item 8k. Facility Point of Contact**. For cleared facilities and visitor groups, list the on site contractor employee who will be the liaison for purposes of contract compliance. Identify by job title and list, for cleared facilities, a direct dial telephone number.

t. **Item 9. Name and Address Changes During the Last 10 Years**. This data field has limited meaning for on-base cleared facilities and no meaning for visitor groups. If a cleared facility changes its physical address during its stay on-base, this is addressable pursuant to ISR requirements. Prior addresses and time frames should be identified. Name changes should also be reported as they occur.

u. **Item 10a**. All on-base cleared facilities are branch offices of an MFO, as opposed to a subsidiary. This block is checked for cleared facilities only. Visitor groups may leave this data field blank.

v. **Item 11. Home Office**. Identify the facility which executed the DD Form 441. There may be an intermediary cleared division providing management and security oversight for the cleared facility or visitor group. This is known as a Principal Management Facility (PMF). A home office may be a PMF, but PMFs are not always home offices. Do not list the PMF in this data field. However, since PMFs provide primary management oversight for the cleared facility or visitor group, they may be referenced in the remarks section.

w. **Item 11e. Clearance Status**. The CSO can confirm the clearance status of the home office.

x. **Item 11f. Clearance Level Required.** A HOF must be cleared at least to the level of the classified access required for on-base performance. A HOF may be cleared at a level higher than that required for the on-base cleared facility or visitor group. However, a HOF may not be processed for a higher level of clearance than necessary for contract performance. For example, a home office may have a TOP SECRET FCL when its on-base cleared facility or visitor group requires only SECRET or CONFIDENTIAL access. A home office may not be sponsored for a TOP SECRET FCL for performance on a classified contract requiring only SECRET or CONFIDENTIAL access.

y. **Item 11g. Facility Point of Contact**. Identify the official at the HOF responsible for ensuring satisfactory cleared facility or visitor group compliance with contract requirements. Include job title and direct dial telephone number.

z. **Item 12. Parent Corporation**. This data field has no value to the SSA or CSO for on-base cleared facilities or visitor groups. All on-base cleared facilities are divisions or branches of HOFs under the oversight of a CSO. The existence and status of parent organizations to the HOF are addressed by that CSO. Visitor groups are transparent to the CSO, but the HOF sponsoring the visitor group is under CSO oversight. Parent organizations for visitor group HOFs are addressed by the appropriate CSO and are not a visible concern for the SSA. This data field may be left blank.

aa. **Part III. Organizational Structure. Owners, Officers, Directors and Executive Personnel (OODEPs). Item 13. Organizational structure**. Part II is concerned primarily with FCLs. Visitor group input is required only for item 14.

bb. **Item 13c.** On-base cleared facilities are **always** divisions or branch offices. No other answers in the affirmative should be reflected for this item. Remaining data field for this item may be annotated with "N/A."

cc. **Item 14. OODEPs Identification**. List the principal management official at the on-base cleared facility or visitor group and, if different, the person assigned responsibility for ensuring compliance with security requirements. For cleared facilities, both are cleared to the level of the FCL. For visitor groups, both are cleared to the level of classified access necessary for on-base performance.

dd. **Part IV. Negotiators. Item 15. Identification**. Negotiators are key cleared facility employees, not OODEPs by definition, whose clearances are processed concurrently with OODEP clearances at the beginning of the FCL process to ensure their prompt issuance. Negotiator clearances are needed immediately upon issuance of the FCL to ensure that the contractor can respond promptly to bid or contract needs. Negotiator clearance documents are annotated "Negotiator" and submitted with OODEP personnel clearance documents to the CSO. For visitor groups, this data field may be left blank.

ee. **Part V. Foreign Ownership, Control or Influence (FOCI).** Data reported applies to HOF and parent organizations and has no meaning for on-base cleared facilities or visitor groups. This data field may be left blank.

ff. **Part VI. Administrative Notes. Item 17. Processing Data**. Completed for cleared facilities only. Item 17a does not apply to the SSA and may be left blank. For item 17b, the "ISFO" means "Industrial Security Field Office" and is intended to identify the local DIS Industrial Security Field Office assigned inspection oversight for the cleared facility. For on-base cleared facilities, this is the SSA. For items 17c and d, include data current as of the time the form is prepared. Suspense receipt of remaining documentation.

gg. **Part VII. Remarks**. Include data as directed above as well as any unique operating conditions worthy of attention to assist the CSO (for cleared facilities) and subsequent SSA representatives to have a clearer understanding of the cleared facility or visitor group.

Chapter 9

SECURITY CONTRACTING DOCUMENTS AND AGREEMENTS

9.1. DD Form 254, DoD Contract Security Classification Specifications:

9.1.1. The DD Form 254 is a legally binding contract document. Its preparation (drafting and revision) is a program manager responsibility. The contracting officer is responsible for ensuring its internal AF coordination and distribution. The SSA and other installation security discipline OPRs review the DD Form 254 to ensure that appropriate and approved security guidance have been incorporated into the contract.

9.1.2. National and DoD policy directs that all potential classified procurement actions contain a DD Form 254 that identifies the security requirements so all prospective contractors understand what is required. As a baseline, security requirements of the NISPOM are applicable to all classified contracts. (See Figure 9.1. and Figures 9.1., Attachment 1 and Attachment 2)

9.1.3. The installation commander has the authority to specify equivalent security safeguards for on-base DoD contractor operations. These equivalent security measures must be clearly specified in the DD Form 254**, Statement of Work (SOW)** or Performance Work Statement (PWS), and Visitor Group Security Agreement (VGSA), when used.

9.1.4. Contract security requirements must be concise, specific, and understandable to the contractor. Unclear, no value added and redundant requirements should be challenged to avoid unwarranted additional costs.

9.1.5. The DD Form 254, VGSA and other referenced contract documents establish contractual requirements on the contractor to provide adequate protection for the classified information for which it has been entrusted.

9.1.6. Identify security requirements at the earliest possible stage of the procurement process, ideally before Milestone Zero. For this reason, establishing and maintaining close contact with the program manager and contracting officer is a must during the preliminary drafting of security requirements that will be applicable to the contract. Plus, it fosters continued SSA, program manager and contracting officer interaction when security related questions or problems arise.

9.1.7. A revised DD Form 254 is required for the various stages of a contract, i.e., bidding stage, awards stage, revision stage or completion stage. Preparation of DD Form 254 at these various stages ensures currency and accuracy.

9.1.8. Pre-award Stage : Prepared to inform the prospective bidders of security requirements associated with the contract.

9.1.9. Award Stage : Prepared to confirm contract security requirements.

9.1.10. Revision Stage : Prepared , as appropriate, to modify or change security requirements. Negotiating changes or modifications to a contract is a contracting officer responsibility.

9.1.11. Completion Stage : Prepared to provide disposition and/or retention instructions, as applicable, per AFMAN 37-139.

9.1.12. In contractual terms, security requirements identified in the DD Form 254 are "deliverables," and must be satisfied as a condition of the agreement or the contractor may be subject to penalty.

Figure 9.1. Instructions for Preparing DD Form 254, DoD Contract Security Classification Specification.

1. General Information

1.1. A classified contract is any contract that requires, or will require, access to classified information by contractor personnel in performance of the contract. (A contract may be a classified contract even though the contract document is not classified.)

1.2. The government provides guidance to prime contractors for classified contracts primarily by incorporating DD Form 254, DoD Contract Security Classification Specification, into every classified contract. The DD Form 254 tells the contractor what needs to be protected and to what degree. The DD Form 254, with its attachments and incorporated references, is the only authorized means for providing security classification guidance to a contractor. It should be written as specifically as possible, and it should include only that information that pertains to the contract for which it is issued. Do not cite government regulations in the DD Form 254. The contractor rarely has the regulation and may be confused by the citing. If access to a regulation is absolutely essential, cite the appropriate regulation in the DD Form 254. The government program manager must ensure the contractor receives a copy of the necessary regulation.

1.3. If any attachment to the DD Form 254 includes classified information, refer to it in Item 13 as a separately transmitted instruction rather than as an attachment. Cite a short title or use whatever means necessary to identify such instructions without inserting classified information on the form. Transmit classified information separately from the DD Form 254.

1.4. The contracting office forward one copy of the DD Form 254 and a copy of the SOW to the SSA for review and coordination purposes. The SSA's coordination is annotated in "Block 13" of the DD Form 254 or a separate attachment, if required.

1.5. The DD Form 254 must be an original, and all entries must be typewritten. Do not staple the DD Form 254 to any other document. For original (new buy) DD Forms 254, enter the Purchase Request (PR) number in pencil in the margin. Corrections made using correction fluid or tape must be neat and legible.

1.6. DD Forms 254 should be forwarded to the SSA for coordination, through the base mail system if time allows.

1.7. The form must contain the signature of the certifying official prior to distribution.

2. Item-By-Item Instructions

2.1. ITEM 1. Clearance and Safeguarding.

2.1.1. 1.a. Insert the highest level of facility clearance required by the contractor for performance of the contract. Use only the words "TOP SECRET," "SECRET," or "CONFIDENTIAL." Special caveats such as RESTRICTED DATA, FORMERLY RESTRICTED DATA, COMSEC INFORMATION, etc., are not appropriate in this item. The contractor must have a valid facility clearance at least as high as the classification indicated in this item.

2.1.2. **1.b.** Insert the highest level of safeguarding capability required by the contractor for performance of the contract. The classification level shown in 1.b. may not be higher than that shown in Item 1.a. If the contractor will not possess classified information at the cleared facility in performing the contract, enter "Not Applicable" (N/A) or "None."

2.1.3. ***NOTE*:** If 11.a. is "YES," safeguarding capability **IS NOT** required. If 11.b. or c. is "YES," safeguarding capability **IS** required.

2.2. ITEMS 2. and 3.

2.2.1. **For an original (new buy) DD Form 254:**

2.2.1.1**. ITEM 2.a.** Insert "X" (Contract number is entered at time of award by contracting official.)

2.2.1.2. **ITEM 2.b.** Do not use. For Prime contractor use only.

2.2.1.3. **ITEM 2.c.** Insert "X" (Solicitation or other number and due date (YYMMDD).

2.2.1.4**. ITEM 3.a.** Insert "X" in block before 3.a. and the current date (YYMMDD).

2.2.2. **For a revised DD Form 254:**

2.2.2.1. **ITEM 2.a.** Enter existing contract number.

2.2.2.2. **ITEM 3.a**. Enter date of original.

2.2.2.3. **ITEM 3.b.** Enter "X," latest revision number, and current date (YYMMDD).

2.2.2.4. ***NOTE:*** The date of the original will appear unchanged on each revised DD Form 254. Any change to DD Form 254 once it has been provided to a contractor either during the solicitation process or upon award, will be made by revising the form. Each time a revision is issued, it shall be given a sequential revision number.

2.2.3. **For a final DD Form 254:**

2.2.3.1. **ITEM 3.a.** Enter date of original.

2.2.3.2. **ITEM 3.b.** Enter latest revision number and date of latest revision (YYMMDD).

2.2.3.3. **ITEM 3.c.** Enter "X" in 3.c. and current date (YYMMDD).

2.2.3.4. ***NOTE:*** When a final DD Form 254 is issued, Item 5 is always marked "YES." Issue a final DD Form 254 only when a contract is completed and retention of the classified material has been authorized, or the material in question is declassified.

2.3. ITEM 4: This item pertains to follow-on contracts. To qualify as a follow-on contract, the new contract must be to the same contractor for the same item or service as the preceding contract. When these conditions exist, enter "X" in the "YES" box, and enter the preceding contract number in the space provided. This item authorizes the contractor to transfer classified material received or generated under the preceding contract to the current contract. It is assumed that the contractor will require access to the same information for performance of the follow-on contract as was required for the previous contract. If the preceding contract is not complete, transfer of accountability is not permitted; enter "X" in "NO." An active contract justifies possession of the classified material.

2.4. ITEM 5. Issue a final DD Form 254 only when a contract is complete and retention of the classified material has been authorized, or the material in question has been declassified. If a final DD Form 254 is being issued, enter "X" in the "YES" box, the date of the contractor's request for retention and the authorized period of retention in the spaces provided. Retention period will not extend beyond 2 years. If a final DD Form 254 is not being issued, enter "X" in "NO."

2.5. ITEM 6.

2.5.1. (This item is completed by the contracting official when the successful offer has been determined.) Enter the name and address of the prime contractor in Item 6.a. as it appears on the contract. Enter the contractor's Cage Code in 6.b. and the name and address of the appropriate DIS cognizant security office (CSO) in 6.c. See attached listing for CSO information.

2.5.2. ***NOTE:*** When applicable, enter the name and address of the prime foreign contractor in Item 6.a., when contract performance is outside the U. S., Puerto Rico, or a U. S. possession, territory, or trust territory. In Item 6.c., enter the name and address of the following government agency who will notify the appropriate security officials of the foreign government responsible for enforcing security requirements in the foreign contractor facility:

Defense Investigative Service

Office of International Programs

1340 Braddock Place

Alexandria, VA 22314-1651

2.5.3. Also, the USAF program/project manager (Item 13) and certifying official (Item 16) must include in the contract document or in Item 13, any special security clauses or physical security requirements necessary by virtue of the foreign location.

2.5.4. All release of classified information to foreign nationals must agree with National Disclosure Policy. Coordinate any classified contract involving foreign disclosure with your Foreign Disclosure office.

2.6. ITEM 7. Enter "N/A" in 7.a., b., and c. (This item is not used by the Air Force, only the prime contractor when subcontracting.)

2.7. ITEM 8. If work is to be performed at another contractor's facility other than as specified in 6.a., enter the appropriate name and address in Item 8.a., the Cage Code in 8.b., and the CSO in 8.c. If work will not be performed at another contractor's facility, enter "N/A" in 8a., b., and c. If work will not be performed at another contractor's facility, but at a government installation, enter "See Item 13" in 8a., and list the performance location in item 13. The CSO is always the DIS Director of Industrial Security who has industrial security jurisdiction over the geographical area in which the contractor is located -- no other activity should be shown in this block. If inspections will be conducted by someone other than the CSO, enter "See Item 15" in 8c and enter that information in Item 15. (See instructions for ITEM 11a., for additional information.)

2.8. ITEM 9. Enter a brief, yet sufficiently complete unclassified statement to identify the nature of the procurement. Use a general description of the procurement. Do not use stock numbers or part numbers.

2.9. ITEM 10.

2.9.1. **10.a. COMSEC INFORMATION.** A contractor who requires access to COMSEC material/ information must submit a request to the appropriate Air Force or National Security Agency (NSA) central office of record through the contracting or program office. If applicable, mark this item "YES." COMSEC information includes accountable or non-accountable COMSEC information and controlled cryptographic items (CCI). If accountable COMSEC information is involved, the contractor must have an Air Force or NSA COMSEC account or be supported by a COMSEC account and Item 11.h should be marked "YES." An "X" in the "YES" box imposes the requirements of the COMSEC Supplement to the NISPOM on the contractor for safeguarding the COMSEC information. If this item is marked "YES," enter the following statement in Item 13:

2.9.1.1. "Ref. 10.a: COMSEC material/information may not be released to DOD contractors without Air Force Cryptological Support Center (AFCSC) approval. Contractor must forward requests for COMSEC material/information to the COMSEC officer through the program office. The contractor is governed by the DOD 5220.22-S COMSEC Supplement to the NISPOM in the control and protection of COMSEC material/information. Access to COMSEC material by personnel is restricted to U. S. citizens holding final U. S. Government clearances. Such information is not releasable to personnel holding only reciprocal clearances."

2.9.2. **10.b. RESTRICTED DATA.** This item will be marked "YES" if access to RESTRICTED DATA, information which is classified and controlled under the Atomic Energy Act of 1954, or CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) is required. This item will always be marked "YES" if Item 10.c. is marked "YES." Access to RESTRICTED DATA requires a final U.S. Government clearance at the appropriate level.

2.9.3. **10.c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION**. This item will be marked "YES" if access to CNWDI is required. Permission of the Air Force is needed prior to subcontracting CNWDI. Special briefings and procedures are also required. Access to CNWDI requires a final U. S. Government clearance at the appropriate level. If this items is marked "YES," enter the following statement in Item 13:

2.9.3.1. "Ref. 10.c. This contractor is permitted access to CNWDI in performance of this contract. The government program manager or designated representative will ensure the contractor security supervisor is briefed for CNWDI."

2.9.3.2. ***NOTE:*** DIS briefs the contractor for access to CNWDI, upon request. The Air Force program official must request this action of the appropriate DIS office if desired. If the program official retains this responsibility, advise the appropriate DIS office in writing.

2.9.4. **10.d. FORMERLY RESTRICTED DATA.** This item will be marked "YES" if access to FORMERLY RESTRICTED DATA is required. Access to FORMERLY RESTRICTED DATA requires a final U. S. Government clearance at the appropriate level.

2.9.5. **10.e. INTELLIGENCE INFORMATION**. SSO coordination is required on each DD Form 254 for contracts involving intelligence releases and should coordinate prior to the SSA. If a determination is made that the contractor will require access to intelligence information during contract performance, the contract monitor prepares the DD Form 254 and routes through SSO for coordination and instructions on release of intelligence information to contractors. The contract monitor will receive instructions from the SSO for SCI or non-SCI (or both if applicable), attach the appropriate one to the DD Form 254, and show as an attachment in Item 14. Item 10.e.(1) or (2) should be marked accordingly. The contract monitor must ensure the appropriate release of intelligence letter is forwarded to SSO after the contract has been awarded and the final DD Form 254 has been processed by the contracting official.

2.9.5.1. If access to SCI intelligence information is required by the contractor, mark 10.e.(1) "YES" and:

2.9.5.1.1. Enter "TOP SECRET" in Item 1.a. and b.

2.9.5.1.2. Mark Item 11.k. "YES." (Defense Courier Service is authorized.)

2.9.5.1.3. Enter "PUBLIC RELEASE OF SCI IS NOT AUTHORIZED" in Item 12.

2.9.5.1.4. Mark 14 and 15 "YES" and enter the following in:

2.9.5.1.4.1. **Item 13:** "Ref. 10.e.(1). Contractor will require access to DCID's 1/7 and 1/19."

2.9.5.1.4.2. **Item 14:** "Ref. 10.e.(1). (List the designated contract monitor's name, telephone number and address, and the designated Special Security Office telephone number and address.) See attached SCI Release of Intelligence Information for additional security requirements. Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefings and a U. S. Government clearance at the appropriate level."

2.9.5.1.4.3. **Item 15:** "Ref. 10.e.(1). The (enter appropriate U. S. Government activity) has exclusive security responsibility for all SCI classified material released to or developed under this contract and held within the contractor's SCIF. DIS is relieved of security inspection responsibility for all such material but retains responsibility for all non-SCI classified material released to or developed under the contract and held within the contractor SCIF." DIA with trained DIS augmentees shall be responsible for reviewing all the contractor's SCIF documentation to ensure compliance with SCI directives or regulations.

2.9.5.1.5. Enter "SSO" in Item 17 and obtain the SSO coordination prior to submitting to the SSA.

2.9.5.2. If access to non-SCI intelligence information is required by the contractor, mark 10.e.(2) and 14 "YES". Mark 15 "NO" and enter the following in:

2.9.5.2.1. **Item 13:** "Ref. 10.e.(2). Contractor will require AFI 14-302 (DCID 1/7) and AFI 14-303."

2.9.5.2.2. **Item 14:** "Ref. 10.e.(2). See attached non-SCI Release of Intelligence Information for additional security requirements. Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefings and a final U. S. Government clearance at the appropriate level."

2.9.5.2.3. **Item 17:** Enter "SSO" and obtain SSO coordination prior to submitting to the SSA.

2.9.5.3. ***NOTE:*** If the contractor requires access to both SCI and non-SCI intelligence information, the contract monitor must use both non-SCI and SCI Release of Intelligence Information Instructions, mark Items 10.e.(1), 10.e.(2), 14 and 15 "YES," and include in Items 13, 14, and 15 all the required information in the previous instructions which apply to all intelligence information releases. Refer questions regarding intelligence information to the local SSO.

2.9.6. **10.f. SPECIAL ACCESS PROGRAM INFORMATION.** A special access program (SAP) is one which is established and approved by the Secretary of the Air Force to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for Top Secret, Secret, or Confidential information. A "carve-out" is a classified contract awarded by the Air Force in connection with a SAP in which DIS has been relieved of security and/or oversight responsibility in whole or in part. Prior approval of the contracting activity is required for subcontracting. Access to SAP information requires a final U. S. Government clearance at the appropriate level.

2.9.6.1. If the contractor is required to have access to a SAP (which is not a "carve out"), mark 10.f. "YES," and enter the following statement in Item 13:

2.9.6.1.1. "Ref. 10.f.: DIS maintains cognizance over the SAP. The inspecting Industrial Security Representative must be briefed into the SAP (insert unclassified nickname) by the government program manager or designated representative prior to access to the SAP material."

2.9.6.2. If the contractor is required to have access to a SAP, but the program office is not the OPR for the SAP, insert the following statement in Item 13:

2.9.6.2.1. "Ref. 10.f.: The OPR for the SAP is not the office shown in Item 13 of this form. However, the contractor requires access to (insert unclassified SAP nickname) material. The contractor must adhere to the special access requirements/procedures developed by the OPR."

2.9.6.3. If the contractor is required to have access to a "carve-out" classified contract, mark Items 10.f. and 14 "YES" and enter the following statement in Item 14:

2.9.6.3.1. "Ref. 10.f: DIS has no responsibility for (insert unclassified nickname) SAP material. (Insert AF symbol and address) has exclusive security responsibility for all SAP material released or developed under this contract."

2.9.7. **10.g. NATO INFORMATION**. This means information belonging to, and circulated by, the North Atlantic Treaty Organization (NATO). Special briefings are required for access to NATO. Prior approval of the contracting activity is required for subcontracting. Access to classified NATO information requires a final U. S. Government clearance at the appropriate level.

2.9.8. **10.h. FOREIGN GOVERNMENT INFORMATION.** This item includes any foreign government information except NATO. Prior approval of the contracting activity is required for subcontracting. Access requires a final U. S. Government clearance at the appropriate level.

2.9.9. **10.i. LIMITED DISSEMINATION INFORMATION (LIMDIS).** This category of information has been abolished. Mark "NO" in all cases.

2.9.10. **10.j. FOR OFFICIAL USE ONLY INFORMATION (FOUO).** When this item is marked "YES," the Air Force is responsible for providing the contractor with the safeguards and procedures necessary for protection of the information. Attach a copy of "Protecting FOUO Information and enter the following statement in Item 13:

2.9.10.1. "Ref. 10.j: FOUO information provided under this contract shall be safeguarded as specified in the attachment "Protecting For Official Use Only (FOUO) Information."

2.9.10. **10.k. OTHER (Specify).** Use this item for any other information not included in 10.a. through j. Specify the type of information and include any additional remarks needed in Item 13.

2.9.11. ***NOTE:*** The access requirements previously listed are included as a part of the form because they are common situations that occur in classified contracts. If they are not applicable to the contract requirements, indicate "NO" for all of them. For those access requirements which are applicable but are not specified by 10.a. through j., add in Item 10.k, "See Item 13," and include appropriate statements in Item 13.

2.10. ITEM 11.

2.10.1. These items are marked "YES" or "NO" according to the requirements of each contract. An explanation of each item follows this illustration. ***NOTE:*** Only one of 11.a., b., or c. may be marked "YES." The other two must be marked "NO."

2.10.1.1. **11.a. HAVE ACCESS ONLY AT ANOTHER CONTRACTOR'S FACILITY OR AT A GOVERNMENT ACTIVITY.** Note the word ONLY. This means there will be no access to classified information related to this contract at the contractor's facility. The contractor will not be required to have safeguarding capability at his facility and Block 1.b. of the DD Form 254 would be marked "N/A" or "NONE." If "YES" is marked for this item, add the following statement in block 13:

2.10.1.1.1. "Ref. 11.a.: Contract performance is restricted to (enter name and address of government activity). Using activity will provide security classification guidance for performance of this contract."

2.10.1.1.2. Insert the following statements in blocks 14, 15, and 17 of the DD Form 254 if contract performance will be on **another** government installation (including overseas):

2.10.1.1.2.1. **Block 14:** "Provide the information requested by the Notification of Government Security Activity Clause, AFFARS 5352.204-9000, and Visitor Group Security Agreements Clause, AFFARS 5352.204.9001, to the Servicing Security Activity (SSA) address in block 17 of this form. Refer to the contract document for these clauses."

2.10.1.1.2.2. **Block 15:** "Industrial Security Reviews, while operating on an Air Force Installation, will be conducted by the SSA."

2.10.1.1.2.3. **Block 17:** (Insert the Servicing Security Activity's address at the operating location.)

2.10.2. 11.b. RECEIVE CLASSIFIED DOCUMENTS ONLY. Note the word ONLY. This means the contractor will receive classified documents, but is not expected to generate classified information or have any classified hardware in performance of the contract. The classification markings shown on the documents will provide the necessary guidance. If the "YES" box is marked for this item, add the following statement in Block 13:

2.10.2.1. "Ref. 11.b: Contractor will receive classified documents for reference only; however, if any classified information is generated in performance of this contract, it shall be derivatively classified and marked consistent with the source material. (Reference applicable security classification guide)"

2.10.2.2. ***NOTE:*** If this item is marked "YES," the contractor will be required to have safeguarding capability at their facility, therefore mark 1.b. as required.

2.10.3. **11.c. RECEIVE AND GENERATE CLASSIFIED INFORMATION.** This means the contractor is expected to receive and generate classified information (documents and/or hardware) and will require detailed security classification guidance for performance of the contract. If the YES box is marked for this item, detailed security classification guidance must be provided to the contractor. Detailed guidance is usually contained in a security classification guide. The guidance may be included in Item 13, attached to the DD Form 254, forwarded under separate cover, or included in the contract document itself. Statements, as appropriate, shall be included in Item 13 to direct the contractor to the guidance for the contract. References to SCGs should include the title, date and a list of all changes and dates.

2.10.3.1. ***NOTE:*** If this item is marked "YES," the contractor will be required to have safeguarding capability at his facility, therefore mark 1.b. as required. Marking 11.c. "YES" permits contract performance at both the contractor's facility and at a government activity. If work will be performed at a government activity as well as the prime contractor's facility, refer to instructions for ITEM 11a. for additional information.

2.10.4. **11.d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE.** If "YES" and the hardware is of a size and/or quantity that prohibits storage in a standard (2 cubic feet) container, enter the following statement in Item 13:

2.10.4.1. "Ref. 11.d: Contractor must provide adequate storage for classified hardware to the level of (enter Top Secret, Secret, or Confidential) which exceeds two cubic feet but not more than _____ cubic feet."

2.10.5. **11.e. PERFORM SERVICES ONLY.** "YES" in this item will require a statement in Item 13 to explain the services and to provide appropriate guidance. Sample statements are given below. For service-type contracts not covered, add any appropriate statement in Item 13 that explains why the contract is a classified contract and provide guidance as necessary to ensure protection of the classified information.

2.10.5.1. For ENGINEERING SERVICES, add the following statement in Item 13:

2.10.5.1.1. "Ref. 11.e.: Contract is for engineering services. Classification markings on the material to be furnished will provide the guidance necessary for performance of the contract."

2.10.5.2. For EQUIPMENT MAINTENANCE SERVICES, add the following statement in Item 13:

2.10.5.2.1. "Ref. 11.e: Contract is for equipment maintenance services on equipment which processes classified information. Actual knowledge of, generation, or production of classified information is not required for performance of the contract. Cleared personnel are required to perform this service because access to classified information cannot be precluded by escorting personnel."

2.10.5.3. For a service contract in which the contractor is only required to be physically present in an area containing classified information and security measures which are in force do not prevent the gaining of knowledge of classified information, add the following statement in Item 13:

2.10.5.3.1. "Ref. 11.e.: Actual knowledge of, generation, or production of classified information is not required for performance of the contract. Cleared personnel are required to perform this service because security measures which are in force do not preclude access to classified information."

2.10.6. **11.f. HAVE ACCESS TO U. S. CLASSIFIED INFORMATION OUTSIDE THE U. S., PUERTO RICO, U. S. POSSESSIONS AND TRUST TERRITORIES.** If "YES," indicate city and country of overseas performance in Item 13. Item 14 may be "YES" and should be completed if appropriate. A copy of the DD Form 254 must be provided to the U. S. Air Force servicing security activity responsible for overseas inspections. Under 17.d. type "USAFE/SPI" or "HQ PACAF/SPI" as applicable. Provide a copy to the SSA where any work will be performed under terms of the contract.

2.10.7. **11.g. BE AUTHORIZED TO USE THE SERVICES OF DTIC OR OTHER SECONDARY DISTRIBUTION CENTER.** "YES" in this item means the contractor is authorized to use the services of DTIC and will require the contractor to prepare and process DD Form 1540 and DD Form 1541. In authorizing the use of this service, the contracting official must critically review and clearly establish a contractor's need-to-know for DTIC scientific and technical information before approving the DD Form 1540 and 1541. The contracting official, with concurrence of the program/ project manager, must ensure specific fields of interest are identified only as they relate to the contract.

2.10.8. **11.h. REQUIRE A COMSEC ACCOUNT.** If accountable COMSEC information will be provided to the contractor, enter an "X" in the YES box. If non-accountable COMSEC information is involved, enter an "X" in the NO box. (See Item 10.a.)

2.10.9. **11.i. HAVE EMSEC (TEMPEST) REQUIREMENTS.** Contractors are required to comply with EMSEC (TEMPEST) requirements according to AFI 33-203. If EMSEC requirements for the contract are over and above those normally called for in the NISPOM, the government program manager and the contracting official must ensure such requirements are specifically included in the contract. Contractor shall not implement specific EMSEC countermeasures nor shall they impose any EMSEC requirements on a subcontractor without prior approval of the Air Force. Contact the Wing Information Protection Office for information concerning EMSEC requirements. If EMSEC requirements are in addition to those specified in the NISPOM, mark 11.i. and 14 "YES" and enter the following statement in Item 14:

2.10.9.1. "Ref. 11.i.: See Contract Clause No. _____ (enter clause number) for additional EMSEC requirements."

2.10.9.2. ***NOTE:*** See AFI 33-203, *The Air Force Emission Security Program,* for additional guidance and requirements.

2.10.10. **11.j. HAVE OPSEC REQUIREMENTS.** The NISPOM does not require the contractor to implement or comply with OPSEC requirements, unless these special security requirements are specifically incorporated into the contract. If OPSEC requirements are required, the government program manager and the contracting official must included such requirements in the contract. Imposing OPSEC requirements will added additional costs to the contract. A contractor shall not implement OPSEC requirements nor shall they impose any OPSEC requirements on a subcontractor without prior approval of the Air Force. If OPSEC requirements are imposed, mark 11.j. and 14 "YES" and enter the following statement in Item 14:

2.10.10.1. "Ref. 11.j: See Contract Clause No. _____ (enter clause number) for additional OPSEC requirements."

2.10.11. **11.k. AUTHORIZED USE OF THE DEFENSE COURIER SERVICE.** This item authorizes the contractor to use the services of DCS. "YES" in this item requires the contracting activity to request DCS services from the Commander, Defense Courier Service, ATTN: Operations Division, Fort George G. Meade, MD 20755-5370. Only certain classified information qualifies for shipment by DCS. It is the responsibility of the contracting activity to comply with DCS policy and procedures. (This item will be marked "YES" when Blocks 1a and 1b are marked TOP SECRET, when 10a and 11h are marked "YES," and when 10e(1) is marked "YES.")

2.10.12. **11.l. OTHER (Specify).** Use this term to add any additional performance requirements, i.e., automated information systems (AISs) processing not covered above. Item 13 should be appropriately annotated to provide any necessary remarks.

2.11. ITEM 12.

2.11.1. The contractor must obtain permission from the Air Force, prior to public release of any information, regardless of classification, under the contract. Enter "X" in the THROUGH block and enter the local public affairs office in the space provided.

2.11.2. If release is not authorized, enter "NONE AUTHORIZED."

2.12. ITEM 13.

2.12.1. This is the most important part of the entire DD Form 254. This item, when properly completed, will convey to the contractor the applicable classification and declassification specifications for the classified information involved in the contractual effort.

2.12.1.1. If a security classification guide exists, reference it in this item. List all guides if more than one applies. The reference must include the title and date of the guide. If the entire guide does not apply to this contract, cite only the specific portions which apply, such as "Only Section IV of the security classification guide applies to this effort."

2.12.1.2. NEVER insert specific guidance, such as "Transmitter frequency classified SECRET."

2.12.1.3. If specific guidance is required, and there is no guide for the program, develop a letter guide. An authorized original classification authority must sign all guides, no matter what the form. (Individuals developing letter guides are encouraged to seek the advice and assistance of the SSA.

2.12.1.4. USAF PROGRAM/PROJECT MANAGER: Enter the information as requested. Ensure this item has a signature prior to submitting to the SSA for coordination. The SSA will coordinate in the space provided. (There should be no changes made to the form after the SSA coordination unless those changes are coordinated with the SSA.)

2.13. ITEM 14. This item applies any time security requirements are imposed on a contractor that are in addition to the requirements of the NISPOM or its Supplements. "YES" in this item requires the contracting activity to incorporate the additional requirements in the contract document itself, or to incorporate the additional requirements by statements or reference in Item 13. Attendant costs incurred due to additional security requirements are subject to negotiation by, and reimbursement to, the contractor and are the responsibility of the contracting activity imposing the additional requirements. A copy of the additional security requirements shall be provided to the cognizant security office. Examples of additional security requirements are:

2.13.1. SCI.

2.13.2. Special Access Programs.

2.13.3. EMSEC.

2.13.4. OPSEC.

2.14. ITEM 15. This item applies when the CSO is relieved of inspection responsibility in whole or in part. "YES" in this item requires the Air Force to provide information on the specific area DIS is relieved of inspecting and to identify the activity responsible for inspection. A copy of the DD Form 254 must be provided to the appropriate CSO or to the servicing security activity for overseas performance. Refer to ITEM 11a. for more information.

2.15. ITEM 16. The contracting official completes the requested information in this item. (The DD Form 254 is not considered a valid document unless this item has been completed.)

2.16. ITEM 17. Items 17.a., c., e., and f. (the SSA) will appear marked on the overprinted form. If contract performance will occur overseas enter "X" in 17.d. and add "USAFE/SPI" or "PACAF/SPI" and any other geographic location where work will be performed (see 11.a. and f. these instructions). If Item 10.e.(1) or (2) are marked "YES," add "SSO" to this item and obtain the local SSO coordination prior to submitting to the SSA for coordination. If contract performance will occur at a military installation (other than overseas), add the address of the servicing security activity. If contract performance will occur at

many locations, type in "SEE ATTACHED" in Item 17 and attach a list of locations with the address of the servicing security activity for each. You may also put your office symbol in this block to receive a copy of the DD Form 254 for the awarded contract.

Figure 9.2. Attachment 1, Sample Release of Non-SCI Intelligence Information to DoD Contractors DD Form 254 Attachment.

ATTACHMENT TO DD FORM 254 FOR CONTRACT NO: _____

CONTRACT EXPIRATION DATE:

RELEASE OF NON-SENSITIVE COMPARTMENTED INFORMATION (NON-SCI) INTELLIGENCE INFORMATION TO US CONTRACTORS

1. Requirements for access to non-SCI:

a. All intelligence material released to the contractor remains the property of the US Government and may be withdrawn at any time. Contractors must maintain accountability for all classified intelligence released into their custody.

b. The contractor must not reproduce intelligence material without the written permission of the originating agency through the Intelligence Support Office. If permission is granted, each copy shall be controlled in the same manner as the original.

c. The contractor must not destroy any intelligence material without advance approval or as specified by the contract monitor (CM). (EXCEPTION: Classified waste shall be destroyed as soon as practicable in accordance with the provisions of the Industrial Security Program).

d. The contractor must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract with a valid need to know. Further dissemination to other contractors, subcontractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the originating agency through the CM.

e. The contractor must ensure each employee having access to intelligence material is fully aware of the special security requirements for this material and shall maintain records in a manner that will permit the contractor to furnish, on demand, the names of individuals who have had access to this material in their custody.

f. Intelligence material must not be released to foreign nationals or immigrant aliens whether they are consultants, US contractors, or employees of the contractor and regardless of the level of their security clearance, except with advance written permission from the originator. Requests for release to foreign nationals shall be initially forwarded to the contract monitor and shall include:

(1) A copy of the proposed disclosure.

(2) Full justification reflecting the benefits to US interests.

(3) Name, nationality, particulars of clearance, and current access authorization of each proposed foreign national recipient.

g. Upon completion or termination of the classified contract, or sooner when the purpose of the release has been served, the contractor will return all classified intelligence (furnished or generated) to the source from which received unless retention or other disposition instructions (see AFMAN 37-139) are authorized in writing by the CM.

h. The contractor must designate an individual who is working on the contract as custodian. The designated custodian shall be responsible for receipting and accounting for all classified intelligence material received under this contract. This does not mean that the custodian must personally sign for all classified material. The inner wrapper of all classified material dispatched should be marked for the attention of a designated custodian and must not be opened by anyone not working directly on the contract.

i. Within 30 days after the final product is received and accepted by the procuring agency, classified intelligence materials released to or generated by the contractor, must be returned to the originating agency through the contract monitor unless written instructions authorizing destruction or retention are issued. Requests to retain material shall be directed to the CM for this contract in writing and must clearly indicate the justification for retention and identity of the specific document to be retained.

j. Classification, regrading, or declassification markings of documentation produced by the contractor shall be consistent with that applied to the information or documentation from which the new document was prepared. If a compilation of information or a complete analysis of a subject appears to require a security classification other than that of the source documentation, the contractor shall assign the tentative security classification and request instructions from the contract monitor. Pending final determination, the material shall be safeguarded as required for its assigned or proposed classification, whichever is higher, until the classification is changed or otherwise verified.

2. Intelligence material carries special markings. The following is a list of the authorized control markings of intelligence material:

a. "Dissemination and Extraction of Information Controlled by Originator (ORCON)." This marking is used, with a security classification, to enable a continuing knowledge and supervision by the originator of the use made of the information involved. This marking may be used on intelligence which clearly identifies, or would reasonably permit ready identification of an intelligence source or method which is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may not be used when an item or information will reasonably be protected by use of other markings specified herein, or by the application of the "need-to-know" principle and the safeguarding procedures of the security classification system.

b. "Authorized for Release to (Name of Country(ies)/International Organization." The above is abbreviated "REL _____." This marking must be used when it is necessary to identify classified intelligence material the US government originator has predetermined to be releasable or has been released through established foreign disclosure channels to the indicated country(ies) or organization.

3. The following procedures govern the use of control markings.

a. Any recipient desiring to use intelligence in a manner contrary to restrictions established by the control marking set forth above shall obtain the advance permission of the originating agency through the CM. Such permission applies only to the specific purposes agreed to by the originator and does not automatically apply to all recipients. Originators shall ensure that prompt consideration is given to recipients' requests in these regards, with particular attention to reviewing and editing, if necessary, sanitized or paraphrased versions to derive a text suitable for release subject to lesser or no control markings.

b. The control marking authorized above shall be shown on the title page, front cover, and other applicable pages of documents, incorporated in the text of electrical communications, shown on graphics, and associated (in full or abbreviated form) with data stored or processed in automatic data processing systems. The control marking also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions. If the control marking applies to several or all portions, the document must be marked with a statement to this effect rather than marking each portion individually.

c. The control markings shall be individually assigned at the time of preparation of intelligence products and used in conjunction with security classifications and other marking specified by E.O. 12958 and its implementing security directives. The marking shall be carried forward to any new format in which the same information is incorporated including oral and visual presentations.

4. Request for release of intelligence material to a contractor must be prepared by the contract monitor (CM) and submitted to the Intelligence Support Office. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirements and copies of the DD Form 254 and Statement of Work.

Figure 9.3. Attachment 2, Sample Release of SCI Intelligence Information to DoD Contractors DD Form 254 Attachment.

ATTACHMENT TO DD FORM 254 FOR CONTRACT NO:_____

NUMBER OF SCI BILLETS AUTHORIZED: _____

CONTRACT EXPIRATION DATE: _____

RELEASE OF SENSITIVE COMPARTMENTED INFORMATION (SCI) INTELLIGENCE INFORMATION TO US CONTRACTORS

1. Requirements for access to SCI:

a. All SCI will be handled in accordance with special security requirements which will be furnished by the designated responsible special security office (SSO).

b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.

c. Names of contractor personnel requiring access to SCI will be submitted to the contract monitor (CM) for approval. (The contract monitor is identified on the reverse side of the DD Form 254.) Upon receipt of written approval from the CM, the company security officer will submit request(s) for special background investigations in accordance with the NISPOM, to the Intelligence Support Office. The entire personnel security questionnaire package should not be forwarded to the Intelligence Support Office. The Contractor Special Security Officer (CSSO) must follow the instructions provided by the Intelligence Support Office to the CSSO.

d. Inquiries pertaining to classification guidance on SCI will be directed through the CSSO to the responsible CM as indicated on the DD Form 254.

e. SCI furnished in support of this contract remains the property of the Department of Defense (DoD) department, agency, or command originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the CM.

f. SCI will be stored and maintained only in properly accredited facilities at the contractor location.

2. The contract monitor (CM) will:

a. Review the SCI product for contract applicability and determine that the product is required by the contractor to complete contractual obligations. After the CM has reviewed the SCI product(s) for contract applicability and determined that the product is required by the contractor to complete obligations, the CM must request release from the originator through the Intelligence Division. Originator release authority is required on the product types below:

(1) Documents bearing the control markings of ORCON, PROPIN.

(2) GAMMA controlled documents.

(3) Any NSA/SPECIAL marked product.

(4) All categories as listed in USAF Intel 201-1.

b. Prepare or review contractor billet/access requests to insure satisfactory justification (need-to-know) and completeness of required information.

c. Approve and coordinate visits by contractor employees when such visits are conducted as part of the contract effort.

d. Maintain records of all SCI material provided to the contractor in support of the contract effort. By 15 January (annually), provide the contractor, for inventory purposes, with a complete list of all documents transferred by contract number, organizational control number, copy number, and document title.

e. Determine dissemination of SCI studies or materials originated or developed by the contractor.

f. Within 30 days after completion of the contract, provide written disposition instructions for all SCI material furnished to, or generated by, the contractor with an information copy to the supporting SSO.

g. Review and forward all contractor requests to process SCI electronically to the accrediting SSO for coordination through appropriate SCI channels.

h. Request for release of intelligence material to a contractor must be prepared by the contract monitor (CM) and submitted to the Intelligence Support Office. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirement and copies of the DD Form 254 and Statement of Work.

9.2. Visit Group Security Agreement (VGSA):

9.2.1. DoD security policy does not specifically provide direction on visitor groups. However, all security requirements contractually imposed on a contractor are legally binding and as such, appropriate language (contract security requirements clause) should be inserted into agreements which establish visitor groups and ultimately drives the Visitor Group Security Agreement (VGSA). (See recommended security clause verbiage at paragraph 9.2.5.1.1.)

9.2.2. The Visitor Group Security Agreement (VGSA) is a documented and legally binding contractual agreement between an Air Force activity and a DoD contractor, whereby the contractor commits to rendering or performing specific security services for compensation. The VGSA attests to and certifies the existence of such an agreement, including applicable changes, and amendments, attachments, supplements and exhibits.

9.2.3. The VGSA is customized to suit the operational needs of the AF activity and the installation. The VGSA provides operational efficiency and flexibility.

9.2.4. The VGSA may be used to impose negotiated contractual security requirements upon the contractor. Like the DD Form 254, the VGSA must be coordinated with those security discipline OPRs and other AF entity that imposes requirements on the contractor via the agreement.

9.2.5. The VGSA may be used to specify security requirements and/or to provide security classification guidance in support of on-base classified work efforts.

9.2.5.1. When visitor group security agreements are contemplated, include the clause at AFFARS 5352.204.9011 in solicitations and contracts.

Figure 9.4. Sample Visitor Group Security Agreement (DoD 5200.1-R/AFI 31-401 Specific).

VISITOR GROUP SECURITY AGREEMENT

1. Contractual Agreement: This agreement, promulgated by DoD 5220.22-R, *Industrial Security Regulation* and DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Chapter 1, Section 2, Paragraph 1-200, is entered into by the Installation Commander, **(insert name of installation)** Air Force Base (AFB), and **(insert commercial name of company),** (hereafter referred to as visitor group), prescribes the specific actions to be taken by the visitor Group's employees and the Department of the Air Force (DAF), to properly protect classified information involved in the on-base contract performance at the visitor group's on-base operating location (insert physical operating location). Responsibilities are delineated as follows: **NOTE: As used in this agreement, the terminology visitor group, contractor, company, and home office facility (HOF) are synonymous. Furthermore, the verbiage Air Force (AF) activity, unit, contracting officer, program/project manager, Servicing Security Activity (SSA), etc., refers to entities or representing of the DAF in their appropriate and respective capacity.**

a. **Visitor Group Security Supervision.** Under the terms of this agreement, the visitor group will operate per DoD 5200.1-R, *Information Security Program Regulation,* Air Force Instruction 31-401, *Information Security Program Management,* and supplements thereto, and the Air Force (AF) activity's unit security program operating instructions (OIs), plans and/or procedures. The installation servicing security activity (SSA) is responsible for providing security program oversight and the AF activity is responsible for implementing and managing the AF activity security program per DoD 5200.1-R and AFI 31-401.

(1) The visitor group's home office facility (HOF) will identify (in writing) to the SSA and AF activity an on-base employee to interface with and serve as the visitor group's focal point for security related matters. Under the terms of this agreement, the identified employee per this paragraph, will provide appropriate security program management assistance to the AF activity's unit security manager.

(2) The visitor group's HOF's will provide the SSA and AF activity unit security manager the name of the HOF's Facility Security Officer (FSO) and the SSA will likewise provide the visitor group's FSO with the names of the SSA Information Security Specialist and the activity's unit security manager.

(3) All parties, the AF activity, contracting office (sponsor), visitor group, and SSA will perform duties specified by this agreement in a timely manner.

b. **Standard Practice Procedures (SPP):** Compliance with this agreement eliminates SPP publication requirement. The visitor group will use and comply with the AF activity's unit security program operating instructions (OIs), procedures and/or requirements, per this agreement and other applicable

DoD or AF directives. This provision of the agreement is not intended nor does it interfere with the visitor group's internal management policies, procedures, or requirements unless stated otherwise.

c. **Access to and Accountability of Classified Material:**

(1) All access to and/or possession of classified material by on-base visitor group personnel, including oral and/or visual at (insert name of installation), will be under the AF activity's supervision. The AF activity maintains accountability, control, and ownership of all classified information involved under the terms of this contract at all times per DoD 5200.1-R and AFI 31-401. The visitor group's access to classified information will be controlled by the AF activity and limited to "contract-specific, need-to-know" information only.

(2) The visitor group receives, releases, and disseminates classified material at (insert AF activity designation and name of installation) in accordance with DoD 5200.1-R, *Information Security Program*, AFPD 31-4, *Information Security* and AFI 31-401, *Information Security Program Management.*

(3) If contractor personnel during contract performance discover unattended classified material or an insecure/unattended security container they will immediately secure the classified materials and notify the AF activity's unit security manager. During non-duty hours visitor group personnel will notify the security police law enforcement desk at (insert Security Police unit designation and Law Enforcement Desk telephone number). Classified material will be turned over to the base security police when the AF designated safe custodian cannot be contacted.

d. **Storage of Classified Material:**

(1) The visitor group is authorized to store and handle classified information in accordance with DoD 5200.1-R, AFI 31-401, and the AF activity's unit operating instructions (OIs). All classified information shared with the visitor group must be stored in an approved government owned and controlled security container. The contractor is prohibited from establishing and/or maintaining a separate classified information system. All classified material will be returned and secured in the designated government security container at the end of the duty day.

(2) Under the terms of this agreement, the AF activity will have access to and control all security containers. The responsibility for setting the storage container combination rests with the AF activity. Each container will have a government safe custodian appointed. The Standard Form (SF) 700, **Security Container Information,** will be used to identify persons having knowledge of the combination(s). This form will be posted inside the locking drawer of each security container.

e. **Transmission of Classified Material:**

(1) The on-base visitor group is not authorized for direct receipt or dispatch of classified material at **(insert name of installation)** through U.S. postal channels or commercial carrier.

(2) Classified material is to be transmitted via U.S. postal channels directly from **(insert identification of AF activity)** and must be prepared in accordance with DoD 5200.1-R, AFI 31-401, and processed through the classified information control system of **(insert name of installation).**

(3) Classified material may be handcarried onto or off (insert name of installation) by an appropriately cleared and briefed visitor group courier, provided the employee is so designated in writing by the contractor as a courier, and the AF activity's commander or designee per DoD 5200.1-R and AFI 31-401.

f. Disposition of Classified Material. The visitor group will return all classified information jointly shared and/or involved, under the terms of this agreement, to the AF activity at the end of contract performance or when no longer required, unless authorized to do otherwise by the contracting officer.

g. Reproduction of Classified Material. Only AF approved and controlled reproduction equipment will be used by the visitor group, when so authorized, per DoD 5200.1-R and AFI 31-401. The visitor group can not reproduce classified material without permission of the AF activity.

h. Security Education. The visitor group's security focal point shall:

(1) Conduct and/or ensure employees who requires access to classified information receive initial and recurring security education training (at least annually) regarding their individual responsibility for safeguarding classified information. These briefings should be tailored to those responsibilities associated with the individual's assigned duties, the provisions of this agreement, any associated DD Form 254, and the results of the most recent self-inspections or security reviews (as applicable). The AF activity will be responsible for administering security education training per DoD 5200.1-R and AFI 31-401.

(2) Conduct and/or ensure employees are briefed and complete the Standard Form (SF) 312, **Classified Information Nondisclosure Agreement.** Once completed, the SF 312 will be retained on file at the visitor group's HOF. Certification of accomplishment of part 1 of the SF 312 will be included in the visit request. Visitor group employees will be debriefed in accordance with DoD 5200.1-R and the debriefing will be recorded on AF Form 2587, **Security Termination Statement.** The AF Form 2587 will be maintained by the AF activity's unit security manager and destroyed in accordance with AFMAN 37-139, **Disposition of Air Force Records - Records Disposition Schedule.**

(3) Conduct and/or ensure employees attend and participate in the AF activity's Security Education and Awareness Training Program, per DoD 5200.1-R and AFI 31-401.

i. Personnel Security Clearances. The visitor group's HOF will submit (VALs **(insert frequency - annually or duration of contract)** for on-base employees to the AF activity's unit security manager, per DoD 5200.1-R and DoD 5220.22-M. The VAL will include certification and compliance with of SF 312 requirements. A copy of the VAL will be forwarded to and retained by the on-base visitor group's management. The AF activity (contracting officer) serves as sponsor for the visits.

j. Reports. The visitor group must immediately submit to the SSA, in writing, reports required under any of the situations outlined in DoD 5200.1-R and AFI 31-401. The SSA coordinates and/or reports security violations committed by visitor group employees to the appropriate Defense Investigative Service (DIS) Cognizant Security Agency (CSA), base contracting office, and the visitor's group HOF, if and when appropriate. The visitor group must keep the AF activity and SSA advised of any reports submitted per AFI 71-105, *Counterintelligence Awareness and Briefing Program.*

(1) The AF activity's unit commander appoints inquiry or investigation officials. Inquiry or investigation officials coordinate findings and reports with the appointing official and SSA.

(2) The visitor group's HOF will advise the SSA of any changes in management, location, address, or contractual performance requirements.

k. Contractor Restricted Area Badges. When required for contract performance, the AF Form 1199 Series (Green, Pink, Yellow or Blue), **USAF Restricted Area Badge,** will be issued to visitor group personnel for entry into USAF Restricted Areas on **(insert name of installation).** Entry credentials are issued at the request of the AF activity. Request for badge issuance must be supported by a current VAL.

l. Contractor Local Area Badges. When required for contract performance locally developed installation badges **(list the form number)** will be issued to visitor group personnel for entry into designated areas. Entry credentials are issued at the request of the AF activity.

m. Security Checks. Visitor group personnel will be scheduled to perform end-of-day security checks within their assigned work areas by the AF activity per DoD 5200.1-R, AFI 31-401, and AF activity's security program OI. These checks will ensure security precautions are taken to protect classified material. The Standard Form 701, **Activity Security Checklist,** and Standard Form 702, **Security Container Check Sheet,** will be used to record these checks.

n. Emergency Protection. The visitor group will make every effort to secure all classified material in an approved storage container in the event of a natural disaster, major accident, or civil disturbance per DoD 5200.1-R, AFI 31-401, and AF unit's security program OIs. If the area is evacuated and/or the container(s) abandoned, the visitor group employees will, upon termination of the emergency condition, examine classified holdings to ensure there has been no compromise or loss of exposed information. In the event of missing material or possible compromise, the visitor group employees will immediately notify the AF activity's unit security manager.

o. Protection of Government Resources. The visitor group will comply with AFI 31-209, *The Air Force Resource Protection Program*, and other security and safety OIs of the AF activity. File systems containing classified records will be maintained in accordance with AFMAN 37-123, and publication files are maintained per AFI 37-160V7, *Publication Libraries and Sets*.

p. Clarification of Security Requirements. The visitor group will address inquiries or questions pertaining to the provisions of DoD 5200.1-R and AFI 31-401 to the AF activity's unit security manager.

q. Contract and Associated DD Form 254. The visitor group's on-base management will maintain on file a copy of all contracting documents, any associated DD Form 254, **DoD Contract Security Classification Specification,** and this VGSA. The responsible AF activity will review the DD Form 254 at least biennial and will issue revisions as necessary.

r. Foreign Involvement: Under the terms of this agreement, the visitor group is required to notify the AF activity and contracting office, prior to any foreign involvement, regardless of access requirements or the sensitivity of information to be disclosed (classified or unclassified).

2. Security Reviews:

a. Staff Assistance Visits (SAVs), Information Security Program Reviews (PRs), or self-inspections will not be conducted by the SSA of the visitor group, independent of the AF activity.

b. The SSA conducts PRs, if applicable, in the following manner:

(1) The SSA will notify and schedule all PRs through the AF activity's unit security manager. PRs will be conducted per DoD 5200.1-R, AFI 31-401, supplements thereto, and this agreement. A copy of PR report will be provided to the visitor group by the AF activity. The visitor group is not required to acknowledge receipt, nor respond unless directed to do so in the report.

(2) The AF activity's PR or self-inspection will include the visitor group. The visitor group will also be included in the AF activity's semiannual security self-inspection program. The AF activity will use the VGSA and the unit's self-inspection criteria to monitor the visitor group's performance and compliance. Document and maintain the inspection report as required by DoD 5200.1-R and AFI 31-401.

3. Expenditure of Funds for Security. This agreement is not an authorization for a commitment of funds. Nothing in this agreement shall be construed to impose any liability on the part of the U.S. government for injury to the agents, employees of the visitor group, its subcontractors, assignees, or other individuals acting for or on behalf of the visitor group, to the property of the same, nor shall anything in this agreement be construed to modify the provisions of existing contracts.

4. Review of this Agreement. All parties must review this agreement at least annually for accuracy. The AF activity is responsible for keeping this agreement current. In addition, the AF activity will keep on file a copy of the last evaluation, self-inspection or equivalent review. copies of reports may be made available to the visitor group for their files.

5. Other:

a. Forms. The AF activity furnishes all government forms and applicable AFIs, OIs, and/or unit security plans required in support of this agreement.

b. Sub-contracts. A VGSA shall be initiated whenever the HOF or on-base visitor group enters into a sub-contract arrangement with another contractor for classified performance on **(insert name of installation).** This VGSA must address the subcontractor operation separately. The AF activity, visitor group or it's HOF, as applicable, and all sub-contractors must sign the agreement. A separate DD Form 254 is completed for each subcontractor requiring access to classified information. The visitor group or it's HOF, as applicable, is responsible for preparing the DD Form 254 for any subcontractors and must provide a copy to the SSA for review. The AF activity ensures that all questions pertaining to the DD Form 254 are resolved. The visitor group or it's HOF signs item 16 of the DD Form 254 for subcontracts and makes required distribution.

c. Notification. Notify the SSA 30 days prior to contract completion or shutdown on **(insert name of installation)** in order to review contractor's operations to ensure proper disposition of classified materials per DoD 5200.1-R, AFI 31-401, and this security agreement.

d. Government Liability. Nothing in this agreement shall be construed to impose any liability on the part of the US government for injury to the agents, employees of the contractor, its subcontractors, assignees, or other individuals acting for or on behalf of the contractor, to the property of the same, nor shall anything in this agreement be construed to modify the provisions of existing contracts.

_____ _____

Installation Commander or Designee Visitor Group - Executive Manager

Date: _____ Date: _____

_____ _____

Program Manager (Government) Contracting Officer or Designee

Date: _____ Date: _____

Figure 9.5. Sample Visitor Group Security Agreement (Installation Security Program Specific).

VISITOR GROUP SECURITY AGREEMENT

1. **Contractual Agreement:** This agreement, entered into by the Installation Commander, **(insert name of installation)** and **(insert commercial name of company),** hereafter referred to as "visitor group." It prescribes the specific actions to be taken by the visitor group's employees and the Department of the Air Force (DAF), to properly protect classified information involved in the on-base contract performance at the visitor group's on-base operating location (insert physical operating location). Responsibilities are delineated as follows: **(*NOTE:* As used in this agreement, the terminology visitor group, contractor, company, and/or home office facility (HOF) are synonymous. Furthermore, the verbiage Air Force (AF) activity, unit, contracting officer, program/project manager, SSA, etc., refers to entities or representatives of the DAF in their appropriate and respective capacity.)**

a. Visitor Group Security Supervision. Under the terms of this agreement, the visitor group will operate under the guidance and requirements of the Installation Security Program, **(insert applicable Installation Security Program Directive)** and the AF activity's unit operating instructions (OIs). The servicing security activity (SSA) is responsible for providing security program oversight and guidance.

(1) The visitor group's home office facility (HOF) will identify (in writing) to the SSA an on-base employee to interface with and serve as the visitor group's (i.e., security manager, focal point, Facility Security Officer , etc.) for security related matters.

(2) The visitor group's HOF's will provide the SSA the name of the HOF's Facility Security Officer (FSO) and the SSA will likewise provide the HOF FSO with the names of the SSA Information Security Specialist.

b. Standard Practice Procedures (SPP). Compliance with this agreement eliminates SPP publication requirements. The visitor group will use and comply with the installation's or activity's security operating instructions (OIs), procedures, and/or requirements, per this agreement and other applicable DoD or AF directives. This provision of the agreement is not intended nor does it interfere with the visitor group's internal management policies, procedures, or requirements, unless otherwise stated.

c. Access to and Accountability of Classified Material:

(1) All access to, or possession of classified material by contractor personnel, including oral and visual at **(insert name of installation)** will be under supervision and control of the AF activity.

(2) The contractor will establish an information management system and control classified material in accordance with Chapter 5, Section 2, NISPOM, installation security program requirements, and pertinent command security instructions.

(3) Contractor personnel discovering unattended classified material or an insecure/unattended classified container will immediately notify the project manager and Installation Law Enforcement Desk at **(insert telephone number).** Material will be turned over to Security Police for safeguarding, if the appropriate classified custodian can not be contacted.

d. Storage of Classified Material:

(1) The visitor group is not authorized to store classified material independent of the AF activity. Storage containers will be furnished by the AF activity **(insert AF activity's designation).**

(2) Storage containers furnished to the contractor will remain under control of the AF activity **(insert AF activity's designation).** The responsibility for setting the storage container combination rests with the visitor group. The visitor will not use government or private locksmiths to set the combination Standard Form (SF) 700, **Security Container Information,** or equivalent visitor group form, will be used to identify persons having knowledge of the combinations. This form will be posted inside the locking drawer of each security container.

e. **Transmission of Classified Material:**

(1) The visitor group is not authorized direct receipt or dispatch of classified material. Classified information will be transmitted to and through AF base classified information control system via US Postal Channels. For postal receipt the visitor group will use the address of the office of the AF activity, with an attention line indicating the visitor group's on-base operation designation.

(2) Classified material which is to be transmitted by US postal channels directly from AF installation must be prepared in accordance with current installation security program requirements and processed through the base classified information control system.

(3) The visitor group employees may handcarry classified material on or off-base, provided the employee is so designated in writing by a visitor group management official as an official "Visitor Group Courier," and has been briefed regarding his/her responsibilities under Chapter 5, Section 4, NISPOM. The removal will be recorded in the visitor group dispatch records.

f. **Disposition of Classified Material.** The visitor group will return to the **(insert AF activity's designation)** all classified material furnished by the AF activity, including all reproductions thereof, and will surrender all classified material developed by the visitor group in connection with the contract or program when no longer required. Any other disposition must be coordinated with the AF activity and approved by the contracting officer.

g. **Security Education. The contractor shall:**

(1) On a recurring basis, but not less than annually, brief on-base visitor group employees whose duties require access to or safeguarding classified information per Chapter 3, Section 1, NISPOM. These briefings should include pertinent portions of the **(insert Installation Security Program Instruction).** Briefings may be tailored to address those specific responsibilities associated with their assigned duties, the provisions of this agreement, pertinent AF security requirements, any associated DD Forms 254, and any security discrepancies identified in the last security review. Records of these briefings will be maintained at the visitor group's on-base visitor operating location.

(2) Conduct employee security briefings and debriefings, as required by Chapter 3, NISPOM and pertinent Air Force requirements. SF 312s for visitor group personnel will be maintained on file at its HOF or on-base location, if appropriate. Certification of SF 312 accomplishment will be included in the visit request.

(3) The visitor group will ensure participation of all appropriate on-base personnel in any security orientation/education sessions conducted by AF activity to convey security classification guidance.

h. **Personnel Security Clearances (PCLs).** The visitor group's employing facility will submit visit requests annually for on-base employees to the SSA or the AF activity in accordance with **(insert Installation Security Program Instruction)** or Chapter 6, Section 1, NISPOM. The visit request will confirm employee accomplishment of the SF 312. A copy of the visit request will be retained at the visitor group on-base operating location. The contracting AF activity will serve as sponsor for the visit.

i. **Reports.** The visitor group must immediately submit **(in writing)** to the SSA any reports required under any of the situations outlined in Chapter 1, Section 3, NISPOM or Installation Security Program Instruction.

(1) SSA will conduct investigations, as required, in coordination with the AF activity, contracting office, and/or Defense Investigative Service (DIS).

(2) The visitor group or it's HOF will advise the SSA of any changes in management, location, or contractual performance requirements at **(insert name installation location).**

j. **Contractor Controlled/Restricted Area Badges**. AF Form 1199 Series (Green, Pink, Yellow or Blue), **USAF Restricted Area Badge, (insert badge area designation),** will be used by visitor group personnel for entry into USAF Controlled/Restricted Area on **(insert name of installation).** Such entry credentials will be issued at the request of the AF activity. The individual's copy of the AF Form 2586, **Unescorted Entry Authorization Certificate,** will be maintained by the AF activity. All such requests must be supported by a current visit request.

k. **Security Checks.** The visitor group will perform security checks within their assigned on-base work areas to ensure that classified information is properly being protected. Designated visitor group individuals will periodically conduct a security check during normal working hours and at the close of each working day to ensure that:

(1) All classified material has been stored properly

(a) Wastebaskets, routing baskets, typewriters, desks, desk surface litter, and any other work surfaces are void of classified material.

(b) Bags/boxes used to segregate classified waste are stored properly.

(2) All classified containers have been properly secured by an individual to whom the container is assigned, checked by another individual. The person securing the container may also accomplish the check if no one else is available. Record both actions on Standard Form (SF) 702, **Security Container Check Sheet,** or equivalent visitor group form.

(3) Checks of the areas and the security containers will be recorded on Standard Form (SF) 701, **Activity Security Checklist**, or equivalent visitor group form. The visitor group will retain records required by (2) and (3) above until superseding records are initiated.

l. **Emergency Protection.** The visitor group will make every effort to secure all classified material in a GSA-approved storage container in the event of a natural disaster, major accident, or civil disturbance. Visitor group personnel will maintain constant surveillance of insecure classified storage containers, if possible. If the area is evacuated the contractor will, upon termination of the emergency condition,

examine classified holding to ensure there has been no compromise or loss. In the event of missing material or possible compromise, the visitor group will immediately notify the AF activity and SSA.

m. **Protection of Government Resources.** The visitor group will comply with physical security directives of the Air Force.

n. **Clarification of Security Requirements.** To receive clarification or interpretation on security requirements, issues, and/or procedures, the visitor group will:

(1) Submit requests for clarification of DD Form 254 to the SSA through the AF contracting office.

(2) Submit requests for clarification of NISPOM security requirements to the DIS Cognizant Security Office (CSO), through the SSA.

(3) Submit requests for clarification of Installation Security Program Instruction requirements to the SSA.

(4) Submit requests for clarification on the terms of this agreement to the AF contracting office.

o. **Contract and Associated DD Form 254.** The visitor group will maintain on file, at their primary on-base operation location, a copy of the contract, associated DD Form 254, and this agreement.

p. **Foreign Involvement.** Under the terms of this agreement, the visitor group is required to notify the AF activity and contracting office, prior to any foreign involvement, regardless of access requirements or the sensitivity of information to be disclosed (classified or unclassified).

2. **Security Reviews:**

a. The SSA will conduct security reviews of the on-base visitor's operation at intervals determined by the installation commander, to ensure compliance with applicable provisions of the installation security program, NISPOM, and this agreement. Under rare circumstances and with installation commander approval, security reviews may be conducted without prior notification. A written report of the results of any security review will be provided to the visitor group and the AF activity. The visitor group will be required to acknowledge receipt of all review reports and to respond to major security program deficiencies.

b. Visitor group representatives will conduct a self-inspection of their on-base operation at least (insert frequency) using applicable elements of the Installation Security Program, NISPOM, AF activity's OIs, and this agreement. A record of these self-inspections will be maintained on file at their primary on-base operating location.

3. **Other.** Nothing in this agreement shall be construed to impose any liability on the part of the US government for injury to the agents, employees of the contractor, its subcontractors, assignees, or other individuals acting for or on behalf of the contractor, to the property of the same, nor shall anything in this agreement be construed to modify the provisions of existing contracts.

_____ _____

Installation Commander or Designee Visitor Group - Executive Manager

Date: _____ Date: _____

_____ _____

Program Manager (Government) Contracting Officer or Designee

Date: _____ Date: _____

Figure 9.6. Sample Visitor Group Security Agreement (DoD 5220.22-M, NISPOM, Specific). VISI-

TOR GROUP SECURITY AGREEMENT

1. **Contractual Agreement:** This agreement between the Installation Commander, **(insert name of installation)** and **(insert company's commercial name), (insert CAGE number),** is to be performed at (insert name of installation) under the provisions of DoD 5220-22-R, *Industrial Security Regulation,* Section I, Part 1. **(insert company's commercial name),** hereafter referred to as a "visitor group," will be performing on a classified contract, DD Form 254, **DoD Classified Contract Security Specification, (insert contract number)** at (insert physical on-base operation location). This Visitor Group Security Agreement (VGSA) prescribes specific actions to be taken by the visitor group and the **(insert identification of AF organization and installation location),** (hereafter referred to as program manager), to properly protect classified defense information involved in this on-base contract. Under the terms of this agreement, **(insert identification of designated servicing security activity (SSA)** is responsible for providing security program oversight, control, and supervision. ***NOTE:*** As used in the agreement, the terminology visitor group, contractor, company, and home office facility (HOF) are synonymous.

a. All parties, i.e.; the commanders concerned, program manager, contracting officer, staff agencies, Air Force sponsor, visitor group, and their subcontractor (if applicable), and the SSA will comply with the provisions of this agreement without exception or deviation.

b. **Contractor Security Supervision:** The visitor group's home office facility (HOF) will provide the SSA with formal written notice the names of persons (primary and alternate) at their HOF and on-base operations that are responsible for visitor group management and security administration of their operations. The designated on-base visitor group security representative shall complete the Department of Defense (DoD) Industrial Security Management Course, offered by the DoD Security Institute (DODSI), within one year of assumption of security responsibilities.

c. **Standard Practice Procedures (SPP):** This agreement deletes need for the visitor group to publish an addendum/annex or supplement to the HOF SPP for this on-base company activity.

d. **Access and Accountability of Classified Information:**

(1) All on-base access to and/or possession of classified material and hardware in the custody of the visitor group at **(insert name of installation),** will be under the control of the visitor group.

(2) If the visitor group finds unattended or insecure classified material or hardware on-base, they will secure the material, immediately notify the visitor group security representative, program manager or the Law Enforcement Desk at extension **(insert telephone numbers)** and/or report to **(insert physical location Law Enforcement Desk/Operations).** Material(s) will be turned over to security police for safeguarding if the designated primary or alternate classified safe custodian cannot be contacted. The SSA will be notified no later than the close of business or the next duty day with a follow-on formal Administrative Inquiry report no later than fifteen (15) days from date of the security incident; i.e., per DoD 5220,22-M, National Industrial Security Program Operating Manual (NISPOM), Chapter 1 Section 3.

(3) The visitor group shall establish an information management system to control the classified information in their possession (IAW) NISPOM, Chapter 5, Section 2. The disposition and retention of classified material will be in accordance with NISPOM, Chapter 5, Section 7.

(4) Dual access to the visitor group's GSA approved classified security containers or containers combinations is prohibited. In addition, the visitor group is prohibited from using security containers that require lock bar type devices. The visitor group cannot have access to government classified storage containers, nor can the government have sponsor access to the visitor group's containers. However, if an emergency type situation dictates, the contracting officer, in coordination with the program management and SSA may approve temporary dual access and/or storage.

e. **Storage of Classified Material:**

(1) The visitor group is authorized to store classified material and/or hardware necessary for contract performance. GSA approved containers, per DoD 5220.22-M, Chapter 5, Section 3, will be furnished by the government; providing the contract calls for Government Furnished Equipment (GFE).

(2) Under the terms of this agreement, government furnished security containers will be under the control of the visitor group. The responsibility for setting the storage container combination(s) rests with the contractor. The visitor group will not use a government or private locksmith to set the combination. SF Form 700, **Security Container Information,** or the equivalent visitor group form, will be used to identify authorized persons having knowledge of the combination(s), to include their telephone number. This form will be posted inside the locking drawer of each security container. Classified safe combination number(s) will be on the "2A" portion of the SF Form 700. ***NOTE:*** If the combination is recorded, it must be secured in another GSA-approved safe.

f. **Transmission of Classified Material:** Classified material must be transmitted through official AF channels (BITS) using the following address **(insert government mailing address).** Classified information transmitted off the installation must also go through official AF mail channels using the above address as the sending addressee. Consent is granted by the program manager as stipulated by signature of this agreement.

g. **Disposition of Classified Material:** The visitor group will return to the program manager or designated government classified custodian all classified material furnished by the government; to include, surrendering all classified material developed by the visitor group in connection with the contract program or project when the classified material is no longer required, unless retention is granted by the contracting officer.

h. **Reproduction of Classified Material:** The visitor group is not authorized to reproduce classified material without the consent and/or approval of the program manager.

i. **Security Education and Awareness Training:** The visitor group will:

(1) On a recurring basis, but not less than annually (calendar year), brief all on-site cleared visitor group personnel on their responsibilities for safeguarding classified information per DoD 5220.22-M, Chapter 3, Section 1. These briefings need not include all provisions of the NISPOM, but should be tailored to operational classified and unclassified duties. Awareness training should include, contents of this agreement, applicable Department of Defense (DoD) form(s) and security discrepancies noted during the most recent reviews conducted by the SSA and reporting requirements per DoD 5220.22-M, Chapter 1, section 3.

(2) Conduct initial and refresher briefings and debriefings per DoD 5220.22-M, Chapter 3, Section 1. Certification of accomplishment of the Standard Form 312, **Classified Nondisclosure Agreement** (NDA) will be included in the classified Visit Authorization Letter (VAL).

(3) Insure participation of all on-site contractor personnel in security awareness orientation/education sessions conducted or scheduled by the visitor group security representative.

j. **Personnel Security Clearance (PCL):** The visitor group's HOF will submit VALs (classified and unclassified) annually (1 Jan 9X - 31 Dec 9X) to the AF activity's security manager for their on-base personnel per DoD 5220.22-M, Chapter 6, Section 1. In addition, a copy of the VAL will be provided to the visitor group's on-base security representative. ***NOTE:*** A copy of each VAL will be retained at the contractor's on-site operating location. The contracting AF activity serves as sponsor for the visit. The government must approve "need-to-know" certification for all incoming visit requests.

k. **Reports:** The visitor group must immediately submit, in writing, to the SSA, a preliminary inquiry report required per DoD 5220.22-M, Chapter 1, Section 3. Paragraphs 1-301, 1-302, 1-303 and 1-304. The visitor group must also keep the SSA, Defense Investigative Service Clearance Office (DISCO), the Air Force Office of Special Investigation (AFOSI) and the Federal Bureau of Investigation (FBI) advised on any reports made per DoD 5220.22-M, Chapter 1, Section 3, Paragraphs 1-301 and 1-302.

(1) The SSA and/or AFOSI will conduct investigations within their purview as required and coordinate their investigation with the program manager and/or contractor security representative, as appropriate.

(2) The visitor group's HOF will advise the SSA of any changes in ownership or management, classified P.O. Box mail drop location at **(insert name of installation).**

l. **USAF Controlled Area and Company Badge:** Per **(insert name of installation),** Supplement 1, AFI 31-209, *Resource Protection Program*, the visitor group employees will used the AF Form 1199**, USAF Restricted Area Badge,** to gain unescorted entry into USAF Controlled Area(s) on **(insert name of installation).** Restricted or controlled area badges will be issued only upon the request of the program manager or designated representative. A copy of the AF Form 2586, **Unescorted Entry Authorization Certificate,** will be filed and maintained by the requesting AF activity. Request for badge issuance must be supported by a valid VAL. Visitor group employees must wear, or have in their immediate possession, a company photo badge and/or wallet size identification that reflects the complete company name of the visitor's group, employee's name and photograph, and **(insert name of the installation)** prominently reflected on the face of the identification credential and any additional data deemed appropriate by the visitor group management.

m. **End-of-Day Security Checks:** At the close of each working day, the visitor group will perform physical security checks within their assigned on-base work and/or operating locations per DoD 5220.22-M, Chapter 5, Section 1. The supervisor of the visitor group will designate, in writing, individuals to perform the end-of-day security checks to ensure:

(1) All classified material has been properly stored.

(2) Wastebaskets, routing baskets, typewriters, desk surface litter, classified computer systems, and any other work surfaces are void of classified material; i.e., "clean desk policy".

(3) Bag or boxes used to segregate classified waste are properly safeguarded in an approved container or classified waste bin.

(4) All classified containers have been properly secured by the designated company employee, checked by another individual, and both checks are recorded on SF 702, **Security Container Check Sheet,** or equivalent contractor form.

(5) Checks of the area and the security container will be recorded on SF Form 701, **Activity Security Checklist,** or equivalent contractor form.

n. **Emergency Protection:** In the event of a natural disaster, major accident, or civil disturbance, the visitor group will make every effort to secure all classified material in a GSA-approved container. If unable to properly secure classified information, the visitor group will maintain constant surveillance of the affected area, if possible. If the work area is evacuated, upon termination of the emergency condition, the visitor group will inventory exposed classified holdings to verify no compromise or loss has occurred. In the event of such an occurrence, the discovering visitor group employee will immediately notify their on-base security representative, the program manager and the SSA.

o. **Protection of Government Resources:** Visitor group will comply with applicable AF activity's physical security and resource protection requirements, directives, and/or procedures.

p. **Clarification of Security Requirements:** Visitor group submit a request for clarification on security requirements as follows:

(1) For clarification of DoD host installation or activity procedures or applicable DD Form 254 programs requirements; submit to the program manager or designee, who, in turn, coordinates with the governing contracting office and SSA.

(2) Visitor Group's request for exceptions, deviations and/or waiver of security requirements of DoD 5220.22-M, NISPOM and this agreement will be submitted in writing to the SSA.

q. **Contract and associated DD Form 254:** The visitor group will maintain on file a copy of the contract, Statement of Work (SOW), Performance Work Statement (PWS), Contract Data Requirements List (CDRL), associated DD Forms 254, and/or revisions, to include any related correspondence .

2. **Reviews:**

a. The SSA will conduct security reviews of the on-base visitor group's operation at (specify) intervals to ensure compliance with applicable provisions of DoD 5220.22-M, AF directives, instructions, and this agreement. Written results of the security review will be provided to the visitor group and program manager. The visitor group is not required to acknowledge receipt or respond unless so directed in the report e.g.; Letter of Requirements (LOR) for serious review discrepancies.

b. The visitor group shall conduct formal self-inspections at intervals consistent with risk management principals. A written record of these self-inspections will be maintained on file (until next self-inspection is completed) at the on-base facility, and is subject to SSA review.

3. **Expenditures of Funds for Security:** This agreement is not an authorization for payment of funds for associated security expenditures. Nothing in this agreement shall be construed to impose any liability on the part of the U.S. Government for injury to the agents, employees of the contractor, its subcontractors, (if applicable) assignees, or other individuals acting for or on behalf of the contractor, to the property of the same, nor shall anything in this agreement be construed to modify the provisions of existing contract(s).

4. **Review of this Agreement:** All parties must review this agreement at least annually, upon program changes, concept of operations, etc. The program manager or designee is responsible for the review and

keeps a record of the last review. If changes are necessary, report them in writing, to the contracting officer.

5. **Visitor Register:** The visitor group shall maintain a record of all classified and unclassified visits to their on-base operating facilities. The register will reflect as a minimum: 1) the visitor's last name, first name, and middle initial; 2) the name of the company or agency he/she represents; 3) the visitor record need not indicate whether the visitor actually did or did not have access to classified information, but it must distinguish between a "classified" and "unclassified" visit; 4) the date(s) of his/her arrival and departure from the facility. Records of all such visits shall be maintained in accordance with AFMAN 37-139.

6. **Other:** The program manager or designee (normally the contracting officer) will furnish all government forms to the visitor group required under the terms of this agreement.

7. **Communication Security (COMSEC):** The visitor group will use secure communications (STU III) when discussing sensitive-unclassified information pertaining to this contract, when made available under the terms of this contract by the AF activity.

8. **Computer Security (COMPUSEC):** Automated information systems (AISs) i.e., computers, word processors, networks and stand-alones, etc., used in the processing of classified information in support of this contract must be certified and operated per DoD 5220.22-M, Chapter 8, Sections 1 thru 4 or AFI 31-2XX series and supplements thereto. Submit AISs certification and/or approval requests to the **(insert identification of Base Communication/Information Activity),** Designated Approval Authority (DAA), prior to commencement of classified operations. AIS's processing unclassified-sensitive information in support of this contract must likewise receive certification and/or approved prior to operation. Address Emission Security (EMSEC) concerns to the **(insert the identification of Base Communication/Information Activity).**

9. **Operations Security (OPSEC):** The visitor group will protect critical or sensitive-unclassified operational information per AFI 10-1101, *Operations Security (OPSEC),* and AF activity guidance and/or direction.

10. **Foreign Involvement:** Under the terms of this agreement, the visitor group is required to notify the AF activity and contracting office, prior to any foreign involvement, regardless of access requirements or sensitivity of information to be disclosed (classified or unclassified).

11. **Key AF Point of Contacts (POCs):** (Insert names, organizational address, and telephone numbers of program manager, contracting officer, SSA and other key base contracting or security representatives, as deemed appropriate).

12. **Other:** Nothing in this agreement shall be construed to impose any liability on the part of the US government for injury to the agents, employees of the contractor, its subcontractors, assignees, or other individuals acting for or on behalf of the contractor, to the property of the same, nor shall anything in this agreement be construed to modify the provisions of existing contracts.

_____ _____

Installation Commander or Designee Visitor Group - Executive Manager

Date: _____ Date: _____

_____ _____

Program Manager (Government) Contracting Officer or Designee

Date: _____ Date: _____

RICHARD A. COLEMAN, Brig Gen, USAF
Chief of Security Police

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

DoD 5200.1-R, *Information Security Program Regulation*

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 Program Regulation*

AFPD 10-11, *Operations Security*

AFPD 31-4, *Information Security*

AFPD 31-5, *Personnel Security Program Policy*

AFPD 31-6, *Industrial Security*

AFPD 33-2, *Information Protection*

AFI 10-1110, *Operations Security Instruction*

AFI 14-302, *Control, Protection, and Dissemination of Sensitive Compartmented Information (SCI*

AFI 14-303, *Release of Collateral Intelligence to US Contractors*

AFI 31-209, *Air Force Resource Protection Program*

AFI 31-401, *Managing The Information Security Program*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI 33-201, *The Communications Security (COMSEC) Program*

AFI 33-202, *The Computer Security (COMPUSEC) Program*

AFI 33-203, *The Air Force Emission Security Program*

AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type I*

AFI 35-205, *Air Force Security and Policy Review Program*

AFI 37-124, *The Information Collections and Reports Management Program*

AFI 37-160V7, *Publication Libraries and Sets*

AFH 31-502, *Personnel Security Program*

AFMAN 37-139, *Disposition of Air Force Records - Records Disposition Schedule*

DCID 1/19, *DCI Security Policy for SCI*

Abbreviations and Acronyms

ACO - Administrative Contracting Officer—

AF - Air Force—

AFFARS- -Air Force Federal Acquisition Regulation Supplement—

AFCSC - Air Force Cryptological Support Center—

AFH - Air Force Handbook—

AFI - Air Force Instruction—

AFOSI - Air Force Office of Special Investigations—

AFPD - Air Force Policy Directive—

AFVA - Air Force Visual Aid—

AIS - Automated Information System—

AKA - Also Known As—

ASCAS - Automated Security Clearance Approval System—

ASD(C3I) - Assistant Secretary of Defense (Command, Control,—

Communication & Intelligence—

BITS - Base Information Transfer System—

C4 - Command, Control, Communications, and Computers—

CAF - Central Adjudication Facility—

CCI - Controlled Cryptographic Item—

CDRL - Contract Data Requirement List—

CIA - Central Intelligence Agency—

CM - Contract Monitor—

CNWDI - Critical Nuclear Weapon Design Information—

COMPUSEC - Computer Security—

COMSEC - Communications Security—

COS - Corrected on the Spot—

CSA - Cognizant Security Agency—

CSO - Cognizant Security Office—

CSSO - Computer System Security Officer—

CVA - Central Verification Activity—

DAA - Designated Approving Authority—

DAF - Department of Air Force—

DAFC - Department of the Air Force Civilian—

DCID - Director of Central Intelligence Directive—

DCS - Defense Courier Service—

DDN - Direct Dial Number—

DD/DoD - Department of Defense—

DIA - Defense Intelligence Agency—

DIS - Defense Investigative Service—

DISCO - Defense Industrial Security Clearance Office—

DODSI - Department of Defense Security Institute—

DOE - Department of Energy—

DRU - Direct Reporting Unit—

DTIC - Defense Technical Information Center—

EMSEC - Emission Security (formerly TEMPEST)—

EXORD - Executive Order—

FAR - Federal Acquisition Regulation—

FBI - Federal Bureau of Investigations—

FCL - Facility Security Clearance—

FOA - Field Operating Agency—

FOCI - Foreign Owned, Controlled, or Influenced—

FOIA - Freedom of Information Act—

FOUO - For Official Use Only—

FSCN - Federal Supply Code Number—

FSO - Facility Security Officer—

GFE - Government Furnished Equipment—

GSA - General Services Administration—

HOF - Home Office Facility—

HQ - Headquarters—

IAW - In Accordance With—

ISFO - Industrial Security Field Office—

ISOO - Information Security Oversight Office—

ISR - Industrial Security Regulation—

LAA - Limited Access Authorization—

LIMDIS - Limited Distribution—

LOR - Letter of Requirement—

MAJCOM - Major Command—

MFO - Multiple Facility Organization—

MOA - Memorandum of Agreement—

MOU - Memorandum of Understanding—

NATO - North Atlantic Treaty Organization—

NDA - Classified Nondisclosure Agreement—

NID - National Interest Determination—

NISP - National Industrial Security Program—

NISPOM - National Industrial Security Program Operating—

Instruction—

NISPOMSUP - National Industrial Security Program Operating—

Instruction Supplement—

NO DEF - No Deficiencies—

NRC - Nuclear Regulatory Commission—

NSA - National Security Agency—

NSC - National Security Council—

NTK - Need-to-Know—

OI - Operating Instruction—

OODEP - Owners, Officers, Directors, Partners, Regents,—

Trustees, or Executive Personnel—

OPR - Office of Primary Responsibility—

OPSEC - Operations Security—

ORCON - Dissemination and Extraction of Information—

Controlled by Originator—

OSM - Office Security Manager—

PCL - Personnel Security Clearance—

PCO - Procuring Contracting Officer—

PCS - Permanent Change of Station—

PIC - Personnel Investigative Center—

PIC-CVA - Personnel Investigative Center - Central Verification—

Activity—

PM - Program Manager—

PMF - Principal Management Facility—

POC - Point of Contact—

PR - Purchase Request—

PWS - Performance Work Statement—

RD - Critical Restricted Data—

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—

SCIF - Sensitive Compartmentalized Information Facility—

SECDEF - Secretary of Defense—

SF - Standard Form—

SM - System Manager—

SOO - Statement of Objectives—

SOW - Statement of Work—

SPA - Security Police Administrations—

SPO - System Program Office—

SPP - Standard Practice Procedures—

SSA - Servicing Security Activity—

SSO - Special Security Officer—

TA - Trading As—

TDY - Temporary Duty—

TMO - Transportation Management Office—

USM - Unit Security Manager—

VAL - Visit Authorization Letter—

VGSA - Visitor Group Security Agreement—

Terms

Carve-out Contract.— A carve-out is a classified contract awarded by the Air Force in connection with a SAP in which the DIS has been relieved of security and/or oversight responsibility in whole or in part. The Air Force SAP manager for a carve-out contract designates an Air Force activity to perform these functions.

Cleared Facility.— See definition of cleared facility, this

publication, paragraph 3.1.1.

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 Investigative Service (DIS) to perform this function. The Director of DIS, has further delegated this responsibility downward within the agency. DIS Regional Directors provide industrial security administration for DoD contractor facilities located within their respective geographical area. The exception being, installation DoD contractors designated as "Visitor Group" for

which the SSA have these responsibilities. When used, the

language "Cognizant Security Office" (CSO), always refers to DIS or an entity thereof.

Installation.— A group of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base.

Interim Facility Security Clearances (Interim FCL).— Interim FCL are temporary, limited company security clearances established by the DIS CSO. 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 PCL 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 Visitors.— Contractor employees visiting an Air

Force installation for brief periods of time on a scheduled or on call basis to perform contractual duties that require access to classified information. An intermittent visitor's presence on an installation usually does not exceed 90 consecutive days.

Invalidation. — A temporary 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.

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.

Servicing Security Activity.— This activity implements and oversees the industrial security program for an installation and designated on-base contractors. The installation commander designates the servicing security activity.

Visitor Groups.— See definition of visitor group, this publication, paragraph 3.2.1.

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 rendering or performing specific security services for compensation. The VGSA attest to and certifies the existence of such an agreement, including applicable changes and amendments, attachments, supplements and exhibits.