BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-701

8 JUNE 2011

59TH MEDICAL WING Supplement

21 AUGUST 2012
Certified Current on 24 September 2014
Operations

OPERATIONS SECURITY (OPSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A3Z-CI, Information Operations Division

Certified by: AF/A3Z (Maj Gen Bolton)

Pages: 42

Supersedes: AFI 10-701, 18 October 2007

(59MDW)

OPR: 59 MDW/SGSKX

Certified by: 59 MDSG/CC (Colonel Heather M. Carter)

Pages:3

This publication implements Air Force Policy Directive (AFPD) 10-7, *Air Force Information Operations*. The reporting requirements in this publication have been assigned Report Control Symbol (RCS) DD-INTEL(A)2228 in accordance with DoDD 5205.02, DoD Operations Security (OPSEC) Program. It applies to all Major Commands (MAJCOM), Field Operating Agencies (FOA), Direct Reporting Units (DRU), Air Force Reserve Command and Air National Guard (ANG) organizations. This publication provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through appropriate chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**. The use of the name or mark of any

specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

(59MDW) AFI 10-701, *Operations Security (OPSEC)*, 8 June 2011, is supplemented as follows. This supplement provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing OPSEC programs for the 59th Medical Wing (MDW). This instruction does not apply to the Air National Guard or Air Force Reserve. Refer recommended changes and questions about this publication to the Office of Primary Responsibility using the AF Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System Records Disposition Schedule located at **https://www.my.af.mil/afrims/afrims/afrims/rims.cfm**.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. This updated instruction adds responsibilities for MAJCOMs, FOAs and DRUs (paragraph 1.4.8), Air Combat Command (ACC) (paragraph 1.4.8), commanders (paragraph 1.4.15), requirement to budget, acquire and distribute OPSEC awareness and education materials (1.4.15.8.2), OPSEC Program Managers (PM), Signature Management Officers, Coordinators and Planners (paragraph 1.4.16) and all Air Force personnel (paragraph 1.4.17). Chapter 2 has been renamed Signature Management and OPSEC Process has been moved to Chapter 4. OPSEC measures have been deleted from chapter 4 and are now reflected to read countermeasures (paragraph 4.6). Acquisition planning has been removed from chapter 3, OPSEC Planning and placed within chapter 8, OPSEC Contract Requirements. OPSEC Awareness Education and Training has been moved to chapter 5, OPSEC Education and Training, and includes requirement to provide awareness information to AF family members. OPSEC assessments has been moved to chapter 6 and titled Assessments. Additions to chapter 6 include web site link to the OPSEC Core Capabilities Checklists (paragraph 6.1.5), requirements regarding the assessment of information on AF public and private web sites (paragraph 6.5), and requirement to utilize the operations security collaborations architecture (OSCAR) tool for annual assessments (paragraph 6.6.4). Air Force OPSEC annual awards is located in chapter 7 and chapter 8 includes information regarding OPSEC as a requirement within government contracts.

Chapter 1—GENERAL **5**

1.1. Introduction: 5

1.2. Operational Context: 5

Figure 1.1. OPSEC Functional Structure 5

1.3. Purpose: 6

1.4. Roles and Responsibilities: 6

Chapter 2—SIGNATURE MANAGEMENT **17**

2.1. Signature Management. 17

2.2. Wing or installation commanders will: 17
2.3. Signature Management Officer/Signature Management Non-Commissioned Officer will: 18
2.4. Signature Management Planning and Coordination. 20
2.5. Exploitation Countermeasures (Refer to AFI 10-704, Paragraph 2. 20

Chapter 3—OPSEC PLANNING 21

3.1. General. 21
3.2. Operational Planning. 21
3.3. Support Planning. 21
3.4. Exercise Planning. 21
3.5. Acquisition Planning. 22

Chapter 4—OPSEC PROCESS 23

4.1. General: 23
4.2. Identify Critical Information: 23
4.3. Analyze Threats: 23
4.4. Analyze Vulnerabilities: 23
4.5. Assess Risk: 24
4.6. Apply Countermeasures: 24

Chapter 5—OPSEC EDUCATION AND TRAINING 25

5.1. General. 25
5.2. All Personnel: 25
5.3. OPSEC PMs/SMO/SMNCOs/Coordinators, Planners, Inspection Teams: 26
5.4. Joint and Interagency OSPEC Support: 27

Chapter 6—ASSESSMENTS 28

6.1. General: 28
6.2. Annual OPSEC Program Review: 28
6.3. Staff Assistance Visit (SAV): 29
6.4. Survey: 29
6.5. Web Content Vulnerability Analysis: 30
6.6. Support Capabilities: 30
Table 6.1. OPSEC Assessment Types and Support Capabilities 31

Chapter 7—AIR FORCE OPSEC ANNUAL AWARDS PROGRAM 33

7.1. General: 33

Chapter 8—OPSEC REQUIREMENTS WITHIN CONTRACTS 34

8.1. General: 34

8.2. Guidance and procedures: 34

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 36

Chapter 1

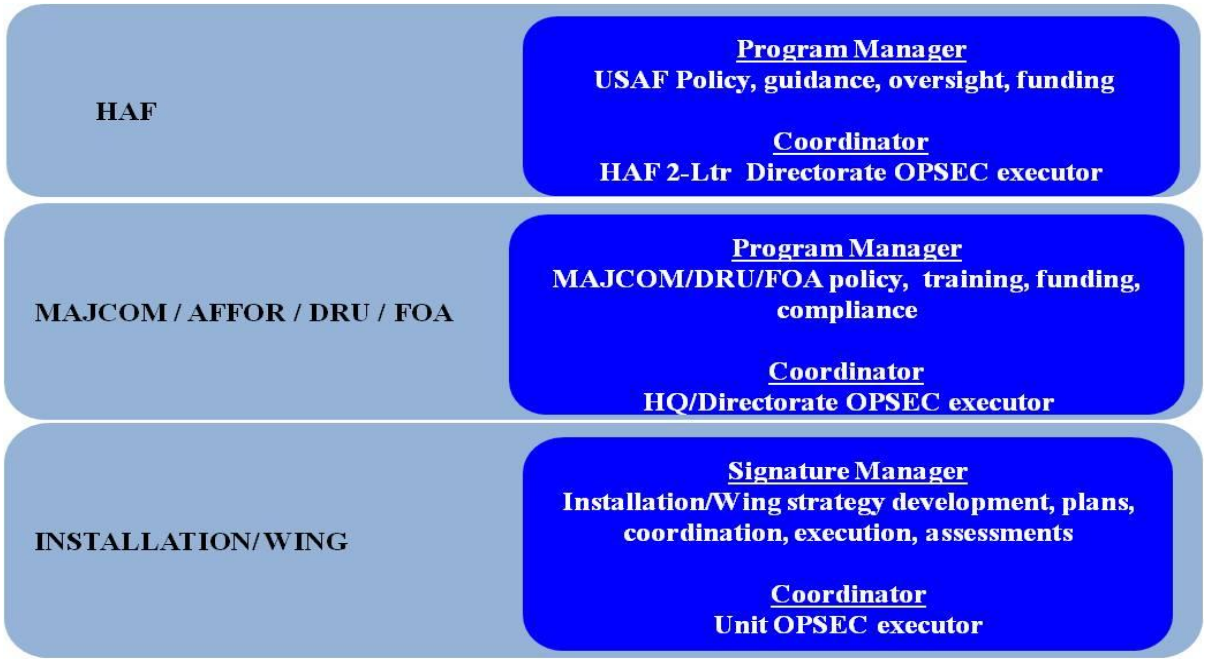
GENERAL

1.1. Introduction: OPSEC is a military capability within Information Operations (IO). IO is the integrated employment of three operational elements: influence operations (IFO), electronic warfare operations and network warfare operations. IO aims to influence, disrupt, corrupt, or usurp adversarial human or automated decision-making while protecting our own. IFO employs the military capabilities of military information support operations (MISO), OPSEC, military deception (MILDEC), counterintelligence operations, public affairs (PA) operations and counterpropaganda operations to affect behaviors, protect operations, communicate commanders' intent and project accurate information to achieve desired effects across the operational environment. OPSEC's desired effect is to influence the adversary's behavior and actions by protecting friendly operations and activities.

1.2. Operational Context:

1.2.1. Operational Focus. The OPSEC program is an operations function or activity and its goals are information superiority and optimal mission effectiveness. The emphasis is on OPERATIONS and the assurance of effective mission accomplishment. To ensure effective implementation across organizational and functional lines the organization's OPSEC Program Manager (PM), Signature Management Officer (SMO), or coordinator will reside in the operations and/or plans element of an organization or report directly to the commander. For those organizations with no traditional operations or plans element, the commander must decide the most logical area to place management and coordination of the organization's OPSEC program while focusing on operations and the mission of the organization. Figure 1.2 illustrates the AF OPSEC functional structure.

Figure 1.1. OPSEC Functional Structure



1.2.2. Operational effectiveness is enhanced when commanders and other decision-makers apply OPSEC from the earliest stages of planning. OPSEC involves a series of analyses to examine the planning, preparation, execution and post execution phases of any operation or activity across the entire spectrum of military action and in any operational environment. OPSEC analysis provides decision-makers with a means of weighing how much risk they are willing to accept in particular operational circumstances in the same way as operations risk management allows commanders to assess risk in mission planning.

1.2.3. OPSEC must be closely integrated and synchronized with other IFO capabilities, security disciplines, and all aspects of protected operations (see references listed in Attachment 1).

1.3. Purpose:

1.3.1. The purpose of OPSEC is to reduce the vulnerability of Air Force missions by eliminating or reducing successful adversary collection and exploitation of critical information. OPSEC applies to all activities that prepare, sustain, or employ forces during all phases of operations.

1.3.2. OPSEC Definition. OPSEC is a process of identifying, analyzing and controlling critical information indicating friendly actions associated with military operations and other activities to:

1.3.2.1. Identify those actions that can be observed by adversary intelligence systems.

1.3.2.2. Determine what specific indications could be collected, analyzed, and interpreted to derive critical information in time to be useful to adversaries.

1.3.2.3. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

1.4. Roles and Responsibilities:

1.4.1. Air Force organizations must develop and integrate OPSEC into their mission planning to ensure critical information and indicators are identified. At a minimum, the Air Force will integrate OPSEC into the following missions: military strategy, operational and tactical planning and execution, military indoctrination, support activities, contingency, combat and peacetime operations and exercises, communications-computer architectures and processing, critical infrastructure protection, weapons systems, Research, Development, Test and Evaluation (RDT&E), Air Force specialized training, inspections, acquisition and procurement, medical operations and professional military education. Although the OPSEC program helps commanders make and implement decisions, the decisions are the commander's responsibility. Commanders must understand the risk to the mission and then determine which countermeasures are required.

1.4.2. **The Deputy Chief of Staff for Operations, Plans and Requirements (AF/A3/5).** The AF/A3/5 is the OPR for implementing DoD OPSEC policy and guidance. This responsibility is assigned to the Director of Cyber and Space Operations (AF/A3Z). AF/A3Z will:

1.4.2.1. Establish an AF OPSEC program focused on senior leadership involvement using the management tools of assessments, surveys, training, education, threat analyses, resourcing, and awareness that, at a minimum, includes:

1.4.2.1.1. Assign a full-time AF OPSEC PM (O-4 or civilian equivalent).

1.4.2.1.2. Establish AF OPSEC support capabilities that provide for program development, planning, training, assessment, surveys, operational support, and readiness training.

1.4.2.1.3. Conduct annual reviews and validations of the AF OPSEC program as prescribed by DoD and AF policy/guidance.

1.4.2.1.4. Ensure OPSEC surveys are conducted for subordinate commands and agencies in order to enhance mission effectiveness and reduce risk.

1.4.2.2. Develop Air Force Departmental publications to define policy, guidance, responsibilities and authorities to establish the internal management processes necessary to carry out DoD policy/guidance. Provide copies of all current service OPSEC program directives and/or policy implementation documents to the Joint Staff J-3.

1.4.2.3. Support OPSEC programs at the national, DoD and Joint-level as necessary.

1.4.2.4. Centrally plan, program, budget and manage training for the Air Force OPSEC program.

1.4.2.5. Provide oversight and advocacy as the focal point for AF OPSEC assessment capabilities.

1.4.2.6. Ensure appropriate levels of standardized OPSEC training and education are established and provided to all AF personnel, to include civil service personnel, and to all contractors who have access to mission critical information.

1.4.2.7. Publish unclassified advisory tips and best practices aimed at educating service members and their families about the official and personal use of social networking sites and potential vulnerabilities exposed by posting military service-related information online.

1.4.2.8. Develop policy and guidance to ensure OPSEC requirements are properly reflected in classified and unclassified contracts.

1.4.2.9. Ensure OPSEC policy development activities are integrated through the Air Force Security Policy and Oversight Board (AFSPOB).

1.4.3. **Secretary of the Air Force Office of Information Dominance and Chief Information Officer (SAF/CIO A6)**

1.4.3.1. Ensures OPSEC principles are included in information assurance policy, guidance, and operational oversight.

1.4.3.2. Ensures OPSEC principles and practices are correctly reflected in the AF Enterprise Architecture.

1.4.3.3. Ensure OPSEC is incorporated into the developing Net-centric operating environments to mitigate the risks of classification through compilation of critical information.

1.4.4. **The Secretary of the Air Force, Office of Public Affairs (SAF/PA)** develops policy and guidance to ensure OPSEC is considered in the public affairs process for releasing information to the public.

1.4.5. **The Assistant Secretary of the Air Force, Acquisition (SAF/AQ)**

1.4.5.1. Develop policy and guidance to ensure OPSEC is considered in AF acquisition and RDT&E for critical information and critical program information (reference DoDI 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*).

1.4.5.2. Ensure Government contract requirements properly reflect OPSEC responsibilities and are included in contracts when applicable.

1.4.6. **The Administrative Assistant to the Secretary of the Air Force (SAF/AA)** provides coordination and integration of OPSEC policy and guidance through the AFSPOB.

1.4.7. **The Secretary of the Air Force, Inspector General (SAF/IG) will**

1.4.7.1. IAW AFPD 90-2, *Inspector General—The Inspection System*, AFI 90-201, *Inspector General Activities*, and this Instruction, assess and report on AF organizational OPSEC programs for compliance, planning, and operational readiness when conducting assessments, inspections, and/or management reviews.

1.4.7.2. Include OPSEC as a critical compliance item for Operational Readiness Inspection (ORI) and Unit Compliance Inspections (UCI) at all levels of command.

1.4.7.3. Provide results of OPSEC assessments, inspections, and/or management reviews to AF/A3Z, Directorate of Cyber and Space Operations.

1.4.7.4. Ensure inspection team members conducting assessments, inspections, and or management reviews on organizational OPSEC programs complete the required OPSEC training listed in Paragraph 5.3.2.

1.4.7.5. Through Air Force Office of Special Investigations (AFOSI), provide OPSEC PMs/SMOs/Coordinators and commanders with AFOSI threat information at CONUS, OCONUS and deployed locations.

1.4.7.6. Provide HUMINT (Human Intelligence) Vulnerability Assessment support when possible for OPSEC vulnerability assessments.

1.4.8. **Air Force MAJCOMs, FOAs, and DRUs will:**

1.4.8.1. Implement AF OPSEC guidance to incorporate and institutionalize OPSEC concepts into relevant doctrine, policies, strategies, programs, budgets, training, exercising, and evaluation methods. At the base/installation level, FOAs and DRUs will comply with host MAJCOM and wing guidance.

1.4.8.2. Develop effective OPSEC programs IAW guidance issued by AF/A3Z.

1.4.8.3. Designate an organization as the OPR for OPSEC and appoint a full-time OPSEC PM position (O-3/4 or civilian equivalent). This position should be placed within the operations or plans element (unless MAJCOM mission and/or structure requires otherwise) and serve as the POC for all OPSEC related issues between headquarters Air Force and the command. DRUs and FOAs may request an exemption to

appointing a full-time OPSEC PM position by submitting a waiver signed by the commander to the AF OPSEC PM with justification for the request.

1.4.8.4. Ensure OPSEC PMs have at a minimum a secret clearance (recommend Top Secret) and accounts established on the SECRET Internet Protocol Router Network (SIPRNET) and the Unclassified but Sensitive Internet Protocol (IP) Router Network (NIPRNET).

1.4.8.5. Enforce policy and issue guidance implementing supplements or other guidance as required.

1.4.8.6. Consolidate OPSEC requirements and submit them according to the AF capabilities based planning process (reference AFI 10-601, *Capabilities-Based Requirements Development*).

1.4.8.7. Ensure subordinate organizations consistently apply and integrate OPSEC into day-to-day operations and/or other IO activities throughout the command.

1.4.8.8. Ensure all subordinate organizations are identifying critical information for each operation, activity and exercise whether it be planned, conducted or supported.

1.4.8.9. Ensure all subordinate organizations are controlling critical information and indicators.

1.4.8.10. Ensure all subordinate organizations plan, exercise and implement countermeasures as appropriate.

1.4.8.11. Program funds for OPSEC through established budgeting and requirements processes.

1.4.8.12. Ensure OPSEC considerations are applied in capabilities development and the acquisition process.

1.4.8.13. Ensure training of OPSEC PMs and planners is accomplished as soon as possible upon being appointed.

1.4.8.14. Whenever practical all OPSEC PM, SMO and OPSEC planner positions (billets) are assigned the OPSEC special experience identifier (SEI) 9O or 234. All individuals performing OPSEC duties will be awarded SEI 9O or 234 when all requirements are met and approval granted by the commander and/or appropriate AFPC assignment managers. SEIs will drive future training allocations upon receipt of orders or upon assignment to organizations with SEI coded positions.

1.4.8.15. Develop and cultivate the intelligence and counterintelligence relationships necessary to support OPSEC programs.

1.4.8.16. Serve as the focal point for MAJCOM-level OPSEC assessments, surveys and support capabilities.

1.4.8.17. Ensure OPSEC considerations are included in annual reviews of AF unclassified public and private web sites and pages (including all AF public and private web sites hosted outside base firewalls) and in the approval process for posting new data to AF public and private web sites.

1.4.8.18. Ensure assistance is provided to PA as needed to ensure OPSEC considerations are included in PA review and approval processes for publishing/releasing information to the public.

1.4.8.19. Forward MAJCOM annual program review report executive summary to include all reports from one level down for the fiscal year period of 1 Oct – 30 Sep to the AF OPSEC PM (AF/A3Z-CI) NLT 15 November each year (See Paragraph 6.2).

1.4.8.20. Ensure OPSEC related briefings or presentations to be given outside the MAJCOM are coordinated through the Air Force OPSEC PM, AF/A3Z-CI, prior to the presentation date.

1.4.8.21. Coordinate with the Air Force Experimentation Office to incorporate Air Force OPSEC initiatives into Joint/Air Force experimentation, traditional and spiral development acquisition activities.

1.4.9. **Air Combat Command (ACC) will:**

1.4.9.1. Assume all duties as lead command for AF OPSEC program.

1.4.9.2. Organize, train, and equip assigned forces to plan and execute OPSEC in a theater of operations for Joint or combined operations in the roles of aerospace control, force application, force enhancement, and force support.

1.4.9.3. Develop, document, and disseminate OPSEC tactics, techniques, and procedures (TTP) for the Combat Air Forces.

1.4.9.4. Integrate OPSEC into the Air and Space Operations Center (AOC) construct.

1.4.9.5. Develop, maintain, program for, and provide Air Force OPSEC initial qualification training.

1.4.10. **Air Mobility Command (AMC) will:**

1.4.10.1. Lead centralized management of OPSEC functions and the establishment and integration of OPSEC in Mobility Air Force operations.

1.4.10.2. Develop Mobility Air Force (MAF) OPSEC TTPs.

1.4.10.3. Integrate OPSEC into the AMC AOC construct.

1.4.10.4. Develop functional area and functional needs analysis for MAF and submit through the AF capabilities based planning process.

1.4.10.5. Centrally program for MAF OPSEC capabilities.

1.4.11. **Air Force Materiel Command (AFMC)** will ensure OPSEC is integrated into all RDT&E efforts. When critical information or critical program information is involved, ensure OPSEC is applied as a protective measure throughout the life cycle of all weapon systems IAW DoDI 5200.39 and AFI 63-101, *Acquisition and Sustainment Life Cycle Management*.

1.4.12. **Air Education and Training Command (AETC) will:**

1.4.12.1. Provide OPSEC orientation for all new Air Force accessions to include what OPSEC is, its purpose, threat awareness, and the individual's role in protecting critical information.

1.4.12.2. Incorporate OPSEC education into all professional military education. At a minimum, this will include the purpose of OPSEC, critical information, indicators, threats, vulnerabilities, and the individual's role in protecting critical information.

1.4.12.3. Incorporate OPSEC concepts and capabilities into specialized courses, such as the Contingency Wartime Planning Course, Joint Air Operations Planning Course, and the Information Operations Fundamental Application Course. These courses will include command responsibilities and responsibilities of OPSEC planners in Joint Forces Command IO Cells and MAJCOMs.

1.4.12.4. Ensure OPSEC is addressed in all technical and specialty school programs.

1.4.12.5. Establish a validation process to ensure AF/A3Z-CI, reviews all AETC OPSEC training materials used in accession and professional military education.

1.4.13. **US Air Force Academy** will provide OPSEC orientation for all new Air Force accessions to include what OPSEC is, its purpose, threat awareness, and the individual's role in protecting critical information.

1.4.14. **Academy of Military Science** will provide OPSEC orientation for all new Air Force accessions to include what OPSEC is, its purpose, threat awareness, and the individual's role in protecting critical information.

1.4.15. **Commanders and Directors will: NOTE: Wing and installation commanders will follow the additional guidance in Chapter 2, *Signature Management.***

1.4.15.1. Issue guidance regarding the establishment of OPSEC measures to all assigned personnel to ensure OPSEC is integrated into day-to-day and contingency operations. Commanders may delegate authority for OPSEC program management, but retain responsibility for risk management decisions and the overall implementation of countermeasures. They must determine the balance between countermeasures and operational needs.

1.4.15.2. Appoint in writing a primary and alternate OPSEC PM, or coordinator and forward to the next higher headquarters (HHQ) OPSEC PM. OPSEC PMs will be assigned for a minimum of two years, or as area tour length dictates (remote tours only). Organizations where an assignment is less than two years will request, in writing a waiver to their HHQ OPSEC PM.

1.4.15.2. **(59MDW)** The 59th Medical Wing's OPSEC program is administered through the 59th Medical Wing's Medical Readiness office [Disaster Preparedness and Plans (DP) section]. The Commander, 59th Medical Support Group will appoint the primary and alternate 59th Medical Wing (MDW) OPSEC PM. The Element Chief, DP, will serve as the primary while an assigned Antiterrorism Officer will serve as alternate. These members will also act as the Signature Management Officer/Noncommissioned Officer (SMO/SMNCO). Members will establish accounts on the National OPSEC Program Interagency OPSEC Support Staff website (IOSS), and complete all relevant training, as prescribed in the parent instruction. Members shall seek the first available course online, meeting time requirements via: **https://www.iad.gov/ioss/department/training-10003.cfm?o8JrsXG140QhW8zYmPdoXQ**.

1.4.15.2.1. Wing or installation primary OPSEC PMs will be an O-3 or above, civilian equivalent, or an E-7. The alternate OPSEC PM will be an E-6 or above, or civilian equivalent. Under no circumstances will contract personnel be appointed as a primary or alternate OPSEC PM. At a minimum, OPSEC PMs will have a secret clearance (recommend Top Secret).

1.4.15.2.2. OPSEC Coordinators can be officers, NCOs or civilian equivalent of any grade. OPSEC Coordinators will have a secret clearance.

1.4.15.2.2. **(59MDW)** Group commanders will appoint in writing a primary and alternate OPSEC Coordinator who will function as the OPR for all group OPSEC and/or SM activities (this includes the 359th Medical Group). Appointment letters will be forwarded to the 59 MLRS/SGSKX (DP section).

1.4.15.3. Submit request through servicing MPF for award of SEI 9O or 234 as appropriate for individuals appointed as OPSEC PMs, or Coordinators who meet all qualifications.

1.4.15.4. Ensure OPSEC is integrated into planning efforts to increase mission effectiveness. Ensure organizational planners are trained to incorporate OPSEC into all functional areas of plans.

1.4.15.4. **(59MDW)** The 59 MDW OPSEC PMs will provide group OPSEC coordinators with program materials that are standardized, predictable and replicable. Promote continuity of program elements within the wing. Provide sufficient guidance to ensure OPSEC program management has the following critical aspects: commander involvement, operational focus, integration, coordination, and self-inspection.

1.4.15.5. Ensure critical information lists (CIL) are developed and procedures are in place to control critical information and associated indicators.

1.4.15.5. **(59MDW)** Provide group OPSEC coordinators with a standardized OPSEC Self-Assessment Checklist.

1.4.15.5.1. **(Added-59MDW)** Provide group OPSEC coordinators with a standardized OPSEC Continuity Folder/Table of Contents:

1.4.15.5.2. **(Added-59MDW)** Tab A: Current OPSEC PM/SM or Coordinator Appointment Memorandum.

1.4.15.5.3. **(Added-59MDW)** Tab B: OPSEC Directives: AFI 10-701 and all related headquarters Air Education and Training Command and 502d Air Base Wing supplements.

1.4.15.5.4. **(Added-59MDW)** Tab C: Self-Inspection: Self-Inspection Checklists and Results, Evaluations, Surveys, Appraisals, and SAVs. 59 MDW self-inspections are conducted annually. The OPSEC program will use the self-inspection results for their annual OPSEC Program Report.

1.4.15.5.5. **(Added-59MDW)** Tab D: Annual OPSEC Program Reports: Current/Previous Year.

1.4.15.5.6. **(Added-59MDW)** Tab E: OPSEC Working Group Minutes.

1.4.15.5.7. **(Added-59MDW)** Tab F: Miscellaneous Information: OPSEC Training Certificates; metrics on annual training completion (SWANK), and other relevant information.

1.4.15.6. Ensure OPSEC is considered for all organizational contracts. (See Chapter 8)

1.4.15.7. Ensure there is a valid mission need to disseminate information publicly and that review procedures are implemented.

1.4.15.8. Develop, establish, and implement policies and procedures to deny adversaries the opportunity to take advantage of publicly available information, especially when aggregated.

1.4.15.8.1. Ensure the OPSEC program includes all personnel who may have potential access to critical information to include Airmen, DAF civilians, DoD contractors, and family members.

1.4.15.8.2. Budget for OPSEC awareness and education training promotional campaign incentives; budget, acquire, and distribute OPSEC education materials.

1.4.15.8.3. Ensure the OPSEC training program clearly communicates to all personnel that the command will consider for appropriate disciplinary action all failures to follow directed OSPEC measures and/or unauthorized disclosure of critical information.

1.4.15.9. Ensure OPSEC assessments are conducted annually to support operational missions.

1.4.15.10. Ensure OPSEC PMs and Coordinators integrate into or liaise with the information protection, force protection, antiterrorism, and threat working groups and if necessary establish a working group to address OPSEC concerns. In addition, an ad-hoc working group will be established for any large-scale operation or exercise. ***NOTE***: Refer to AFTTP 3-1.IO, *Tactical Employment – Information Operations (U), Attachment 4* for additional guidance.

1.4.15.11. Ensure unit deployment managers add OPSEC awareness training as a mandatory requirement for deploying personnel.

1.4.15.12. Ensure all personnel such as, Web Site administrators, Webmasters, supervisors, public affairs specialists, OPSEC coordinators, PMs, SMOs, etc., who review information for public release complete OPSEC training focused on reviewing information that is intended for posting utilizing Internet-based Capabilities.

1.4.16. **OPSEC PMs, Coordinators and Planners: NOTE: Wing and installation SMOs will follow the guidance in Chapter 2, *Signature Management.***

1.4.16.1. OPSEC PMs are assigned in writing at organizations above the wing/installation level. OPSEC PMs may be assigned to FOAs and DRUs depending on their size, need and organizational reporting chain.

1.4.16.2. OPSEC Coordinators are assigned in writing at each subordinate organization below the wing-level. At the MAJCOM level, National Guard Bureau (NGB), FOAs, or DRUs, OPSEC Coordinators will be appointed within HQ directorates, as appropriate.

1.4.16.3. OPSEC PMs, and Coordinators will:

1.4.16.3.1. Have at a minimum a secret clearance (recommend Top Secret for Wing level positions and higher). In addition, OPSEC PMs will have accounts established on SIPRNET.

1.4.16.3.2. Advise commander or director on all OPSEC and signature management related matters to include developing operating instructions, recommending guidance, and OPSEC measures. Review periodically (at a minimum annually) for currency and update as necessary.

1.4.16.3.3. Tenant organization OPSEC PMs and Coordinators will closely coordinate and integrate with host wing on any OPSEC or signature management initiatives and working groups. However, administrative oversight of tenant organization's program still resides with its HHQ OPSEC PM.

1.4.16.3.4. Incorporate OPSEC into organizational plans, exercises, and activities.

1.4.16.3.5. Develop, implement, and distribute commander's OPSEC guidance memorandums to include CILs, and follow up with new or updates to local or MAJCOM supplements to AFI 10-701, Operations Security (OPSEC). Review periodically (at a minimum annually) for currency and update as necessary.

1.4.16.3.6. Ensure procedures are in place to control critical information and associated indicators. Review periodically (at a minimum annually) for currency and effectiveness.

1.4.16.3.7. Utilize assessment results to mitigate discovered vulnerabilities and aid organization OPSEC awareness efforts.

1.4.16.3.8. Work closely with PA, information protection, web administrators, and other officials designated by the commander who share responsibility for the protection and release of information to ensure critical information is protected.

1.4.16.3.8.1. Prior to submitting to PA, conduct for OPSEC concerns a review of organizational information intended for publication or release to the public. This could include, but is not limited to base newspapers, safety magazines, flyers, web pages, interviews, and information for news articles.

1.4.16.3.8.2. Answer questions, assist in the development of guidance, and provide advice to PA and other information-releasing officials concerning protecting critical information during reviews of public and/or private web pages.

1.4.16.3.9. Provide oversight and management of organization's OPSEC education and training.

1.4.16.3.9.1. Ensure initial mission-oriented OPSEC education and awareness training is accomplished upon arrival of newly assigned personnel and then annually thereafter.

1.4.16.3.9.2. Track initial and annual awareness training and report training initiatives via the annual OPSEC program report to the next HHQ OPSEC PM.

1.4.16.3.10. Coordinate, facilitate, and conduct annual OPSEC assessments such as surveys, annual program reviews and vulnerability assessments as listed in Chapter 6.

1.4.16.3.10.1. Coordinate with appropriate organizations to resolve/mitigate assessment findings as required.

1.4.16.3.10.2. OPSEC PMs will establish and maintain Operations Security Collaboration ARchitecture (OSCAR) accounts.

1.4.16.3.11. Conduct and forward annual program review for the period of 1 Oct through 30 Sep each fiscal year to HHQ according to MAJCOM guidance.

1.4.16.3.12. OPSEC PMs will establish, train, and chair working groups to address OPSEC or signature management concerns and to assist with planning and execution of OPSEC plans and signature management activities.

1.4.16.3.13. Conduct Staff Assistance Visits (SAV) as required or requested.

1.4.17. **All Air Force Personnel:** OPSEC is everyone's responsibility. Ideally, the AF uses OPSEC measures to protect its critical information. Failure to properly implement OPSEC measures can result in serious injury or death to our personnel; damage to weapons systems, equipment and facilities; loss of sensitive technologies; and mission degradation or failure. OPSEC is a continuous process and an inherent part of military culture. Failure to implement directed OPSEC measures will be considered by commanders/directors for appropriate disciplinary action. OPSEC must be fully integrated into the execution of all Air Force operations and supporting activities. All AF personnel (active duty, reserve, ANG, Air Force civilians, and DoD contractors) will:

1.4.17.1. Be familiar with their organization's critical information.

1.4.17.2. Protect critical and/or sensitive information from disclosure.

1.4.17.2.1. When publicly posting or publishing work-related information that potentially contains critical or sensitive information airmen are encouraged to solicit the advice of their immediate supervisor, security office and/or OPSEC PM/SM/coordinator. This will aid in preventing disclosure of critical and/or sensitive information within the public domain. Personnel that do not know what information is critical to an organization cannot reasonably conclude that posting or publishing information will not result in an unauthorized disclosure.

1.4.17.2.1.1. This includes, but is not limited to letters, resumes, articles, electronic mail (e-mail), web site postings, web log (blog) postings, internet message board discussions, or other forms of dissemination or documentation.

1.4.17.2.1.2. Supervisors will provide guidance to personnel regarding critical and/or sensitive information to ensure it is not disclosed in public forums. Each organization's OPSEC PM/SM/coordinator will advise supervisors on means to prevent the public disclosure of critical and/or sensitive information.

1.4.17.2.1.3. Encryption serves as one measure to protect critical or sensitive information transmitted over unclassified networks. Encrypt all e-mail messages containing critical information, OPSEC indicators, and other sensitive information. (AFI 33-119, *Air Force Messaging* Paragraph 6.1.2)

1.4.17.2.2. Do not publicly disseminate, or publish photographs displaying critical and/or sensitive information. Examples include but are not limited to: Improvised Explosive Device strikes, battle scenes, casualties, destroyed or damaged equipment, personnel killed in action (both friendly and adversary), and the protective measures of military facilities.

1.4.17.2.3. Do not publicly reference, disseminate, or publish critical and/or sensitive information already compromised. This provides further unnecessary exposure of the compromised information and may serve as validation.

1.4.17.2.4. Actively encourage others (including family members and family readiness groups) to protect critical and/or sensitive information.

1.4.17.2.5. Destroy (burn, shred, etc.) critical and/or sensitive unclassified information no longer needed to prevent the inadvertent disclosure and/or reconstruction of this material.

1.4.17.3. Implement protection measures as ordered by the commander, director, or an individual in an equivalent position.

1.4.17.4. Know who their organization's OPSEC PM and Coordinator is and contact them for questions, concerns, or recommendations for OPSEC or signature management related topics.

1.4.17.5. Consider attempts by unauthorized personnel to solicit critical and/or sensitive information as human intelligence (HUMINT) gathering and consider it a HUMINT incident.

1.4.17.5.1. AF personnel who have been involved in or have knowledge of a possible incident will report all facts immediately to the nearest supporting AFOSI office as required by AFI 71-101, Vol 4, *Counterintelligence*.

1.4.17.5.2. If these offices are not readily available, HUMINT incidents will be reported to the organization's security manager or commander who will ensure that, without exception, reports are relayed as securely and expeditiously within 24 hours to the nearest AFOSI organization.

Chapter 2

SIGNATURE MANAGEMENT

2.1. Signature Management. Signature management (SM) utilizes a process of profiling day-to-day observable activities and operational trends at installations and each of its resident units. SM incorporates preparatory methodologies of OPSEC and MILDEC creating synergies and resource efficiencies for both the OPSEC and MILDEC wing/installation programs. These methodologies result in identified processes and details that can be used in efforts to defend or exploit operational profiles resident at a given military installation. Defense of operational profiles is accomplished by implementing protective measures to deny or mitigate adversary collection of critical information. Development of protective measures is often accomplished using MILDEC tactics, techniques and procedures (TTPs). The TTPs used for protection of operational profiles are collectively referred to as Deception in Support of OPSEC (DISO).

NOTE: The guidance in this chapter is intended for Signature Management personnel at the wing/installation level. The Signature Management Officer (SMO) and Signature Management NCO (SMNCO) take on the responsibilities of the OPSEC and Military Deception (MILDEC) PM.

2.1.1. Signature Management is administered through a wing or installation SMO/SMNCO. An SMO/SMNCO can be appointed the primary or alternate wing or installation OPSEC PM. When an air component commander's MILDEC plan requires Air Force wings and installations to present specified observable activities, the air component commander's MILDEC planner will determine the actions required by the supporting unit(s) and will communicate those requirements to the SMO/SMNCO.

2.1.1. **(59MDW)** Signature Management is administered through the DP section. The officer in charge of the section will serve as the primary, while one of the assigned Antiterrorism Officers will serve as alternate SMO/SMNCO. (**Note**: Both primary and alternate OPSEC PMs will meet the rank/grade requirements set forth in paragraph 2.2., and training requirements listed in paragraph 1.4.15.2., of AFI 10-701).

2.1.2. Signature management, OPSEC, and MILDEC are a commander's responsibility. The SMO/SMNCO will define the local operating environment and capture process points that present key signatures and profiles with critical information value. This process, known as the Base Profiling Process (BPP), is the deliberate effort to identify functional areas and the observables they produce to contribute to the overall signature of day-to-day activities and operational trends. Once the BPP is complete, the results can be used to develop a wing level CIL and identify key process points for potential protection or exploitation. This ultimately provides commanders several options to exploit or deny operational signatures to ensure mission effectiveness.

2.1.2. **(59MDW)** The SMO/SMNCO will solicit and compile information collected from Group OPSEC Coordinators to identify functional areas and observables to contribute to the overall signature of day-to-day activities and operational trends. These results will be used to help develop a wing level critical information list (CIL) and identify key process points for potential protection or exploitation.

2.2. Wing or installation commanders will:

2.2.1. Appoint in writing a primary and alternate SMO/SMNCO who will function as the OPR for all SM activities. The primary SMO will be an O-3 or above, or civilian equivalent. The alternate SMO will be an E-6 or above, or civilian equivalent. Under no circumstances will contract personnel be appointed as a primary or alternate SMO/SMNCO. At a minimum, SMO/SMNCOs will have a secret clearance (recommend Top Secret) and have two years retainability in the position or as area tour length dictates (remote tours only). Organizations requiring appointment of an SMO/SMNCO for less than two years will request, in writing, a waiver through their MAJCOM OPSEC PM from AF/A3Z-CI.

2.2.1.1. In the event that host and tenant organizations on a given installation are subordinate to different MAJCOMs, the host MAJCOM OPSEC PM will coordinate and document how SM using protective and exploitation countermeasures will be conducted on that installation.

2.2.1.1.1. All wings based on the installation, regardless of their MAJCOM affiliation, will have a SMO/SMNCO assigned. However, the host wing/installation SMO/SMNCO will act as the lead for all SM activities. This agreement will be stipulated on a Memorandum of Agreement (MOA) and should carry the weight of each signatory Wing Commander on the MOA as the designated SMO/SMNCO executes their duties for the installation.

2.2.1.1.1. **(59MDW)** The 502d Air Base Wing (502 ABW) has determined all tenant wings assigned, will act as lead for their own SM activities. The 59 MDW will however, continue to coordinate with the 502 ABW to obtain relevant information and assistance not available within the 59 MDW. No Memorandum of Agreement is required as functions by the 502 ABW will be provided as a courtesy and/or sharing function only.

2.2.1.1.2. The substance of this arrangement will be documented and kept on file for every installation for which this condition applies and incorporated into MAJCOM supplements to this instruction. A copy of the MOA will be forwarded to the MAJCOM OPSEC PM and AF/A3Z-CI.

2.2.2. Submit request through servicing MPF for award of special experience (SEI) 9O or 234 as appropriate for individuals appointed as SMO/SMNCOs who meet all qualifications as identified in the Air Force Officer and Enlisted Classification Directories.

2.3. Signature Management Officer/Signature Management Non-Commissioned Officer will:

2.3.1. Follow guidance in this instruction and when appointed/assigned for MILDEC, follow AFI 10-704, *Military Deception Program*.

2.3.2. Advise the commander on all SM related matters, to include developing and recommending policy, guidance, and instructions. Review periodically for currency and update as necessary.

2.3.3. Use the base profiling process to develop and maintain a master checklist of all activities associated with the mission areas for the wing or installation (i.e., recall, mobility processing, aircraft generation, airlift load generation and marshaling, munitions, personnel and equipment deployment, etc.). The checklist will be modified, as required, to support

tasks associated with supported commander's requirements. Therefore, well-developed master checklists are mandatory.

NOTE: MAJCOM subordinate organizations below the air component level are NOT required to develop supporting MILDEC tabs (C-3A) to combatant command plans or supporting air component plans.

2.3.4. Develop and maintain a current commander approved CIL.

2.3.5. Implement SM execution checklists as directed or authorized by their wing or installation commander, MAJCOM OPSEC PM, or the supported air component commander, as appropriate.

2.3.5. **(59MDW)** Implement SM execution checklists as directed or authorized by the 502 ABW or 802d Mission Support Group (802 MSG), as appropriate.

2.3.6. Identify key personnel involved in the planning and execution of each of the major functional mission areas, and select subject matter experts (SMEs) who can assist in the development, exercising, and execution of the protective or exploitation countermeasures and activities. Grant access to SM material and plans on the commander's authority alone (this may be delegated to the SMO/SMNCO for expediency as determined by the commander).

2.3.6. **(59MDW)** Granting of access to SM material and plans will be delegated to the 59th Medical Support Group Commander/Deputy Commander; 59 MLRS Readiness Flight Commander; and/or Chief, Disaster Preparedness and Plans.

2.3.7. Work closely with antiterrorism, force protection, information protection, PA, web administrators, and other officials designated by the commander who share responsibility for the protection and release of information to ensure critical information is protected.

2.3.7. **(59MDW)** Coordinate with 802 MSG Antiterrorism Office (ATO); 802 Public Affairs (via the 59 MDW/PA), 59 MDW Information Assurance and Protection Office; and other related agencies to ensure critical information is protected.

2.3.8. Answer questions, develop guidance and provide advice to PA and other information releasing officials concerning protecting critical information during reviews of public and/or private web pages.

2.3.9. Attend the Air Force Signature Management Course within 90 days of appointment or by the next available class. If scheduling conflicts exist, MAJCOM OPSEC PMs must document and ensure SMO/SMNCOs are scheduled for the next available course not to exceed 180 days. If training is not completed within 180 days, MAJCOM OPSEC PMs must request a waiver from AF/A3Z-CI.

2.3.10. Conduct SM exercises at the wing or installation as directed by the parent MAJCOMs supplemental guidance.

2.3.11. Work with exercise evaluation teams to observe and evaluate mission profiles and signatures, as well as measures of effectiveness (MOE) and measures of performance (MOP) that assess the organizations ability to mitigate loss of critical information. Evaluate how organization personnel execute protection or exploitation measures. Any deficiencies or best practices will be submitted in after action reports and to the AF lessons learned database

(**https://www.jllis.mil/usaf**/) when applicable. Lessons learned will be used to develop tactics improvement proposals (TIPs) IAW AFI 10-204 and AFI 11-260.

2.3.12. Establish, train, and coordinate with the unit SM working group (SMWG) members to assist with planning and execution of SM activities.

2.3.13. Coordinate, facilitate, and serve as the focal point for all assessments in support of SM activities such as surveys, annual program reviews, and vulnerability assessments as listed in Chapter 6.

2.3.14. Develop and forward annual program reviews/reports for the period of 1 Oct through 30 Sep each fiscal year to HHQ according to MAJCOM guidance.

2.4. Signature Management Planning and Coordination. NOTE: Ensure proper security guidelines are followed when planning and coordinating SM activities.

2.4.1. Submit SM exercise concepts and execution checklists to their MAJCOM for coordination (refer AFI 10-704 and the MAJCOM Supplement for more details).

2.4.1. **(59MDW)** Submit SM exercise concepts and execution checklists to the 59 MDW Exercise, Evaluation, and Training (EET) Team Chief for coordination with the 802 MSG/ATO and/or 502 ABW OPSEC PM.

2.4.2. Submit SM execution checklists supporting real-world operations to the appropriate tasking authority (e.g., supported air component commands or MAJCOM OPSEC PM).

2.4.3. For SM activities utilizing exploitation countermeasures that require implementation outside of the installation, coordinate with the host wing/installation MILDEC POC (refer to AFI 10-704, Paragraph 2.4.3).

2.4.4. Request assistance from the intelligence organization at the next level of their administrative and/or operational chain of command when requiring intelligence that exceeds organic capability. Counterintelligence support will be requested from the unit's local AFOSI detachment.

2.4.4. **(59MDW)** Ensure all requests for assistance from intelligence organizations are coordinated through the 802 ATO and/or 502 ABW OPSEC PM.

2.4.5. Organizations needing assistance from Air Staff will make their request through their MAJCOM OPSEC PM.

2.5. Exploitation Countermeasures (Refer to AFI 10-704, Paragraph 2 4.3 for additional guidance).

Chapter 3

OPSEC PLANNING

3.1. General. This chapter provides direction for planners at wings, Air Force Component Headquarters (AFFOR and AOC) to integrate OPSEC into plans. Air Force forces can be under observation at their peacetime bases and locations, in training or exercises, while moving, or when deployed to the field conducting actual operations. OPSEC methodology provides systematic and comprehensive analysis designed to identify observable friendly actions that could betray intentions or capabilities. Therefore, OPSEC principles must be integrated into operational, support, exercise, and acquisition planning. All plans will be reviewed periodically to ensure currency and updated when required.

3.1.1. OPSEC PMs, SMO/SMNCOs, or Coordinators will assist organization planners to incorporate protection of critical information and indicators into supported operational plans (OPLANS) and supporting plans. They will also assist exercise planners in developing master scenario events listings (MSEL) and MOP to train organization personnel in the application or execution of countermeasures (See AFDD 2, *Operations and Organizations*, for more information concerning MOE and MOP.

3.1.2. OPSEC Planners will follow guidance as outlined in AFI 13-1AOC, Volume 3, *Operational Procedures-Air and Space Operations Center*, and Chapter 3 of this document.

3.2. Operational Planning. OPSEC will be included in all OPLANs, concept plans (CONPLANs), functional plans (FUNCPLANs), and operation orders (OPORDS), etc.. Planners will use existing TTPs to develop Tab C to Appendix 3 to Annex C to the OPORD or OPLAN. The planning staff will identify critical information and OPSEC indicators from all functional areas requiring protection throughout each phase of the operation. Risk assessments will be used to identify applicable countermeasures to mitigate any unacceptable operational risks. MOP and MOE will be developed for each OPSEC measure.

3.2.1. Operational planning is typically focused at the Air Force Component Headquarters (AFFOR and AOC), with reach-back support outside the theater when appropriate. When planning duties are split, all responsible entities will integrate OPSEC into their planning efforts (see also JP 3-13.3, *Operations Security*, Chapter 3). As the supported organization, the theater AOC will resolve debates and provide general guidance.

3.3. Support Planning. Integrate OPSEC into all wartime and contingency plans as well as support plans, i.e., programming plans and in-garrison expeditionary site plans.

3.4. Exercise Planning. In order to enhance combat readiness and improve crisis response, OPSEC will be included in all exercise plans (EXPLANs). Specific OPSEC and/or signature management scenarios will be included in the exercise MSELs with MOE and MOP to assess the proficiency of functional planners to mitigate loss of critical information and organization personnel to execute countermeasures. Deficiencies or best practices will be submitted to the AF lessons learned database (**https://www.jllis.mil/usaf**/) when applicable to assist in the assessment of critical information being posting in public forums. Lessons learned will be used to develop tactics improvement proposals (TIPs) IAW AFI 10-204, *Readiness Exercises and After-Action Reporting Program*, and AFI 11-260, *Tactics Development Program*.

3.4.1. OPSEC measures will also be employed during exercises to minimize observations of sensitive training activities by adversary surveillance and treaty verification activities.

3.5. Acquisition Planning. OPSEC requirements will be determined for all acquisitions and contractor-supported efforts beginning with operational capabilities requirements generation and continues through design, development, test and evaluation, fielding, sustainment and system disposal. When required to protect sensitive military operations, commanders will ensure OPSEC requirements are added to contracts. Commanders will evaluate contractor-developed and proposed OPSEC programs for compliance with required standards.

NOTE: For more detailed planning instructions, refer to AFI 10-400 series publications.

Chapter 4

OPSEC PROCESS

4.1. General: OPSEC is an iterative five-step process: 1) Identify critical information; 2) Analyze threats; 3) Analyze vulnerabilities; 4) Assess risk; and 5) Apply countermeasures. Although normally applied in a sequential manner the process during deliberate or crisis action planning, dynamic situations may require any step to be revisited at any time.

4.2. Identify Critical Information:

4.2.1. Critical information is a specific fact about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively, so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. The product of the first step in the OPSEC process is to record your critical information in a critical information list (CIL).

4.2.2. Critical information is best identified by the individuals responsible for the planning and execution of the organization's mission. A working group or staff planning team can most effectively accomplish this task. Once a CIL is developed, commanders must approve the list and then ensure their critical information is protected and/or controlled.

4.2.3. Critical information will be identified at the earliest stages of planning an operation or activity and continuously updated as necessary to support mission effectiveness.

4.3. Analyze Threats:

4.3.1. A threat is an adversary with the capability and intent to undertake action detrimental to the success of program activities or operations.

4.3.2. The primary source of local threat information is your local AFOSI detachment. For mission related intelligence support, contact your local intelligence unit. Generic validated threat data is provided by the Defense Intelligence Agency via the OPSEC assessment tool, OSCAR.

4.3.3. Intelligence organizations analyze the threat through research of intelligence, counterintelligence, and open source information to identify who is likely to disrupt, deny, degrade, or destroy planned operations.

4.3.4. A threat assessment should identify adversaries, their goals, what they already know, their capability and intent to collect critical information, and potential courses of action.

4.4. Analyze Vulnerabilities:

4.4.1. A vulnerability exists when the adversary is capable of collecting critical information or indicators, analyzing them and then acting quickly enough to impact friendly objectives. The vulnerability can be your procedures, a failure of traditional security, poor judgment on the part of leadership, the fact that we process critical information on data based systems, or the system's design itself.

4.4.1.1. An indicator is a friendly detectable action and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

4.4.2. A vulnerability exists when the adversary is capable of collecting critical information and/or indicators, correctly analyzing them, and then takes timely action. The adversary essentially uses your critical information to support their decision-making process. The adversary has then exploited your vulnerability to obtain an advantage over you.

4.4.3. A vulnerability analysis is the examination of your processes, projects or missions to determine if you have inherent, naturally occurring or self-induced vulnerabilities or indicators that put your critical information and thus your mission at risk.

4.5. Assess Risk:

4.5.1. A risk is a measure of the potential degree to which protected information is subject to loss through adversary exploitation. Risk is assessed as the probability an adversary will gain knowledge of your critical information and the impact (on your mission) if the adversary is successful. A working group or staff planning team must conduct a risk assessment and develop recommended countermeasures based on operational planning and current operating environment. A typical risk assessment will:

4.5.1.1. Compare vulnerabilities identified with the probability of an adversary being able to exploit it in time to be useful to determine a risk level.

4.5.1.2. Determine potential countermeasures to reduce vulnerabilities with the highest risk. The most desirable countermeasures are those that combine the highest possible protection with the least resource requirements and/or adverse effect on operational effectiveness.

4.6. Apply Countermeasures:

4.6.1. Countermeasures are anything that effectively negates or mitigates an adversary's ability to exploit vulnerabilities. Countermeasures may be both offensive and defensive in nature.

4.6.2. Potential countermeasures, among other actions are, camouflage, concealment, deception (CCD), intentional deviations from normal patterns, and direct strikes against adversary collection.

4.6.3. The working group or staff planning team through the OPSEC PM, SMO or Coordinator will submit recommended countermeasures for commander approval through the operational planning process for employment or through appropriate staffing process. Organizations that do not have or require a planning cell will submit recommended countermeasures to the commander through appropriate staffing process.

4.6.4. Countermeasures must be synchronized with other components of IO to achieve synergies in efforts to influence the adversary's perceptions and situational awareness. Care must be taken so that countermeasures do not become vulnerabilities or unacceptable indicators themselves.

4.6.5. During the execution of countermeasures, the adversary's reaction to the measures is monitored, if possible, to provide feedback that can be used to assess effectiveness or determine potential unintended consequences.

Chapter 5

OPSEC EDUCATION AND TRAINING

5.1. General. All Air Force personnel (military and civilian) and contractors who have access to mission critical information require a general knowledge of threats, vulnerabilities and their responsibilities associated with protecting critical information. This is accomplished through initial and annual OPSEC training. Standardized AF OPSEC awareness training located on the AF Advanced Distributed Learning Service is the baseline training required for all personnel. Organization specific training will be provided in addition to this training to ensure all personnel in the Air Force are aware of local threats, vulnerabilities and critical information unique to their duty assignment. OPSEC PMs/SMO/SMNCOs/Coordinators, and planners assigned to OPSEC positions require more in-depth training designed to ensure proper management, planning, and execution of organizational OPSEC programs.

5.2. All Personnel:

5.2.1. Awareness education will be provided to all personnel (military, civilian and contractors) upon initial entrance/accession into military service.

5.2.2. Awareness education provided in accession programs will encompass what OPSEC is, its purpose, threat awareness and the individual's role in protecting critical information.

5.2.3. Organization-specific initial OPSEC awareness training will be provided at each new duty location as part of in-processing and annually thereafter, at a minimum. Personnel must understand the scope of the threats, the nature of the vulnerabilities and their responsibility to execute countermeasures to protect critical information and organization specific OPSEC indicators. Annual training must include, at a minimum, updated threat and vulnerability information, changes to critical information and new procedures and/or countermeasures implemented by the organization.

5.2.3. **(59MDW)** Unit-specific initial OPSEC training is the responsibility of the group OPSEC coordinator (can be delegated to unit OPSEC coordinators who meet grade/training requirements). As a minimum, this training must include a review of the 59 MDW Critical Information List; a discussion of Joint Base San Antonio threat and vulnerability information; and new procedures and/or OPSEC measures implemented by the organization. In addition to items listed in this paragraph for Annual OPSEC Awareness Training, group OPSEC coordinators will direct unit personnel to the Advance Distributed Learning Service (ADLS) OPSEC Awareness course (embedded within the Information Assurance/Protection course). The course must be accomplished once each calendar year.

5.2.3.1. In addition, commanders/directors shall encourage assigned personnel to share OPSEC awareness information with family members (both immediate and extended) and social network "friends". This will ensure family members and friends understand how adversaries can use public media sources such as but not limited to web sites, blogs, social networking sites, newspapers, and television to obtain critical information that can be used to target AF members and their families.

5.2.3.2. Procurement of low value promotional and awareness aids such as pens, pencils, magnets, key chains, lanyards, etc., is authorized for the exclusive intent to promote

OPSEC awareness and education in accordance with organizational missions. For Guidance, refer to AFI 65-601, Vol 1, *Budget Guidance and Procedures*.

5.2.4. OPSEC PMs/SMO/SMNCOs/Coordinators will provide OPSEC training or training materials to contract employees within 90 days of employees' initial assignment to the contract.

5.2.4. **(59MDW)** OPSEC PMs/SMO/SMNCOs/Coordinators will provide OPSEC training or training materials to contract employees within 90 days of employees' initial assignment to the contract. Additional training is located on the SWANK website. Contractors without access to ADLS will complete training via SWANK.

5.3. OPSEC PMs/SMO/SMNCOs/Coordinators, Planners, Inspection Teams:

5.3.1. Formal OPSEC training. Formal OPSEC training is required for all OPSEC PMs/SMO/SMNCOs, and planners assigned to OPSEC positions. Formal OPSEC training is any in-residence course intended to support the AF OPSEC Program.

5.3.1.1. Completion of the Air Force Signature Management Course is mandatory for OPSEC PMs (below MAJCOM level), SMO/SMNCOs and planners within 90 days of appointment and within 180 days of appointment for MAJCOM OPSEC PMs. If scheduling conflicts exist, MAJCOM OPSEC PMs must document and ensure SMO/SMNCOs are scheduled for the next available course not to exceed 180 days. If training is not completed within 180 days, MAJCOM OPSEC PMs must request a waiver from the AF OPSEC PM.

5.3.1.1. **(59MDW)** 59 MDW OPSEC PMs and group OPSEC coordinators will complete the OPSE 1300 course located on the IOSS website within 30 days of appointment. Group OPSEC coordinators will receive additional training from the 59 MDW OPSEC PM.

5.3.1.2. Completion of OPSE-2500, *OPSEC Analysis and Program Management Course* is required for all OPSEC PMs within 90 days of appointment. If scheduling conflicts exist, OPSEC PMs must document and ensure they are scheduled for the next available course not to exceed 180 days. If training is not completed within 180 days, individuals must notify their HHQ OPSEC PM.

5.3.2. OPSEC Orientation Training. OPSEC Coordinators, planners, vulnerability assessment team, inspection team, and Operations Security Working Group (OWG) members are required to complete OPSEC orientation training within 30 days of assignment to OPSEC duties. The Interagency OPSEC Support Staff's (IOSS) multimedia product "An Introduction to OPSEC (An Interactive Primer by the Department of Defense)" is the accepted method for completing OPSEC orientation. It is high recommended personnel seek out additional OPSEC training to assist in accomplishing their duties. Information regarding required and additional OPSEC training can be received from OPSEC PMs or SMO/SMNCOs.

5.3.3. OPSEC Planner Mission Readiness Training (MRT). Personnel working as OPSEC planners in an AOC require MRT that encompasses initial qualification training (IQT), mission qualification training (MQT), and continuation training (CT). IQT will consist of formal training (either SMC or OSPE-2500, OPSEC Analysis and Program Management

Course). MQT will consist of mission specific training and will be documented via Stan/Eval processes. CT will be provided as needed. MRT will be accomplished during training exercises.

5.3.4. Quality Assurance Evaluators (QAE) and Contracting Officer Technical Representatives (COTR) will complete OPSEC training designed for QAE and COTR duties provided by the OPSEC PM/SMO/SMNCO/Coordinator within 90 days of being assigned duties. OPSEC PM/SMO/SMNCO/Coordinators are encouraged to use the training located on Defense Acquisition University - "CLC 107, OPSEC Contract Requirements" **https://learn.dau.mil/html/clc/Clc1.jsp** along with any specific unit tailored OPSEC training.

5.3.5. Web Site Administrators, Webmasters, and anyone (superiors, public affairs specialist, OPSEC coordinators, PMs, SMO/SMNCO, etc.) who has the responsibility to review information for public release will complete OPSEC training focused on reviewing information to be posted on Internet-based Capabilities. The IOSS OSPE 1500, OPSEC & Public Release Decisions and OPSE-3500, OPSEC & Web Risk Assessment are the AF acceptable training methods to fulfill this requirement.

5.4. Joint and Interagency OSPEC Support:

5.4.1. Joint Operations Security Support Center. The Joint OPSEC Support Center (JOSC) provides direct support to the Joint Information Operations Warfare Command (JIOWC) and Joint Force Commanders through the integration of OPSEC into operations, plans, and exercises and by providing staff-level program development and training and OPSEC vulnerability assessments when directed. The JOSC serves as the OPSEC Joint Center of Excellence and provides OPSEC training and instruction in support of the Combatant Commands.

5.4.2. Interagency Operations Security Support Staff. The Interagency OPSEC Support Staff (IOSS) supports the National OPSEC Program by providing tailored training, assisting in program development, producing multimedia products and presenting conferences for the defense, security, intelligence, research and development, acquisition and public safety communities. Its mission is to help government organizations develop their own, self-sufficient OPSEC programs in order to protect United States programs and activities. IOSS offers a multitude of OPSEC training aids available to all OPSEC professionals.

5.4.3. Air Force personnel are welcome and encouraged to receive training from the JOSC and IOSS. The courses offered by the JOSC and IOSS provide a broader perspective of OPSEC at the joint and interagency level while Air Force OPSEC training is oriented specifically to an Air Force audience.

Chapter 6

ASSESSMENTS

6.1. General:

6.1.1. Assessments are performed to achieve two specific purposes: To ensure required policies and procedures are in place to protect critical information and to gauge the overall effectiveness of countermeasures (See Table 6.1 for OPSEC assessment types).

6.1.2. The Air Force provides several tools to assist OPSEC PMs/SMO/SMNCOs/Coordinators and planners to obtain information and data to perform risk analysis. These tools assist in assessing the level of exposure of critical information and operational indicators to adversary observation, surveillance, and intelligence sensors. OPSEC planners, PMs and Coordinators use assessment results within the risk management process to determine countermeasures which can mitigate or negate risk to operations.

6.1.3. Assessment of program effectiveness is accomplished through the development of MOP and MOE. MOP are developed to measure how well an activity is performed via the execution of countermeasures. MOE measure how well an activity achieved its intended effect. Any deficiencies or best practices identified are documented in lessons learned and TIPs. Inspector General (IG) inspections are also used to assess organization compliance, operational readiness, and nuclear surety. Submit TIPs IAW AFI 11-260.

6.1.4. OPSEC PMs, SMO/SMNCO and Coordinators will utilize the OPSEC risk assessment tool OSCAR to accomplish annual assessments and program reviews.

6.1.5. For assistance in preparing for inspections and assessments, utilize the OPSEC Core Capabilities Checklists provided at the below link to the Air Force Inspection Agency's (AFIA) web site. The AFIA checklists are divided into functional levels (wing, unit and AOC) and provide the basics for maintaining your OPSEC program. MAJCOM and AF IG teams will utilize these checklists when conducting inspections. **https://webapps.afrc.af.mil/afia/SearchChecklist.aspx?Command=AFIA&Type=CI&State=live&Dir=A3** .

6.1.6. Any request for external assessments must be made through your respective HHQ OPSEC PMs.

6.1.7. MAJCOM OPSEC PMs are the focal point for requesting and scheduling all external assessments and setting all priorities between command organizations.

6.2. Annual OPSEC Program Review:

6.2.1. The Annual OPSEC program review is a continual processes that involve combining data collected from MOP, MOE, exercise after action reports, lessons learned, nuclear surety, operational readiness/compliance inspections, and annually conducted self-assessments/self-inspections. Annual program reviews will be accomplished utilizing OSCAR and report to the HHQ OPSEC PM. This has been assigned Report Control Symbol (RCS) DD-INTEL(A) 2228.

6.2.2. OPSEC PMs, SMO/SMNCOs, and Coordinators will conduct annual program reviews to ensure the health of their program, evaluate compliance with applicable policies and to identify short-falls and vulnerabilities.

6.2.3. Annual OPSEC Program Reviews will provide information relating to the following areas:

6.2.3.1. Executive Summary: Full-time OPSEC PM appointed, budget plan developed, level of importance within the organization.

6.2.3.2. OPSEC Initiatives/Projects/Successes: How is the commander making OPSEC a priority? (Policy and guidance, social networking site reviews, etc.)

6.2.3.3. OPSEC Training and Awareness: Has the commander assigned a fully trained SMO/SMNCO to the SMO/SMNCO position? How is OPSEC awareness education and training conducted in the organization? (Commander's call, unit newsletter, incorporating OPSEC into exercises).

6.2.3.4. OPSEC in Operational Planning: How has the commander incorporated OPSEC into the unit's operational plans? (Implementing OPSEC measures, unique tools used to incorporate OPSEC, integration efforts)

6.2.3.5. Assessment/Surveys: Does the assigned OPSEC PMs have an established OSCAR account? Total number of assessments and surveys accomplished to determine the overall effectiveness of the unit's OPSEC program?

6.2.4. At MAJCOM-level, this report will be signed by the Director responsible for the MAJCOM's OPSEC program or higher-level authority. At wing-level and below the commander or their designated representative will sign it.

6.3. Staff Assistance Visit (SAV):

6.3.1. SAVs may be conducted as needed by HHQ OPSEC PMs, SMOs or other organization SMEs to assist organizations in repairing dormant, non-compliant, deficient programs or for any other reason deemed necessary by the commander. The organization will request such assistance through their respective chain-of-command and will fund travel. SAVs check for program compliance (i.e., Special Interest Items, Air Force Instructions, MAJCOM policies, etc.), identify and resolve shortfalls, and provide guidance to OPSEC PMs, SMOs, and Coordinators as required.

6.4. Survey:

6.4.1. An OPSEC survey is the application of the OPSEC methodology by a team of subject matter experts to conduct a detailed analysis of all activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries. The purpose of an OPSEC survey is to determine if OPSEC countermeasures are effectively mitigating identified threats and vulnerabilities.

6.4.1.1. The survey requires a team of experts to look at an activity from an adversary's perspective to determine if critical information may be disclosed through normal operations and functions, to identify vulnerabilities, and propose countermeasures to mitigate them.

6.4.1.2. Survey team members attempt to use the collection techniques and tools of known adversaries. Commanders/directors are encouraged to use OPSEC support capabilities (reference Paragraph 6.6) to assist in conducting surveys, if available.

6.5. Web Content Vulnerability Analysis:

6.5.1. Web content vulnerability analysis is a formal, structured process of evaluating information posted on organizational public and private web sites. This analysis complements each organization's requirement to have processes in place ensuring all information posted to publicly accessible web sites are reviewed and approved prior to posting.

6.5.2. Organizations will conduct web content vulnerability analysis of content on their organization's public and private web sites for its sensitivity (i.e., critical information, For Official Use Only, or other controlled unclassified information categories) or sensitivity in aggregate to determine potential vulnerabilities by adversary exploitation. Prior to conducting a web content vulnerability analysis, follow these guidelines:

6.5.2.1. Ensure a legal review is conducted by the Judge Advocate (JA) of your web vulnerability analysis processes prior to conducting assessments of information on your organizational public and private web sites.

6.5.2.2. Ensure automated key word searching software (i.e. web crawlers) are approved for use by the local Systems Integration organization prior to utilization.

6.5.2.3. If using automated software to retrieve information from web sites, ensure it is used only to assess the owning organizations public and private web sites.

6.5.2.4. Develop strict procedures regarding who can conduct assessments, when the assessments will be conducted, what will be done with the information retrieved, who can view the information, and how long the information will be maintained on file.

6.5.2.5. Manage and dispose of information collected and analyzed in accordance with AFMAN 33-363, *Management and Records* and The AF Records Disposition Schedule (AFRIMS).

6.6. Support Capabilities:

6.6.1. Telecommunication Monitoring Assessment Program (TMAP) involves the collection and analysis of information transmitted via unsecured and unprotected communications systems (email, radio, telephone, and internet-based capabilities) to determine if these systems are being used to transmit critical, sensitive or classified information. TMAP helps in evaluating an organization's OPSEC posture and determining the amounts and types of information available to adversary collection entities. TMAP is accomplished only within certain legal parameters and may only be performed by authorized personnel. See AFI 10-712, *Telecommunication Monitoring Assessment Program (TMAP)* for further guidance.

6.6.2. Information Operations Mobile Training Teams (IO MTT) provide a three-phased event conducted by the 57th and 177th Information Aggressor Squadrons (57/177 IAS) where they assess an organization's network security, physical security, and counter-HUMINT capabilities. The first phase is executed remotely through dot-com capabilities and the collection and exploitation of open source information; the second phase is accomplished at the installation itself and finally through replication of the attack, the 57/177 IAS trains the

information owners and base personnel on the threat to USAF critical information and their responsibilities of securing it. IO MTT identify operation vulnerabilities, operational impacts, and exercise threat response procedures. OPSEC PM/SMO/Coordinators use information identified by the IO MTT to conduct the OPSEC process.

6.6.3. HUMINT Vulnerability Assessments (HVA) are used to assess the types and amount of information being exposed to potential HUMINT collection with respect to your missions.

6.6.3.1. Results of these collection capabilities identify the possible level of exposure of critical information and operational indicators to adversary observation, surveillance, and intelligence sensors. Once analyzed, the information assists in the performance of risk assessments for blue forces to develop measures to counter the threat based on vulnerabilities identified.

6.6.4. OSCAR is a web-based tool developed to provide a standardized process to assist the OPSEC community with assessing and quantifying risk to critical information allowing decision makers to make informed decisions on what countermeasures to implement to reduce the organization's overall risk and vulnerabilities. OSCAR provides posture, vulnerabilities and risk level status, which can provide assistance in developing plans and management reports. It provides a platform for planners to test remediation options and scenarios and provides an expert knowledge base to assist in threat assessments. All OPSEC program managers are required to establish an OSCAR account. OSCAR accounts can be requested by going to the following link: **https://register.dtic.smil.mil/wobin/WebObjects/RegLite?SiteID=OSCAR** on SIPR.

6.6.5. Organizations will request support through their SMO or OPSEC PM to their respective MAJCOM OPSEC PM. MAJCOM OPSEC PMs will submit TMAP requests to 624 OC/CPD at 624OC/**CPD@lackland.af.smil.mil**; IO MTT request are submitted to HQ ACC/A3I at **acc.xoz.iwd@langley.af.mil** and HVA requests are submitted IAW procedures of your local AFOSI detachment.

Table 6.1. OPSEC Assessment Types and Support Capabilities

Assessment Type	Purpose	Methodology	Frequency	Request Procedures	Reporting
IO MTT	Assess and identify operations vulnerabilities, operational impacts, and exercise threat response procedures.	Red team simulates threats to identify vulnerabilities, operational impacts, and exercise threat response procedures	As requested or required	Wing or installation CC requests through MAJCOM OPSEC PM	Out-brief and report to wing and/or installation CC
OPSEC Survey	Determine if OPSEC countermeasures are effectively	The survey team, from an adversarial perspective,	At least every three years	N/A (CC may request other	Out-brief and report to organization CC

	mitigating identified threats and vulnerabilities.	identifies information disclosed through normal operations and functions		OPSEC support capabilities to assist if available)	
OSCAR	Web-based tool that provides a standardized process to assist in assessing and quantifying risk to critical information	OPSEC PMs/SMOs/Coordinators utilize to assist in evaluating risk to mission	At least Annually	N/A	OPSEC PM/SMO/coordinator reports to organization CC and up channel to HHQ PM when required (i.e., annual program reviews)
Program reviews	-Program health -Policy compliance -Shortfalls	OPSEC PMs, SMOs and Coordinators evaluate the health of OPSEC programs, evaluate compliance with applicable policies and identify vulnerabilities	Annual	N/A	OPSEC PM/SMO/ coordinator reports to organization CC for signature and up channel to HHQ PM
SAV	- Policy compliance - Shortfalls - Provide guidance	OPSEC PMs/SMOs assess subordinate organizations	As requested or required	N/A	Report to subordinate organization CC and OPSEC PM/SMO/ coordinator
TMAP	ID potential vulnerabilities	Collect and analyze communications	As requested or required	Organization CC requests through HHQ OPSEC PM	Report to requesting organization

Chapter 7

AIR FORCE OPSEC ANNUAL AWARDS PROGRAM

7.1. General:

7.1.1. The annual Air Force OPSEC Awards program provides recognition of Air Force OPSEC professionals and is a priority for the Air Force OPSEC program. This awards program runs concurrently on a fiscal year basis with the National OPSEC Awards program conducted by the IOSS. Only AF OPSEC awards submitted by the Air Force OPSEC PM will be considered by the IOSS for the National OPSEC Awards.

7.1.2. Air Force organizations wishing to compete for AF OPSEC annual awards must submit nominations through their respective MAJCOMs to reach AF/A3Z-CI, NLT 31 Oct each year.

7.1.3. The Air Force does not award an AF-level award in the multimedia area. Any Air Force organization wishing to compete for the National OPSEC Multimedia Achievement Awards must submit nominations through their respective MAJCOM to reach AF/A3Z-CI, NLT 15 November to meet the IOSS suspense. Go to **http://www.ioss.gov** for further descriptions of the awards and nomination criteria.

7.1.4. Requirements for AF OPSEC awards are listed in AFI 36-2807, Chapter 23, Headquarters United States Air Force Deputy Chief of Staff Operations, Plans and Requirements Annual Awards Program.

Chapter 8

OPSEC REQUIREMENTS WITHIN CONTRACTS

8.1. General:

8.1.1. Contractors for defense systems acquisition programs as well as other types of Air Force contracts will practice OPSEC to protect critical information for specific government contracts and subcontracts.

8.1.2. It is the responsibility of the organization to determine what measures are essential to protect critical and sensitive information for specified contracts. Organizations should identify OPSEC measures in their requirements documents and ensure they are identified in resulting solicitations and contracts. The organization is responsible for ensuring the appropriate critical program information; OPSEC measures and costs are billed and tracked as a separate line item in all contracts.

8.2. Guidance and procedures:

8.2.1. Organizations will consider OPSEC for all contractual requirements. They must first determine whether there is any form of critical or sensitive information or activities involved in the contract. It is the organization's responsibility to inform the contracting officer when a determination has been made that there are no OPSEC requirements for the contract.

8.2.1. **(59MDW)** 59 MDW PMs will advise 59 MDW OPSEC Coordinators on how to assist their section Contracting Officer Representatives (CORs) prior to initiation of a contract Statement of Work (SOW) or Performance Work Statements (PWS). Information to be considered will be located on the 59 MDW Sharepoint website: **https://readiness.sammc-eis.lackland.af.mil/OPSEC/Shared%20Documents/Forms/AllItems.aspx**.

8.2.2. If there are OPSEC requirements, the organization is responsible for conducting an OPSEC review of the Statement of Work (SOW) or Performance Work Statement (PWS) prior to the time the contracting officer publicizes the SOW or PWS. The SOW/PWS is a publicly released document that can reveal critical information or indicators of critical information. It is critical that the organization OPSEC PM or SMO identify OPSEC requirements in the scope of work.

8.2.3. The organization will specify OPSEC requirements for classified contracts on DD Form 254, *Department of Defense Contract Security Classification Specification*. This form defines classification, regarding, downgrading, declassification, and OPSEC specifications for a contract. Though the DD Form 254 applies to classified contracts, and classified subcontracts, it may also be used for unclassified contracts to specify OPSEC requirements. For unclassified contracts, if the DD Form 254 is not used, the organization will define the specific OPSEC requirements in the contract and the SOW/PWS.

8.2.4. The organization's designated representative is responsible for preparation of the prime contract's DD Form 254. Based on the classification guidance or OPSEC requirements in the prime contract, the prime contractor is responsible for preparation of DD Forms 254 for any subcontracts. This should be done in coordination with the organization's SMO or OPSEC PM and security manager.

8.2.5. The organization will state OPSEC requirements on DD Form 254, contracts and SOW/PWSs with sufficient detail to ensure complete contractor understanding of the exact OPSEC provisions or measures required by the organization. If the OPSEC block is checked on the DD Form 254, the organization shall:

8.2.5.1. Task the contractor to develop an OPSEC program plan to address how the contractor plans to protect critical and sensitive contracted information, and upon organization acceptance, implement the OPSEC program plan.

8.2.5.2. Provide OPSEC guidance for the contractors to use in developing their own OPSEC plan.

8.2.6. The organization will determine OPSEC requirements when the contract involves sensitive information. When it does, the organization will ensure that the contract and SOW/PWS include OPSEC requirements, which must include establishing an OPSEC training program to protect the organization's critical information.

8.2.7. For a contractor to effectively comply with OPSEC provisions of the contract, the organization must provide the following guidance:

8.2.7.1. Organization's critical information.

8.2.7.2. Adversaries' collection threat information as it applies to the organization's mission and the contract.

8.2.7.3. Operations security guidance (at a minimum, the organization will provide a copy of this instruction).

8.2.7.4. Specific OPSEC measures the organization requires (as appropriate).

HERBERT J. CARLISLE, Lt Gen, USAF
DCS, Operations, Plans & Requirements

(59MDW)

GLENN A. YAP, Colonel, USAF, MSC
Administrator, 59th Medical Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DODI 5200.39, *Critical Program Information Within the Department of Defense,* 16 July 2008

DODD 5205.02, *DOD Operations Security (OPSEC) Program,* 6 March 2006

DODM 5205.02-M, DoD Operations Security (OPSEC) Program Manual, 3 November 2008

JP 3-13.3, *Joint Doctrine for Operations Security,* 29 June 2006

JP 1-02, *DOD Dictionary of Military and Associated Terms,* 13 June 2007

CJCSI 3213.01B, *Joint Operations Security,* 27 January 2007

AFPD 10-7, *Information Operations,* 6 September 2006

AFPD 63-1, *Acquisition and Sustainment Life Cycle Management,* 3 April 2009

AFPD 90-2, *Inspector General—The Inspection System,* 26 April 2006

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

AFI 10-204, *Readiness Exercise and After-Action Reporting Program,* 12 July 2002

AFI 10-601, *Capabilities-Based Requirements Development,* 31 July 2006

AFI 10-704, *Military Deception Program, 3*0 August 2005

AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP),* May 2011

AFI 11-260, *Tactics Development Program,* 12 December 2003

AFI 31-501, *Personnel Security Program Management,* 27 January 2005

AFI 33-119, *Air Force Messaging,* 24 Jan 2005

AFI 63-10, *Acquisition and Sustainment Life Cycle Management,* 17 April 2009

AFI 65-601, Vol 1, *Budget Guidance and Procedures,* 3 March 2005

AFI 71-101, Vol 4, *Counterintelligence,* 1 August 2000

AFI 90-201, *Inspector General Activities,* 22 November 2004

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

DD Form 254, *Department of Defense Contract Security Classification Specification*

Abbreviations and Acronyms

AFOSI—Air Force Office of Special Investigations

AFSPOB—Air Force Security Policy and Oversight Board

AFPD—Air Force Policy Directive

ANG—Air National Guard

AOC—Air and Space Operations Center

CCD—Camouflage, Concealment, and Deception

CIL—Critical Information List

CONPLAN—Contingency Plan

CPI—Critical Program Information

CT—Continuation Training

DISO—Deception in Support of OPSEC

DOD—Department of Defense

DODD—Department of Defense Directive

DRU—Direct Reporting Unit

EXPLAN—Exercise Plan

FOA—Field Operating Agency

FSA—Functional Solutions Analysis

FUNCPLAN—Functional Plan

HHQ—Higher Headquarters

HUMINT—Human Intelligence

HVA—HUMINT Vulnerability Assessments

IFO—Influence Operations

IG—Inspector General

IO—Information Operation

IOSS—Interagency OPSEC Support Staff

IQT—Initial Qualification Training

MAF—Mobility Air Forces

MAJCOM—Major Command

MILDEC—Military Deception

MOA—Memorandum of Agreement

MOE—Measures of Effectiveness

MOP—Measures of Performance

MQT—Mission Qualification Training

MRT—Mission Readiness Qualification

MSEL—Master Scenario Events Listing

OPLANS—Operational Plans

OPORDS—Operation Orders

OPR—Office of Primary Responsibility

OPSEC—Operations Security

OSCAR—Operations Security Collaboration ARchitecture

PA—Public Affairs

PM—Program Manager

MISO—Military Information Support Operations

RDT&E—Research, Development, Test and Evaluation

SAV—Staff Assistance Visit

SEI—Special Experience Identifier

SM—Signature management

SME—Subject Matter Expert

SMO—Signature Management Officer

SMWG—- Signature Management Working Group

SOW—Statement of Work

TIP—Tactics Improvement Proposal

TMAP—-Telecommunication Monitoring and Assessment Program

TTP—Tactics, Techniques, and Procedures

Terms

Acceptable Level of Risk—An authority's determination of the level of potential harm to an operation, program, or activity due to the loss of information that the authority is willing to accept.

Acquisition Program—A directed, funded effort that is designed to provide a new, improved, or continuing material, weapons system, information system, or service capability in response to a validated operational need.

Adversary—An individual, group, organization or government that must be denied critical information. Synonymous with competitor/enemy.

Adversary Collection Methodology—Any resource and method available to and used by an adversary for the collection and exploitation of sensitive/critical information or indicators thereof.

Base Profiling—Defining the local operating environment and capture process points that present key signatures and profiles with critical information value. This process is the deliberate effort to identify functional areas and the observables they produce to contribute to the overall signature of day-to-day activities and operational trends.

Continuation Training—Additional advanced training exceeding the minimum upgrade training requirements with emphasis on present or future duty assignments.

Counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities.

Countermeasures—Anything, which effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

Critical Information—Specific facts about friendly intentions, capabilities, or activities vitally needed by adversaries for them to plan and act effectively to guarantee failure or unacceptable consequences for friendly mission accomplishment.

Critical Information List—Those areas, activities, functions, or other matters that a facility/ organization considers most important to protect from adversaries.

Critical Program Information—Elements or components of an research, development and acquisition (RDA) program that, if compromised, could cause significant degradation in mission effectiveness; shorten the expected combat-effective life of the system; reduce technological advantage; significantly alter program direction; or enable an adversary to defeat, counter, copy, or reverse engineer the technology or capability. Includes information about applications, capabilities, processes, and end-items; information about elements or components critical to a military system or network mission effectiveness; and technology that would reduce the U.S. technological advantage if it came under foreign control.

Deception in Support of Operations Security (DISO)—A military deception activity that protects friendly operations, personnel, programs, equipment, and other assets from foreign intelligence security services (FISS) collection.

Human Intelligence monitoring (HUMINT)—A category of intelligence derived from information collected and provided by human sources.

Indicator— Data derived from friendly detectable actions and open-source information that adversaries can interpret and piece together to reach conclusions or estimates of critical or classified information concerning friendly intentions, capabilities, or activities.

Influence Operations— The employment of capabilities to affect behaviors, protect operations, communicate commander’s intent, and project accurate information to achieve desired effects across the cognitive domain. These effects should result in differing behavior or a change in the adversary decision cycle, which aligns with the commander’s objective.

Information Operations—Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Integrated Control Enablers—Critical capabilities required to execute successful air, space, and information operations and produce integrated effects for the joint fight. Includes intelligence, surveillance, and reconnaissance, network operations, predictive battlespace awareness and precision navigation and timing.

Measures of Effectiveness (MOE)—Independent qualitative or quantitative measures assigned to an intended effect (direct or indirect) against which the effect’s achievement is assessed. At

the direct effect level, MOEs answer such questions as, "was the intended direct effect of the mission e.g., target destruction, degradation (to a defined point), or delay (for a given time) created?" At the indirect level, they may answer things like, "has the enemy IADS been degraded sufficiently to allow unimpeded air operations above 15,000 feet?" (*AFDD 2*)

Measures of Performance (MOP)—Objective or quantitative measures assigned to the actions and against which the action's accomplishment, in operations or mission terms, is assessed. MOPs answer questions like, "were the weapons released as intended on the planned target?" (*AFDD 2*)

Operations Security (OPSEC)—OPSEC is a process of identifying, analyzing and controlling critical information indicating friendly actions associated with military operations and other activities to: Identify those actions that can be observed by adversary intelligence systems; Determine what specific indications could be collected, analyzed and interpreted to derive critical information in time to be useful to adversaries; Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

OPSEC Assessment— An evaluative process, conducted annually of an organization, operation, activity, exercise, or support function to determine if sufficient protection measures are in place to protect critical information. An OPSEC program review may include self-generated program reviews, Inspector General inspections, or higher headquarters reviews that specifically address OPSEC.

OPSEC Compromise—The disclosure of critical information or sensitive information which has been identified by the information owner (commander/director) and any higher headquarters that jeopardizes the unit's ability to execute its mission or to adequately protect its personnel and/or equipment. Critical or sensitive information that has been compromised and is available in open sources and the public domain should not be highlighted or referenced publicly outside of intra-governmental or authorized official communications because these actions provide further unnecessary exposure of the compromised information.

OPSEC Coordinator—Acts as an interface to direct and manage all relevant OPSEC matters below the wing-level and reports to the SMO or OPSEC PM.

OPSEC Indicator—Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information.

OPSEC Measure—Methods and means to gain and maintain essential secrecy about critical information.

OPSEC Program Manager—Focal point for all OPSEC related matters at an organization above the squadron level that is not a wing. Ensures OPSEC requirements are in compliance as directed and reviews organizational plans to ensure OPSEC is appropriately considered.

OPSEC Planner—An individual who has been formally trained in the planning and execution of OPSEC.

OPSEC Survey— An OPSEC survey is the application of the OPSEC methodology by a team of subject matter experts to conduct a detailed analysis of all activities associated with a specific organization, operation, activity, exercise, or support function by employing the known collection capabilities of potential adversaries.

OPSEC Vulnerability—A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to prove a basis for effective adversary decision making.

Risk—A measure of the potential degree to which protected information is subject to loss through adversary exploitation.

Risk Analysis—A method by which individual vulnerabilities are compared to perceived or actual security threat scenarios in order to determine the likelihood of compromise of critical information.

Risk Assessment—A process of evaluating the risks to information based on susceptibility to intelligence collection and the anticipated severity of loss.

Sensitive Information— Unclassified information requiring special protection from disclosure that could cause compromise or threat to our national security, an Air Force organization, activity, military member, AF civilian, DoD contractor, or family member.

Signature—Observable activities and operational trends that reveal critical information to adversary intelligence collection.

Signature Management (SM)—the active defense or exploitation of operational profiles resident at a given military installation. Defense of operational profiles is accomplished by implementing protective SM measures to deny adversary collection of critical information. Exploitation of operational profiles is accomplished by using Deception in Support of OPSEC (DISO) to protect critical information.

Signature Management Officer/Noncommissioned Officer (SMO/SMNCO)— Focal point for all SM related matters at the wing or installation level. Ensures tactical level OPSEC and MILDEC requirements are in compliance as directed and reviews wing or installation level plans to ensure OPSEC and MILDEC are appropriately considered to actively defend or exploit operational profiles resident at a given military installation.

Threat—the capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operations.

Threat Assessment—an evaluation of the intelligence collection threat to a program activity, system, or operation.

Vulnerability Analysis—In information operations, a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. See also information operations, information system, security, and vulnerability.

Vulnerability Assessment—A process that examines a friendly operation or activity from the point of view of an adversary, seeking ways in which the adversary might determine critical information in time to disrupt or defeat the operation or activity.

Web Vulnerability Analysis—Process of evaluating information intended for release outside the control of the organization, including release to the public, i.e., public and private web sites.

Working Group—Designated body representing a broad range of line and staff activities within an organization that provides advice and support to leadership and all elements of the

organization. (This can be an OPSEC, SM, threat, or public affairs working group that addresses OPSEC concerns)