

**BY ORDER OF THE  
SECRETARY OF THE AIR FORCE**

**AIR FORCE INSTRUCTION 10-701**



**8 JUNE 2011**

**AIR COMBAT COMMAND  
Supplement**

**17 SEPTEMBER 2012**

**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](http://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: 84

Supersedes: AFI 10-701, 18 October 2007

**(ACC)**

OPR: HQ ACC/A3I

Certified by: (Maj Gen Charles W. Lyon)  
Pages: 44

Supersedes: AFI10-701\_ACCSUP, 22  
January 2009

---

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.

**(ACC) AIR FORCE INSTRUCTION (AFI) 10-701, OPERATIONS SECURITY (OPSEC) 8 June 2011, is supplemented as follows.** This supplement institutionalizes and standardizes organizational structure within the command. It clarifies and provides needed detail not incorporated in the AFI. This publication applies to all ACC Component-Numbered Air Forces (C-NAFs), Direct Reporting Units (DRUs), Field Operating Agencies (FOAs) and wings. This publication applies to Air National Guard of the United States when gained by ACC. Units' supplemental guidance to this ACC publication will not lessen the requirements nor change the basic content of this document. Units will submit implementing or supplementing publications to the MAJCOM OPR (ACC/A3IF for ACC units) for review and coordination before publishing. Maintain records created as a result of prescribed processes in accordance with (IAW) Air Force Manual 33-363, *Management of Records*, and dispose of them IAW the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afrims/afrims/afrims/rims.cfm>. Contact supporting records managers as required. 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*; through the appropriate functional chain of command to HQ ACC/A3IF 205 Dodd Boulevard, Suite 101 Joint Base Langley-Eustis (JBLE) VA 23665-2789.

### **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.

**(ACC)** This document is substantially revised and must be completely reviewed. Major changes include: clarification of OPSEC program requirements for all echelons of ACC units with the basic tenant being that all ACC units/personnel, at all levels of command, must plan and implement the OPSEC process. It specifies host-tenant relationships and MOA requirements for

specifying details of their working relationships and mutual OPSEC supporting activities. Commander, Program Manager (PM, Signature Management Officer's, and Coordinators responsibilities are defined/clarified to ensure effective OPSEC program implementation, management, and execution. OPSEC products are required to ensure the full process is executed. Following the addition of Signature Management (SM) in the AFI 10-701 this supplement integrates SM guidance and provides SM templates for standardization across the command. For this document all references to C-NAF include all the components under the commander. A C-NAF typically consists of an Air Force Forces (AFFOR) staff (command element, A1- A9, and Personal Staff), an AOC and all other forces assigned or attached to the Component Commander. It may also have an assigned support group / squadron with streamlined overhead to provide organizational control over required support units.

|   |           |
|---|-----------|
| <b>Chapter 1—GENERAL</b>  | <b>6</b>  |
| 1.1. Introduction: .....  | 6         |
| 1.2. Operational Context: .....   | 6         |
| Figure 1.1. OPSEC Functional Structure .....  | 6         |
| 1.3. Purpose: .....   | 7         |
| 1.4. Roles and Responsibilities: .....  | 7         |
| <b>Chapter 2—SIGNATURE MANAGEMENT</b>   | <b>24</b> |
| 2.1. Signature Management. ....   | 24        |
| 2.2. Wing or installation commanders will: .....  | 25        |
| 2.2. (ACC) Wing or installation commanders will: .....  | 25        |
| 2.3. Signature Management Officer/Signature Management Non-Commissioned Officer will: .....       | 27        |
| 2.3. (ACC) Signature Management Officer/Signature Management Non-Commissioned Officer will: ..... | 27        |
| Table 2.1. (Added-ACC) Standard ACC Wing Activities for Base Profiling. ....                      | 28        |
| 2.4. Signature Management Planning and Coordination. ....   | 31        |
| 2.5. Exploitation Countermeasures (Refer to AFI 10-704, Paragraph 2. ....                         | 33        |
| <b>Chapter 3—OPSEC PLANNING</b>   | <b>34</b> |
| 3.1. General. ....  | 34        |
| 3.2. Operational Planning. ....   | 34        |
| 3.3. Support Planning. ....   | 34        |
| 3.3. (ACC) Support Planning. ....   | 35        |
| 3.4. Exercise Planning. ....  | 35        |
| 3.5. Acquisition Planning. ....   | 35        |

**Chapter 4—OPSEC PROCESS 36**

4.1. General: ..... 36

4.2. Identify Critical Information: ..... 36

4.3. Analyze Threats: ..... 36

4.4. Analyze Vulnerabilities: ..... 36

4.5. Assess Risk: ..... 37

4.6. Apply Countermeasures: ..... 37

4.7. (Added-ACC) Required OPSEC products. .... 38

4.8. (Added-ACC) ..... 38

**Chapter 5—OPSEC EDUCATION AND TRAINING 39**

5.1. General. .... 39

5.1. (ACC) General. .... 39

5.2. All Personnel: ..... 39

5.3. OPSEC PMs/SMO/SMNCOs/Coordinators, Planners, Inspection Teams: ..... 40

5.4. Joint and Interagency OSPEC Support: ..... 41

**Chapter 6—ASSESSMENTS 43**

6.1. General: ..... 43

6.2. Annual OPSEC Program Review: ..... 44

6.3. Staff Assistance Visit (SAV): ..... 45

6.4. Survey: ..... 46

6.5. Web Content Vulnerability Analysis: ..... 46

6.6. Support Capabilities: ..... 47

Table 6.1. OPSEC Assessment Types and Support Capabilities ..... 48

**Chapter 7—AIR FORCE OPSEC ANNUAL AWARDS PROGRAM 50**

7.1. General: ..... 50

**Chapter 8—OPSEC REQUIREMENTS WITHIN CONTRACTS 51**

8.1. General: ..... 51

8.1. (ACC) General: ..... 51

8.2. Guidance and procedures: ..... 51

**Chapter 9—(Added-ACC) INFORMATION COLLECTIONS, RECORDS, AND FORMS 53**

9.1. (Added-ACC) Information Collections. .... 53

9.2. (Added-ACC) Records. .... 53

|  |           |
|--|-----------|
| <b>AFI10-701_ACCSUP_I 17 SEPTEMBER 2012</b>  | <b>5</b>  |
| <b>Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>  | <b>54</b> |
| <b>Attachment 1—(ACC) GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>  | <b>61</b> |
| <b>Attachment 2—(Added-ACC) OPSEC PROGRAM MANAGER FOR ACC C-NAF AND DRUS APPOINTMENT LETTER TEMPLATE</b>                           | <b>65</b> |
| <b>Attachment 3—(Added-ACC) OPSEC PLAN FORMAT</b>  | <b>66</b> |
| <b>Attachment 4—(Added-ACC) SIGNATURE MANAGEMENT APPOINTMENT LETTER TEMPLATE</b>   | <b>68</b> |
| <b>Attachment 5—(Added-ACC) OPSEC COORDINATOR/SMWG MEMBER APPOINTMENT LETTER TEMPLATE FOR BELOW WING LEVEL AND HQ DIRECTORATES</b> | <b>70</b> |
| <b>Attachment 6—(Added-ACC) SAMPLE WAIVER MEMO</b>   | <b>71</b> |
| <b>Attachment 7—(Added-ACC) STANDARDIZED ACC UNIT SM/OPSEC CONTINUITY BOOK</b>   | <b>72</b> |
| <b>Attachment 8—(Added-ACC) HOST TENANT RELATIONSHIPS FOR ACC UNITS</b>  | <b>76</b> |
| <b>Attachment 9—(Added-ACC) SMWG MASTER ROSTER</b>   | <b>78</b> |
| <b>Attachment 10—(Added-ACC) EXERCISE PROPOSAL FORMAT</b>  | <b>80</b> |
| <b>Attachment 11—(Added-ACC) SIGNATURE MANAGEMENT EXECUTION CHECKLIST</b>  | <b>82</b> |
| <b>Attachment 12—(Added-ACC) SIGNATURE MANAGEMENT EVENT LOG</b>  | <b>83</b> |
| <b>Attachment 13—(Added-ACC) SELF-INSPECTION REPORT</b>  | <b>84</b> |

## Chapter 1

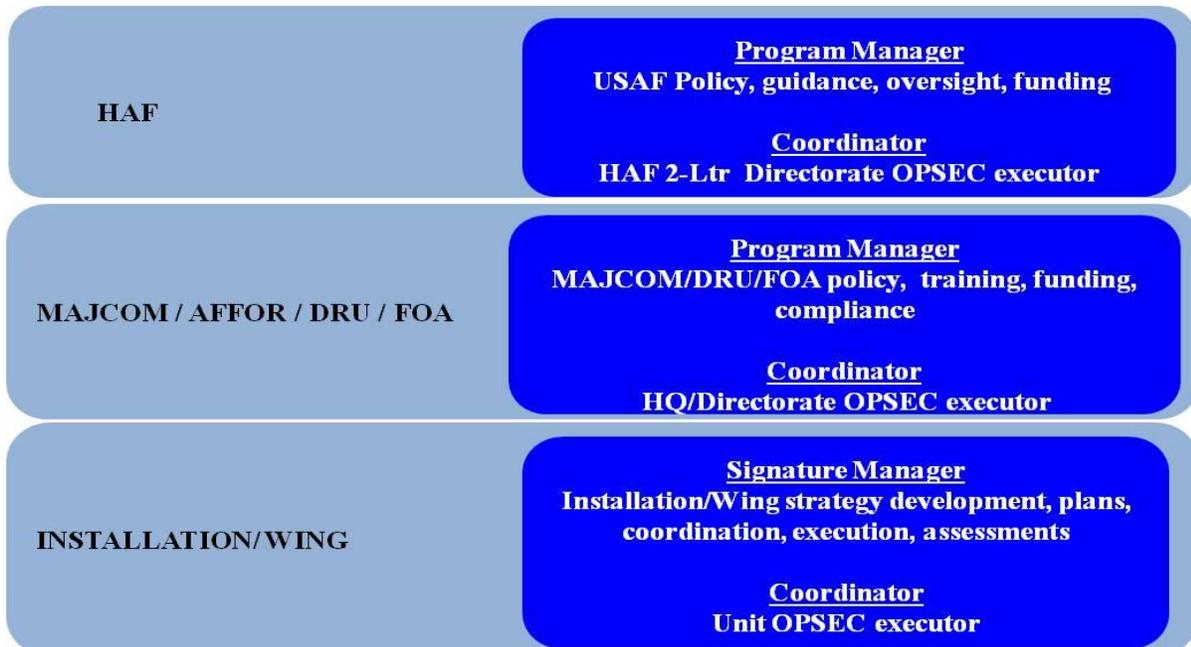
### GENERAL

**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. **(ACC) Air Force MAJCOMs, FOAs, and DRUs will:** As written in AFI 10-701 this paragraph applies only to FOAs and DRUs to Headquarters Air Force (HQ AF). This supplement adds the Air Force MAJCOMS, FOAs, and DRUs requirements from AFI 10-701, paragraph **1.4.8.1** through **1.4.8.21** to ACC assigned FOAs and DRUs such as the USAF Warfare Center (USAFWC), and C-NAF (HQ 1AF/ 601 AOC/AFFOR, HQ 9AF/609 AOC/AFFOR, HQ 12 AF/612 AOC/AFFOR.) Additions to the AFI requirements are included below.

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.

1.4.8.1. **(ACC)** Each ACC C-NAF, DRU, and FOA will implement and maintain their own OPSEC program IAW AFI 10-701 and guidance from ACC/A3IF. Commanders with multiple “hats” may appoint a primary and alternate PM that covers multiple organizations if the mission allows. For example, while in garrison 12AF, 612 AOC/AFFOR can have a single program as long as the commander states so in the appointment letter. If deployed, the organization needs to maintain OPSEC programs at both the deployed and in-garrison location. (see **Attachment 2: OPSEC Program Manager for ACC C-NAF and DRUs Appointment Letter Template**)

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

1.4.8.2. **(ACC)** In addition to establishing and managing their OPSEC program, all ACC tenant units, to include DRUs, FOAs and C-NAFs, will participate in their host installation’s OPSEC program. Tenant units need to be aware and protect host and other tenant unit’s OPSEC information they encounter and integrate countermeasures as required. Each ACC DRU, FOA and C-NAF will submit administrative reports (i.e., annual reports, incident reports, etc.) directly to HQ ACC/A3I.

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.

1.4.8.3. **(ACC)** ACC/A3I, Information Operations Division, is the OPR for implementing the AF OPSEC program within the command and the ACC OPSEC PM is assigned to A3IF, Influence Operations Branch. ACC units will address all formal correspondence concerning OPSEC issues to [acc.a3if@langley.af.mil](mailto:acc.a3if@langley.af.mil) or [acc.a3if@langley.af.smil.mil](mailto:acc.a3if@langley.af.smil.mil).

1.4.8.3.1. **(Added-ACC)** ACC DRUs (USAFWC), and C-NAFs, are encouraged but not required to appoint a full time OPSEC PM and therefore a part time OPSEC PM waiver is not required.

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*).

1.4.8.6. (ACC) HQ ACC/A3I will consolidate and submit OPSEC requirements from all ACC organizations using skip echelon process IAW the AF capabilities based planning process. ACC C-NAF, DRUs, FOAs, and wings will submit requirements to ACC/A3I. ACC/A3I will accept these inputs at anytime but will send a formal call for data whenever tasking directs.

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) 90 or 234. All individuals performing OPSEC duties will be awarded SEI 90 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.

1.4.8.17. (ACC) HQ ACC staff, USAFWC and other MAJCOM DRU/FOAs (if added) will forward identified non-ACC public and private web OPSEC vulnerabilities to ACC/A3IF who will send to HQ AF/A3CI for resolution via Unclassified but Sensitive Internet Protocol (IP) Router Network (NIPRNET) NIPRNET or Secret Internet Protocol router Network (SIPRNET) if required).

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).

1.4.8.19. **(ACC)** Forward C-NAF annual program review report to include all reports from one level down for the fiscal year period of 1 Oct – 30 Sep to the ACC OPSEC PM (ACC/A3IF) not later than (NLT) 15 November each year (See [Paragraph 6.2.1](#))

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.

1.4.8.22. **(Added-ACC)** HQ ACC/A3I staff will develop ACC Inspector General (IG) compliance and readiness checklists to ensure assigned units plan and execute OPSEC as directed.

1.4.8.23. **(Added-ACC)** In addition to the other requirements ACC C-NAFs and USAFWC are responsible for:

1.4.8.23.1. **(Added-ACC)** Protecting their own critical information through an OPSEC program.

1.4.8.23.2. **(Added-ACC)** Soliciting and selecting OPSEC award nominations from subordinate wings/C-NAF organizations. C-NAF/USAFWC selectee packages will be forwarded to ACC per this supplement [paragraph 7.1.2](#)

1.4.8.23.3. **(Added-ACC)** Submitting an annual OPSEC activity report to HQ ACC/A3I NLT 1 Oct for fiscal year (FY) (i.e., 1 Oct – 30 Sep) activities. C-NAFs with direct oversight of a subordinate unit, such as a RED HORSE unit, will consolidate and include the subordinate unit's data within their annual report. See paragraph 1.4.16.3.12 for wing and wing-equivalent organization annual reporting requirements. C-NAFs and DRUs are not responsible for consolidating and forwarding annual reports from wings as the wings will submit annual reports directly to ACC.

#### 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. (ACC) Commanders and Directors will:** To clarify, this section applies to all ACC C-NAF, DRU, FOA, wings, GSU groups and HQ directors. In addition, wing commanders will follow the guidance found in paragraph 2.2. All commands in ACC will

have an OPSEC program. OPSEC PMs at the C-NAF level have responsibilities to include OPSEC considerations in operational planning, to provide policy and guidance for subordinate organizations (e.g. assigned Air Expeditionary Wings), and to implement the OPSEC process to protect critical information across the staff. For installations with multiple units, all wing and above commanders, and geographically separated Group commanders will have their own OPSEC program that is tailored to their mission in addition to participating in the installation OPSEC process led by the host unit. This is especially important for those units that deploy separately from the host unit.

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. (ACC) Commanders will appoint OPSEC PMs to serve a minimum of two years to ensure the health of the OPSEC program and to maximize training investments. Waivers will not be granted lightly. Unit commander endorsed waiver requests will be submitted to ACC/A3I for consideration. (see **Attachment 6 Sample Waiver Memo**). Approved waivers will be retained on file with HQ ACC/A3I. Unit OPSEC PM will file a copy of the approved waiver in their OPSEC continuity book (See Attachment 7). For OPSEC PMs required to attend the AF Signature Management (SM) Course, the unit may be required to fund training for newly appointed PMs when the previous OPSEC PM departs or is re-assigned to other duties prior to the minimum two-year requirement. Appointment letters will clearly state to which organization(s) the PM is appointed. (See **Attachment 4: Signature Management Officer Appointment Letter Template; Attachment 2: OPSEC Program Manager for ACC C-NAF and DRUs Appointment Letter Template**); and **Attachment 5: OPSEC Coordinator Appointment Letter Template for below wing level and HQ directorates.**) For example, the commander can appoint a PM for 9AF HQ, AFCENT and AFFOR/AOC but if it is not specified on the appointment letter additional PMs need to be assigned to ensure all parts of the organization are under an OPSEC program.

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).

1.4.15.2.1. (ACC) Deviation from meeting the minimum rank requirements requires HQ ACC/A3I waiver.

1.4.15.2.1.1. (Added-ACC) Units commanders/Directors will appoint an

additional alternate OPSEC PM to ensure effective OPSEC program oversight and continuity when the appointed primary or alternate is deployed/TDY for more than sixty continuous days. Unit commanders may appoint more than one alternate OPSEC PM when unit size and/or mission dictates; however these additional individuals must materially contribute to the program's administration. Appointment letters will document additional OPSEC PM alternates. Note: HAF funds may not be available for training more than two OPSEC PMs per unit and would require unit funding any additional personnel to attend required SM training course.

1.4.15.2.1.2. **(Added-ACC)** Ensure continuity of operations by identifying, in writing, the replacement OPSEC PM NLT one month prior to the incumbent's departure from the position. Forward new appointment letter(s) to HQ ACC/A3I NLT ten days of the commander signing the appointment letter and before incumbent's departure (See **Attachment 2 OPSEC Program Manager for ACC C-NAF and DRUs Appointment Letter Template**). OPSEC PM appointment letter(s), and two-year waiver request, if required, may be submitted electronically via e-mail.

1.4.15.2.1.3. **(Added-ACC)** For installations with multiple wings, all ACC wings (whether in a host or tenant unit capacity) will have a primary OPSEC PMs (known as SMOs in ACC) assigned. The OPSEC PM/SMO will be an O-3 or above, civilian equivalent, or an E-7.

1.4.15.2.1.4. **(Added-ACC)** For ACC's group-level GSU's, the OPSEC position will be titled as a SMO and will be in the rank of O-3 or above and perform SMO equivalent role and responsibilities. All wing-level and SMO requirements defined in AFI 10-701 and this supplement apply to these units. Any deviations, to include failure to meet minimum rank requirements, require HQ ACC/A3I waiver.

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

1.4.15.2.2.1. **(Added-ACC)** Appoint OPSEC Coordinators at each HQ ACC/C-NAF/USAFWC Directorate and ACC group and/or squadron. Unit commanders/HQ directorate chiefs (upon advice from the PM/SMOs) may require Coordinators below group/HQ directorate level based on mission requirements. For example, an Operations group commander with three squadrons of the same weapon system may decide that a group-level Coordinator may be sufficient to effectively manage OPSEC requirements. However, an Operations Group with three disparate weapon systems may require OPSEC Coordinators at each of the squadrons and not at the group or at both.

1.4.15.2.2.2. **(Added-ACC)** ACC primary and alternate OPSEC Coordinators will have a minimum rank of NCO. Unit commanders may appoint more than one OPSEC Coordinator via the appointment letter; however these additional individuals must materially contribute to the program's administration. To ensure unit OPSEC program continuity, unit commanders will forward above wing OPSEC Coordinator appointment letter to the OPSEC PM and below wing

Coordinator appointment letters to the wing SMO NLT one month prior to the incumbent departure from the position. (See **Attachment 5 OPSEC COORDINATOR/SMWG MEMBER APPOINTMENT LETTER TEMPLATE FOR BELOW WING LEVEL AND HQ DIRECTORATES.**)

1.4.15.3. Submit request through servicing MPF for award of SEI 90 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.

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

1.4.15.5. (ACC) 3 . (Added) Strive to keep unit CIL(s) “UNCLASSIFIED” and **not** “FOR OFFICIAL USE ONLY.” CIL(s) are to assist with reminding personnel to protect related critical information. If some critical information is considered FOUO include that information in an FOUO OPSEC plan with associated countermeasures but do not include on the publically distributed list.

1.4.15.5.1. (Added-ACC) ACC organizations will identify critical information, publish a CIL, and identify/implement countermeasures to protect critical information and indicators for each operation, activity, and exercise whether it be planned, conducted or supported. Organizations will assign a critical information value based on the *Critical Information Value Matrix* (See AFTTP 3.1 *Information Operations*, OPSEC Chapter.)

1.4.15.5.2. (Added-ACC) Wing and above organizations forward the most current (no more than one year old) CIL and countermeasures to the MAJCOM OPSEC PM. CILs and countermeasures will be reviewed annually using the process described in AFI 10-701 chapter 4, updated as necessary, and signed by the commander annually or upon significant change in the unit’s mission, threat, or vulnerabilities.

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.

1.4.15.10. (ACC) OPSEC working groups are an essential part of the OPSEC process. Commanders will ensure OPSEC PMs will formally form and maintain an OPSEC working group (OWG) to ensure individuals are identified, trained, periodically exercised and prepared to respond to a short notice OPSEC planning requirements and/or tasking. OWGs will reside at organizations above wing level and chaired by the appointed OPSEC PM. (See this supplement, paragraph 2.3.12, for wing level SM working group 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.

1.4.15.13. (Added-ACC) Forward DRUs', C-NAFs' and wings' annual program review reports for the fiscal year period of 1 Oct – 30 Sep to ACC/A3I NLT 1 Oct each year.

**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. (ACC) OPSEC PMs, Coordinators and Planners: Wing and Installation SMOs will follow the guidance in this section in addition to the requirements in Paragraph 2.3 of the AFI and this Supplement.

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.

1.4.16.1. (ACC) USAF WC and all ACC DRUs, FOAs and C-NAFs will appoint, in writing, a primary and alternate OPSEC PM. Appointment letters will be forwarded to HQ ACC/A3I IAW Attach 2 of this supplement. If the OPSEC PM also serves as an OPSEC planner, this will be stated on the appointment letter. However, if OPSEC planners are not also appointed as an OPSEC PM, then the commander will appoint the planner(s) separately. Forward OPSEC PM and planner(s) appointment letter(s), signed by the commander, to HQ ACC/A3I within ten days of appointment. (See Chapter 2 of AFI 10-701 and this supplement for wing level requirements of SMO/SMNCOs.)

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.

1.4.16.2. (ACC) OPSEC Coordinators will be appointed at each HQ ACC/C-NAF/USAFWC Directorate. OPSEC Coordinators and/or SMWG members will be appointed at ACC group and/or squadron (including ACC units embedded with other services, such as Air Support Operations Squadrons (ASOS)). Local commanders/Directorate Chiefs (upon advice from the PM/SMOs) may require Coordinators below group/directorate level based on mission requirements. For example, in an Ops group that has three squadrons of the same weapon system the SMO may decide that a group Coordinator may be sufficient. In an Ops Group with three disparate weapon systems the SMO may decide to have Coordinators at each of the squadrons and not at the group or at both. OPSEC Coordinators at HQ ACC/C-NAF/USAFWC Directorates will forward a dated, scanned or faxed copy of the signed appointment letter to their headquarters OPSEC PM within ten working days of appointment. OPSEC Coordinators/SMWG members below wing level will forward a dated, scanned or faxed copy of the signed appointment to the Wing SMO within ten working days of appointment. (See attachment 5).

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.

1.4.16.3.1. (ACC) If C-NAFs have OPSEC planners that are not appointed as OPSEC PMs they must have a security clearance at the same level as the plans created by that unit (minimum Secret). If the organization creates plans at the Top Secret level then the OPSEC planner must have a Top Secret clearance to integrate OPSEC into the plan at inception.

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.

1.4.16.3.2. (ACC) Forward updated operating instructions (OIs), guidance, and countermeasures to HQ ACC/A3I.

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.

1.4.16.3.3. (ACC) Installations that have multiple organizations assigned will establish a Memorandum of Agreement (MOA), signed by the host and each tenant commander, that specifies host/tenant roles and responsibilities. ACC host wings will lead an installation SM (OPSEC/MILDEC) effort; however each ACC wing/wing-equivalent and group-level GSU's will establish and administer their own tailored SM program. For ACC tenant units and group-level GSU's on a non-ACC installation,

the ACC SMO/OPSEC PM will seek out and provide the host SMO with their appointment letter, CIL and countermeasures. ACC SMOs will comply with ACC supplemental guidance, implement and administer their unit's programs IAW ACC procedures and administratively report to HQ ACC/A3I for all OPSEC and/or MILDEC issues and requirements. ACC units embedded within other service units (such as ASOS units) will act as Coordinators to both their host unit and their own administrative ACC group and/or wing.

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

1.4.16.3.4.1. **(Added-ACC)** Assist planning officers to identify critical information; assess threats, vulnerabilities/indicators, and risk; and develop cost effective, actionable countermeasures for inclusion in plans. OPSEC PMs and SMOs will provide training to local organizational planners. These products will be made available for inspections.

1.4.16.3.4.2. **(Added-ACC)** Assist exercise planners to develop event injects in the master scenario events list for wing level exercises to ensure they properly trigger the OPSEC planning process and the execution of OPSEC measures. Also assist in developing adequate measures of effectiveness (MOEs) and measures of performance (MOPs) to evaluate the selection of and execution of directed OPSEC measures. Assist planners and intelligence in developing and inputting Requests for Intelligence (RFIs) for measures. MOPs, MOEs, and RFIs will be made available for inspections.

1.4.16.3.4.3. **(Added-ACC)** Review plans annually and update as needed. Consider changes in the threat, vulnerability, impact to the plan, and assessments of the countermeasures MOEs and MOPs.

1.4.16.3.4.4. **(Added-ACC)** As soon as the unit is notified of an operational deployment or overseas exercise contact the gaining command for their OPSEC requirements. The deploying unit(s) will provide their CIL to the gaining OPSEC PM. Additionally, the SMO at the deploying unit will:

1.4.16.3.4.4.1. **(Added-ACC)** Obtain and disseminate the operation/exercise CIL and countermeasures.

1.4.16.3.4.4.2. **(Added-ACC)** Brief deploying unit personnel on OPSEC considerations and implement any necessary countermeasures to protect and preclude compromise of critical information.

1.4.16.3.4.4.3. **(Added-ACC)** Document these actions and be prepared to provide documentation to the ACC/IG upon request.

1.4.16.3.4.5. **(Added-ACC)** OPSEC exercises will be conducted twice a year at units above wing level. (Wing level refer to this supplement, paragraph 2.3.10.1).

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.

1.4.16.3.5.1. **(Added-ACC)** Documents required to be reviewed include

(minimum): unit OPSEC plan, unit CIL, unit countermeasures, adversary list, SM Master Checklist, and appointment letters.

1.4.16.3.5.2. **(Added-ACC)** Forward updated OIs, guidance, CILs, countermeasures, and supplements to AFI 10-701 ACC Supplement to HQ ACC/A3I.

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.

1.4.16.3.8.2. **(ACC)** Provide Public Affairs (PA) with a copy of all locally developed CILs (host, tenants, wings, groups, squadrons, MAJCOM, C-NAF, directorates, and divisions as appropriate) and assist, upon request, in executing the OPSEC process to determine the probability of mission impact of published or disseminated information on unit operations. GSU groups will provide the CIL to both the installation PA and your wing's home base PA.

1.4.16.3.8.3. **(Added-ACC)** Review all new/revised ACC instructions, briefings, safety magazines, flyers, web pages, interviews, and information for news articles authored by their directorate. SMOs/Coordinators will document the review using an appropriate method, for example, AF Form 673, *Air Force Publication/Form Action Request*, Staff Summary Sheet or ACC Form 22, *Public Affairs Security and Policy Review Worksheet*. All HQ ACC Directorate OPSEC Coordinators will track all reviewed documents by date of review. Review metrics will be included in the directorates' *Annual OPSEC Program Report*.

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.

1.4.16.3.9.3. **(Added-ACC)** Assist trainers to ensure standardized, mission specific OPSEC information (local threats and threats at unit's deploying location, unit CILs, vulnerabilities, and countermeasures) is included in training materials.

1.4.16.3.9.4. **(Added-ACC)** Assist the unit deployment managers to add OPSEC awareness training as a mandatory requirement for deploying personnel consisting of awareness of threats at origin, en-route, and destination; and personal responsibilities to protect associated mission critical information and indicators. (AFI 10-701 1.4.15.11)

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.

1.4.16.3.11. **(ACC)** Each ACC DRU, C-NAF and wing will submit an Annual OPSEC Program Review Report to HQ ACC/A3I, via OSCAR (See paragraph 6.2.1) NLT 1 Oct each year. Review reports will include self inspection/assessment results. Wings will consolidate subordinate unit reports, to include GSUs, into the wing Annual OPSEC Program Report. ACC will not issue a separate tasker as this supplement serves as the official tasking. If OSCAR is not available then submit via email with text based PDF (able to copy text) NLT 1 Oct. ACC OPSEC PM may request additional information be included in the report if needed.

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.

1.4.16.3.14. **(Added-ACC)** Program OPSEC funds through established DRU's, C-NAF's, wing's, or unit's budgeting and requirements process. Funds can be used for OPSEC awareness and education training promotional campaign incentives; budget, acquire, and distribute OPSEC educational materials.

1.4.16.3.15. **(Added-ACC)** All OPSEC PMs, SMOs and OPSEC Coordinators must maintain an OPSEC Continuity Book. Electronic format continuity book/items are sufficient as long as they are readily accessible upon demand. (See **Attachment 7 STANDARDIZED ACC UNIT SM/OPSEC CONTINUITY BOOK.**)

1.4.16.3.16. **(Added-ACC)** Modify OPSEC plans as applicable whenever any mission changes occur or current events dictate adjusting your procedures. Once an OPSEC plan has been approved, an annual review for currency is required by 1 Oct. Submit updated OPSEC plans to ACC/A3I annually by 1 Oct and within 90 days of any updates/changes. See **Attachment 3 OPSEC Plan** for categories that need to be addressed in the OPSEC plan.

1.4.16.3.17. **(Added-ACC)** Ensure OPSEC Risk Assessment, Threat Analysis, Vulnerability Analysis Assessment, and OPSEC Risk Summary Worksheets (see AFTTP 3.1 IO, OPSEC Annex) are developed for each operation, activity, and exercise whether it be planned, conducted or supported. These documents will be kept on file for a minimum of two years (hard or soft copy).

1.4.16.3.18. **(Added-ACC)** Ensure OPSEC related briefings or presentations to be given outside the MAJCOM are coordinated through the Air Force OPSEC PM, AF/A3CI, prior to the presentation date. Send a courtesy copy to ACC/A3I concurrently with the HQ AF coordination.

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.
- 1.4.17.2.5. (ACC) Recommend a 100% shred and recycle policy for documents containing critical information. Examples include, but are not limited to: local/HHQ exercises, test schedules, training and equipment vulnerabilities and limitations, personnel availability and recall procedures, ACC funding, capabilities and long-term planning, and individual/unit travel itineraries and flight plans.
- 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.
- 1.4.18. (Added-ACC) Reports of lost/stolen unit critical information will be sent over SIPRNET or higher secure systems in standard memorandum format. OPSEC PMs/SMOs will up channel OPSEC related incident reports to the ACC/A3I. All OPSEC related incident reports will be sanitized to safeguard personnel involved. If the commander, PM, or SMO deems an OPSEC related incident report(s) requires HHQ notification or resolution, SMOs will forward OPSEC related incident report(s) to the next HHQ OPSEC PM NLT 15 days after the report is signed. OPSEC related incident report(s) will be received by ACC/A3I NLT 30 days after report is signed. Example of OPSEC related incident reports can range from lost/stolen laptop(s) containing critical information to lost/stolen report(s) that contain critical information.
- 1.4.19. (Added-ACC) Local AFOSI will provide local threat information needed for the requesting unit's OPSEC process.

## 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. (ACC) ACC GSU groups are designated as wing equivalents and will maintain their own OPSEC and MILDEC programs under a Signature Management Office unless waived by HQ ACC/A3I. The waiver request should come from the Group commander through his administrative Wing commander, to ACC/A3I stating rationale for not having the programs. ACC GSUs will do SM for their own unit and integrate with host unit by participating in the host's SMWG.

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. (ACC) The SMO will have direct unrestricted access to the wing/installation commander to ensure immediate relay of any actual real-world taskings, potential/actual OPSEC compromise, or critical issues. This arrangement will be communicated to the SMOs chain of command and Commander's staff to streamline the execution of

MAJCOM/Combatant Commander exercise and operational tasking. The commander will consider this requirement when appointing the SMO.

2.1.3. **(Added-ACC)** The installation SMO will provide all new unit commanders a SM orientation briefing within 30 days of assuming commander duties. This orientation briefing will outline the installation SM program, to include SMWG membership, training and exercise requirements, base profiling process (BPP) requirements and status, and commander support responsibilities to ensure sustained SM program continuity and effectiveness. The SMO will document completion of unit commander SM orientation training in the SM Continuity Book and retain documentation until the commander relinquishes command (see continuity book I 3 a.)

## **2.2. Wing or installation commanders will:**

**2.2. (ACC)Wing or installation commanders will:** ACC wing commanders will implement SM operations within 60 days of this supplement effective date. ACC GSUs will implement and conduct SM operations tailored to their unit size, mission and responsibilities and participate in the host installation SMWG. The SMO/SMNCO will assume duties historically assigned to the wing OPSEC PM and Military Deception Officer, as defined in AFI 10-704, *Military Deception Program*, and ACC supplement guidance. Wing Commanders will follow the guidance in this section in addition to the requirements in Chapter 1.4.15. of the AFI and this Supplement.

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. **(ACC) Wing and installation commanders will:** Wing commanders will appoint a SMO/SMNCO to serve a minimum of two years to ensure OPSEC program continuity, long-term stability, and maximize training investment. Wing commander's will not permit the SMO or SMNCO position to go vacant for more than one month and will identify/appoint a replacement NLT one month prior to the incumbent's departure/relinquishing of duties. Wing commanders will notify HQ ACC/A3I when the SMO/SMNCO billet remains vacant for more than one month and provide a get well date. Wing commander requests for waivers (See **Attachment 6 Sample Waiver Memo**) to the two year requirement will receive serious HQ ACC/A3I. Deviation from meeting minimum rank criteria requires HQ ACC/A3I waiver. All approved waivers will be retained at HQ ACC/A3I and a copy filed in the SMO Continuity Book **Note:** For the purpose of this Supplement an installation is an AF base that is geographical entity. For bases that have been grouped together such as in Joint Base Langley-Eustis, there will be an installation SMO for each base-one at Langley and one for Eustis. Another example is Nellis-Creech where there should be an installation SMO for each base.

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. (ACC) At installations with multiple wings/wing-equivalent organizations assigned, all ACC wings/wing-equivalent organizations (whether host or tenant status) will appoint a primary SMO. This individual will be in the grade of O-3 or above, civilian equivalent, or E-7. Deviation from these requirements must be approved by HQ ACC/A3I.

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. (ACC) Although there are some installations with only one wing the majority of installations now have more than one unit. Therefore installation does not mean wing. Installations that have multiple organizations shall have a MOA, signed by the host and all tenant commanders, that specifies host/tenant roles and responsibilities. Each wing is responsible for establishing and maintaining its own OPSEC and MILDEC programs under the SM office tailored to its missions, activities, threats, and vulnerabilities. Each wing commander/GSU group commander is responsible for using the base profiling process to assist in risk analysis based on that unit's mission. These may be different if one unit deploys while others remain in garrison. All hosts and tenants need to work together to share CILs, Countermeasures, Threat Analysis to help protect all the critical information on the base regardless of ownership. ACC host wings will lead an installation SM/OPSEC/MILDEC program and each organization will have their own tailored program see [Attachment 8 Host Tenant Relationships for ACC Units](#). If the ACC wing is a tenant to a non-ACC host, the ACC SMO will seek out the host OPSEC SMO and provide to the host the unit's appointment letter, CIL, and countermeasures. ACC wing SMOs will report to ACC OPSEC and MILDEC PMs. Installation SM/OPSEC MOAs will be reviewed biannually or within 30 days of a change of any one of the signatories. All wing SMOs, whether installation host or tenant will identify the processes that their wing uses per section 2.3. The differences between an installation SMO and a tenant wing SMO will be delineated with these processes that will be approved by ACC/A3I and then codified in the installation MOA.

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.

2.2.1.1.3. (Added-ACC) Wing commanders will appoint an additional alternate SMO to ensure effective OPSEC program oversight and continuity when the appointed primary or alternate is deployed/TDY for more than sixty continuous days. Unit commanders may appoint more than one alternate SMO when unit size and/or mission dictate; however these additional individuals must materially contribute to

the program's administration. Appointment letters will document additional SMO alternates. **Note:** HAF funds may not be available for training more than two SMOs per unit and would require unit funding any additional personnel to attend required SM training course.

2.2.1.1.4. **(Added-ACC)** Ensure continuity of operations by identifying, in writing, the replacement SMO NLT one month prior to the incumbent's departure from the position. Forward new appointment letter(s) to HQ ACC/A3I NLT ten days of the commander signing the appointment letter and before incumbent's departure (See **Attachment 4: SIGNATURE MANAGEMENT APPOINTMENT LETTER TEMPLATE**. SMO appointment letter(s), and two-year waiver request, if required, may be submitted electronically via e-mail.

2.2.2. Submit request through servicing MPF for award of special experience (SEI) 90 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.

2.2.2. **(ACC)** Commander's will comply with AFI 10-701 requirement to request Special Experience Identifiers (SEIs) be awarded to qualified individuals by contacting the servicing personnel office. SEI award criteria can be found in the AF Officer Classification Directory (AFOCD) and the AF Enlisted Classification Directory (AFECD) Part I and Part II located at [https://gum-crm.csd.disa.mil/app/answers/detail/a\\_id/7504/p/8%2C10/c/549](https://gum-crm.csd.disa.mil/app/answers/detail/a_id/7504/p/8%2C10/c/549).

2.2.3. **(Added-ACC)** Wing Commander's will issue and enforce organization OPSEC policy, guidance and instructions.

2.2.4. **(Added-ACC)** The SMWG is a vital element in the OPSEC process. Wing and group-level GSU commanders will ensure the SMO formally establishes and maintains a SMWG and that SMWG members are identified, trained, periodically exercised and prepared to respond to short-notice SM planning requirements and taskings. SMWGs will be established at the wing and installation level and chaired by the appointed SMO/SMNCO.

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

**2.3. (ACC)Signature Management Officer/Signature Management Non-Commissioned Officer will:** Wing level SMOs will accomplish all items in this section in addition to **paragraph 1.4.16** of the AFI and this supplement.

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.

2.3.2. **(ACC)** SMOs will ensure wing policy and guidance is reviewed biannually or more often as required by changing threats, missions, and/or vulnerabilities.

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.

2.3.3.1. **(Added-ACC)** ACC units will develop a signature management master checklists that includes all activities/processes conducted by the installation/wing. **Table 2.1 Standard Wing Activities for Base Profiling** lists the minimum activities/processes that most installations/wings engage in and will be used by the SMO. If a particular installation/wing does not conduct one of the "standard" activities/processes the SMO will request a waiver from the MAJCOM PM stating the reason the unit does not do that activity. The wing and installation SMO will conduct the BPP on all wing activities over and above the minimum stated in this list. If a SMO determines his wing does an activity(ies) not on this list the SMO will identify the activity(ies) to the MAJCOM PM .

2.3.3.2. **(Added-ACC)** SMOs will use the BPP developed checklists to improve OPSEC plans, execution, and assessment. The detailed study of the activities/processes is useful to help identify critical information, vulnerabilities, countermeasures and the MOEs/MOPs needed in the OPSEC process.

**Table 2.1. (Added-ACC) Standard ACC Wing Activities for Base Profiling.**

| <b>Mission Area</b>   | <b>Applicable<br/>(Y or N)</b> | <b>If No<br/>(Reason)</b> | <b>BPP<br/>begun<br/><br/>(Y or N)</b> | <b>BPP<br/>completed<br/><br/>(Y or N)</b> | <b>Date Last<br/>Reviewed</b> | <b>Reviewed<br/>By:</b> |
|---|--------------------------------|---------------------------|--|--|-------------------------------|-------------------------|
| Recall  |                                |                           |  |  |                               |                         |
| Mobility processing<br>(Personnel and<br>Equipment<br>deployment)     |                                |                           |  |  |                               |                         |
| Aircraft generation   |                                |                           |  |  |                               |                         |
| Airlift load generation<br>and marshalling                            |                                |                           |  |  |                               |                         |
| Munitions   |                                |                           |  |  |                               |                         |
| Airspace and ranges<br>(tower, RAPCON, and<br>FAA Centers) activities |                                |                           |  |  |                               |                         |
| Security (ALL)  |                                |                           |  |  |                               |                         |
| Aircraft<br>recovery/launch   |                                |                           |  |  |                               |                         |

2.3.4. Develop and maintain a current commander approved CIL.

2.3.4. (ACC) Strive to keep unit CIL(s) “UNCLASSIFIED” and **not** “FOR OFFICIAL USE ONLY.” CIL(s) are to assist with reminding personnel to protect related critical information. If some critical information is considered FOUO include that information in an FOUO OPSEC plan with associated countermeasures but do not include on the publically distributed list.

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. (ACC) Use the format found in Attachment 11 for the signature management execution checklist.

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).

2.3.7. 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.

2.3.8. 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.

2.3.9. (ACC) Approved waivers (see **Attachment 6 Sample Waiver Letter**) will be retained in the continuity book (see **Attachment 7 STANDARDIZED ACC UNIT SM/OPSEC CONTINUITY BOOK**) by the SMO.

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

2.3.10.1. (**Added-ACC**) All ACC wings and installations, whether a host or tenant unit, will accomplish four quarterly SM exercises each FY. All SMO-tasked units, whether host or tenant, will perform quarterly SM exercises. Of the four exercises, two may be conducted as table-top events and the other two are fully exercised events. SM exercises may be integrated into a host or tenant unit exercise provided specific aspects of the unit's operational indicators are examined and their SMWG is exercised. For all exercises, ACC SMOs will forward their exercise CONOPS, execution checklist and after-action/lessons learned to HQ ACC/A3I IAW AFI 10-704\_ACC SUP requirements. An operational log, capturing all exercise activities, will be accomplished for each exercise (See Attachment 13). This log will be used to assist in internal exercise "hot wash" assessments and to improve overall SM process and products (i.e., checklists, BBP products) Retain the each exercise events log in the SM Continuity Book. (See **Attachment 13 SIGNATURE MANAGEMENT EVENT LOG** for example.)

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.

2.3.11. (ACC) The wing commander and SMO will determine Exercise Evaluation Team involvement considering the event, activities, and close hold methods to be used.

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

2.3.12. (ACC) The SMO is responsible for establishing the SMWG, training SMWG members and coordinating SMWG activities. The SMO will maintain a master SMWG roster, identifying all members. The master roster may also identify which members are assigned SME responsibilities for certain base processes, as OPSEC only duties, or if the member is responsible for SM planning and/or executing exploitative techniques (See Attachment 9).

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.

2.3.14. (ACC) Submit reports via OSCAR to the appropriate MAJCOM PM NLT 1 Oct annually. If OSCAR is not available then submit via email. To facilitate HHQ reporting requirements, do not send reports as an imaged PDF file instead use Word's "Save as a PDF file" option as this will permit text extraction/consolidation and HHQ reporting. Wing commander signatures may be imaged or e-signature.

2.3.15. (Added-ACC) Upon appointment of a new SMO, the out-going SMO will accomplish an OPSEC and MILDEC program management handoff to their replacement. The handoff will include at a minimum a program status briefing and continuity book review.

2.3.16. (Added-ACC) As soon as the unit is notified of an operational deployment or overseas exercise, ensure the gaining command's OPSEC PM is contacted for its OPSEC requirements and the deploying unit can also pass their critical information list (CIL) to the gaining OPSEC PM. Additionally, the SMO at the deploying unit will:

2.3.16.1. (Added-ACC) Ensure their unit(s) obtain and disseminates the operation/exercise CIL and countermeasures.

2.3.16.2. (Added-ACC) Ensure unit deploying personnel are briefed on OPSEC considerations and implement any necessary countermeasures to protect and preclude compromise of critical information.

2.3.16.3. (Added-ACC) When units deploy, a SMO or trained OPSEC Coordinator should deploy with the unit to work with the receiving installation SMO and AF Component OPSEC and MILDEC PMs/planners. This collaboration should begin once the deploying unit is notified until it returns to home station to ensure OPSEC and MILDEC protective countermeasures are implemented pre-, during, and post deployment.

**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. (ACC) ACC units will forward the following documents to HQ ACC/A3IF for each SM exercise/operation:

2.4.1.1. (Added-ACC) Before execution - Exercise Proposal Format. Submit no later than 60 days prior to proposed exercise/operation execution start date. (See **Attachment 10 for Exercise Proposal Format**).

2.4.1.2. (Added-ACC) Before execution – ACC SM execution checklist. Submit within 30 days of exercise/operation execution. (See **Attachment 10 Exercise Proposal Format** and **Attachment 11: Signature Management Execution Checklist**.)

2.4.1.3. (Added-ACC) After execution – Submit SM Lessons Learned (L2) worksheet within 45 days after exercise/operation termination. Use the AFI 90-1601, *Special Management Air Force Lessons Learned Program*, Attachment 3, Observation or Lesson Learned Template.) **Note:** The AF Lessons Learned Program (AFL2P) exists to enhance readiness and improve combat capability by capitalizing on the experiences of Airmen. A L2 is an Observation that, when validated and resolved, results in an improvement in military operations or activities at the strategic, operational, or tactical level and results in long-term, internalized change to an individual or an organization. Coupling L2 with past experiences should also assist senior leaders in programming, budgeting and allocating resources as well as making changes to doctrine, organization, training, materiel, leadership & education, personnel, facilities and policy (DOTMLPF&P). An L2 finding is not a compliance “report card” nor is it automatically accepted and implemented without the scrutiny of functional experts. An L2 is also not “owned” by any one organization. Rather, the mandate for all organizations participating in the AFL2P is to coordinate activities and collaboratively exchange observations and lessons identified for the benefit of the total AF mission.

2.4.1.3.1. (Added-ACC) When accomplishing the L2 worksheet follow the four fundamental L2 components listed in AFI 90-1601, Figure 1.1: Collection, Validation, Dissemination and Resolution.

2.4.1.3.2. (Added-ACC) As the Office of Primary Responsibility (OPR) for SM issues the SMO/SMNCO will establish procedures for monitoring the status of Lessons identified and actions taken. The SM Office will ensure periodic updates are annotated in the SM Master Checklist and should observe corrective actions and be vigilant for similar repeat observations.

2.4.1.3.3. (Added-ACC) L2 Validation and Resolution: The SMO will review L2 observations for accuracy, applicability and completeness and that they are appropriately tracked to closure to ensure they become true L2 and not just forgotten or ignored.

2.4.1.3.4. (Added-ACC) Classify L2 worksheet if required by AF or joint security classification guides.

2.4.1.4. (Added-ACC) After execution – Submit SM After-Action Report (AAR) Worksheet within 45 days after exercise/operation termination. Use AFI 90-1601, *Special Management Air Force Lessons Learned Program*, Attachment 4, After Action Report Template. Submit a separate worksheet for each SM measure/event. Note: Whereas the SMO/SMNCO may have multiple L2 worksheets (one for each observation)

associated with a single SM measure/event the SMO/SMNCO will only have one AAR worksheet for the entire measure/event. AARs are intended to help SMOs/SMNCOs fight a smarter, more capable fight and to be shared with other SMOs/SMNCOs for appropriate cross tell. Timely submissions of AARs (and the individual Observations which comprise them) are the SMOs/SMNCOs responsibility and they are expected to submit a unit-level AAR for the event (deployment, contingency, exercise, etc.) for which they are responsible. Observations to be documented are those which result in improvements in military operations at the strategic, operational, or tactical level. AAR Observations should describe how the mission could be/was improved, potential risks to mission degradation and how to mitigate those risks. AARs are intended to be more than a summary or rollup of unit/tactical actions. Whenever possible, AARs should be submitted as soon as practical to permit timely action but NLT then 45 days after measure/event termination.

2.4.1.5. **(Added-ACC)** Classify AAR worksheet if required by AF or joint security classification guides.

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.

2.4.5. 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.

3.2.1. (ACC) OPSEC PMs at the component Headquarters will provide their OPSEC plan with CIL, threats, vulnerabilities, countermeasures, and points of contact to supporting organizations (e.g. wings that will deploy for overseas exercises and/or operational deployments). This action will occur as soon as the unit(s) is identified so that critical information can be protected before there are compromises. Component OPSEC planners are responsible for creating/updating the OPSEC Annex C, Appendix 3, Tab C (C-3-C) for each OPLAN or CONPLAN as prescribed in CJCSM 3122.03C, *Joint Operation Planning and Execution System Volume II Planning Formats and 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.

**3.3. (ACC) Support Planning. Note:** See AFI 10-404, *Base Support and Expeditionary Site Planning*, for In-garrison Expeditionary Support Plan requirements and format.

**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.

4.3.2. (ACC) Local AFOSI will provide local threat information. Local intelligence unit will provide mission related intelligence support. Threats can include foreign intelligence services, terrorist organizations (foreign and domestic), criminals, cyber, lone extremists (not all inclusive). Reports from cyber/communications, organizations will be used to assess the cyber threat and vulnerabilities.

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.

**4.7. (Added-ACC) Required OPSEC products.** ACC OPSEC PM/SMO/planners will use the OPSEC process as described in AFI 10-701 paragraphs 4.1-4.6 and will produce the following products:

4.7.1. **(Added-ACC)** The unit's operational CIL (proposed and final).

4.7.2. **(Added-ACC)** A Threat Analysis of your unit.

4.7.3. **(Added-ACC)** A list of your unit/installation's Vulnerabilities and Indicators.

4.7.4. **(Added-ACC)** A Risk Analysis of your unit's vulnerabilities (before and after proposed countermeasures are implemented)

4.7.5. **(Added-ACC)** A list of proposed Countermeasures, the costs of implementing those CMs, and those CMs that are chosen to implement.

4.7.6. **(Added-ACC)** MOE(s) and MOP(s) for each countermeasure

4.7.7. **(Added-ACC)** RFIs and other reports needed to assess the MOPs/MOEs.

4.7.8. **(Added-ACC)** Assessments of the countermeasures as determined from Intelligence and OSI reports, and periodic wing exercises.

**4.8. (Added-ACC)** In addition to the PM products listed in 4.7. the wing SMO will use the base profiling process to produce the following products:

4.8.1. **(Added-ACC)** A wing/installation SMWG/POC list

4.8.2. **(Added-ACC)** A list of major wing/installation activities/missions (see **paragraph 2.3.3.1.** and **Table 2.1 Standard ACC Wing Activities for Base Profiling**)

4.8.3. **(Added-ACC)** A detailed flow chart of each major wing/installation activity/mission

4.8.4. **(Added-ACC)** A signature management master checklist of all wing/installation activities/missions.

## 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.

**5.1. (ACC) General.** HQAF has clarified the requirement of 5.1. and 5.2.3. since publishing AFI 10-701. The OPSEC annual refresher awareness education requirement is satisfied by completing the Information Protection block of training within The Advanced Distributed Learning Service (ADLS) site [https://golearn2.csd.disa.mil/kc/login/login.asp?kc\\_ident=kc0001#](https://golearn2.csd.disa.mil/kc/login/login.asp?kc_ident=kc0001#). Refresher education is basic information to reinforce the understanding of OPSEC policy and procedures, critical information, and procedures covered in initial/localized OPSEC training.

#### **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. (ACC) Local organization-specific OPSEC awareness education is required when an individual processes into a new organization and/or when a commander determines the need for awareness education. This is considered event driven and not AF directed annual refresher training. Recommend including the OPSEC awareness education in the unit's in-processing briefings (i.e., Right Start, etc.) to fulfill initial in-processing requirement. Ensure the OPSEC awareness training is appropriately tracked and the individual is given credit for the initial unit training.

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.

### 5.3. 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.

5.3.1.1.1. **(Added-ACC)** For ACC units, if scheduling conflicts exist, a waiver will be sent to ACC/A3I signed by the wing (for SMO/SMNCO) or HQ (for PMs) commander. ACC OPSEC PM will then request a waiver from AF OPSEC PM. The approved waiver will be kept on file by the requesting and approving OPSEC PMs in their continuity books and maintained for three years.

5.3.1.1.2. **(Added-ACC)** Note that the AFI requires OPSEC PMs below MAJCOM level and SMO/SMNCOs to attend both the Signature Management Course (SMC) and the Interagency OPSEC Support Staff 's (IOSS) OPSEC Analysis and Program Management Course, OPSE 2500. HQ ACC cannot "grandfather" PMs. Current OPSEC PMs who have attended only one of the two courses need to attend the other course within 90 days.

5.3.1.1.3. **(Added-ACC)** To schedule SMC attendance, individuals must complete and return a nomination form provided by HQ ACC/A3I. ACC receives an allotment of class seats that will be prioritized across the command.

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.

5.3.1.2. **(ACC)** ACC OPSEC PMs will attend OPSE 2500 within 90 days of appointment. If scheduling conflicts exist, a waiver will be sent to ACC/A3I signed by the wing commander. HQ ACC/A3I will then request a waiver from the AF OPSEC PM.

OPSEC PMs can schedule OPSE 2500 directly with the IOSS. Upon graduation send a copy of the course certificate to the HQ ACC 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 highly 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.

5.3.2. (ACC) To clarify, the IOSS multimedia product —An Introduction to OPSEC (An Interactive Primer by the Department of Defense) is an accepted method for completing OPSEC orientation but not the only method. PMs/SMOs can, and are encouraged to replace or augment the IOSS course with locally-produced, tailored training for Coordinators.

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.

5.3.3. (ACC) OPSEC planners who are not also PMs do not require OPSE 2500 but may attend at unit's expense.

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>.

6.1.5. (ACC) ACC IG inspections will use the Compliance Inspection Checklists (CIC) when inspecting ACC units. ACC expects HQ ACC, NAFs, DRUs, and FOAs to protect critical information by following the checklist for their level and, if applicable, as a tenant to the installation where they are located. For example, HQ ACC will perform all the policy and guidance and program management duties as listed in AFI 10-701 and the core compliance checklist for MAJCOMs. In addition, HQ ACC is a tenant unit of JBLE and as such will perform the duties of the program Coordinator. Installation inspections should include tenant unit programs as well. If there is a non-ACC tenant unit(s), coordinate with the tenant's HHQ(s) or MAJCOM(s). Tenants should have and be familiar with the host unit CIL as well as their own tailored CIL. ACC tenants on an AF installation, to include HHQ organizations, are inspectable when the ACC/IG is assessing the host unit's OPSEC program. Although this supplement is not directive to non-ACC units, should the ACC/IG note that non-ACC tenants are not participating in the installation programs the IG will notify HQ ACC/A3I who will coordinate with the applicable MAJCOM/DRU OPSEC PMs. It is important that all safeguard critical information regardless of organizational differences.

6.1.5.1. **(Added-ACC)** ACC OPSEC PMs, SMOs and OPSEC Coordinators are required to maintain a continuity book that includes the last three years of data. A program that indicate it was only created to “pass the inspection” and does not show sustained continuity of the program between inspections will be downgraded. Unit programs that fail to comply with OPSEC PM and/or SMO retainability requirements and do not had an approved waiver on file will also be documented.

6.1.5.2. **(Added-ACC)** HQ ACC approved OPSEC and SM checklists for IG and self-inspection reside on the ACC/IG web site on the AF Portal and will be posted on the AFRC Management Internal Control Tool (MICT) web site. The ACC CICs are used during ACC/IG compliance inspections at all ACC units. HQ ACC/A3I will also post these CICs on the ACC OPSEC Community of Practice and/or applicable SharePoint sites. Units are encouraged to use these CICs during their internal self-inspection processes.

6.1.5.3. **(Added-ACC)** ACC GSU groups are designated wing equivalents and will use the wing/wing equivalent self-inspection checklist.

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.

6.2.1. **(ACC)** Annual OPSEC Program Review Reports for all ACC wings, C-NAFs DRUs and FOAs will be forwarded directly to HQ ACC/A3I using skip echelon processes. C-NAFs are not to consolidate subordinate wing reviews; however those C-NAFs with oversight of RED HORSE Squadron operations should solicit and incorporate their inputs into the C-NAF final report. Submit reports, via OSCAR, to HQ ACC/A3I NLT 1 Oct annually. If OSCAR is not available then submit via email. To facilitate HHQ reporting requirements, do not send reports as an imaged PDF file; instead use WORD “Save as” a PDF file option as this will permit text extraction/consolidation and HHQ reporting. Wing commander signatures may be imaged or e-signature.

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.

6.2.4. (ACC) ACC DRU and FOAs, reports will be signed by the commander. C-NAF reports will be signed (at the minimum) by DO/A3.

6.2.5. (Added-ACC) ACC units will complete and submit to ACC/A3I by 31 August a SM self-inspection using the ACC CIC checklists. SMOs will generate a self-inspection report on a separate sheet of paper identifying each self inspection item that was marked with a "No". The report (see [Attachment 13 Self-Inspection Report](#)) will be attached to the self inspection checklist. This report states the deficiency, POC, projected corrective action, and estimated corrective date. SMOs will also generate a self-inspection report on a separate sheet of paper identifying each self inspection item that was marked with a "Yes". The report will summarize why the item was in compliance and will be attached to the self inspection checklist. All three will be submitted as a single package signed by the commander.

### 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.

6.3.1. (ACC) SAVs may be conducted as needed by HHQ OPSEC PMs, HQ ACC policy is to conduct a SAV only when specifically requested by the wing commander. However, SAVs may be mandated after major inspections to help correct any identified deficiencies. ACC will not conduct SAVs within six-months preceding an inspection in order not to "teach the test." SAVs requested by the unit may have to be funded by the unit.

6.3.2. (Added-ACC) ACC Electronic-SAV (E-SAV):

6.3.2.1. **(Added-ACC)** ACC E-SAVs are a semi-formal unit assessment and vector check for compliance items. E-SAVs will not be conducted four months prior to any ACC IG Inspection. An E-SAV will quickly assess the health of the unit's OPSEC program without having to invest the man-hours and cost associated with traditional SAVs. Units can receive/request an E-SAV annually. HQ A3I will coordinate an appropriate date and time with the OPSEC PM/SMO/Coordinator.

6.3.2.2. **(Added-ACC)** Notification will be sent one month prior to the E-SAV. The notifications will include documents that will be used for the E-SAV. Inform the unit on currency/completeness of any documentation the HHQ OPSEC PM/SMO has on file, such as appointment letters and waiver requests, this provides the unit the opportunity to update their records prior to the E-SAV date.

#### **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 177<sup>th</sup> 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](mailto:CPD@lackland.af.smil.mil); IO MTT request are submitted to HQ ACC/A3I at [acc.xoz.iwd@langley.af.mil](mailto: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 mitigating identified threats and vulnerabilities.                   | The survey team, from an adversarial perspective, identifies information disclosed through normal operations and functions                        | At least every three years | N/A (CC may request other OPSEC support capabilities to assist if available) | Out-brief and report to organization CC   |
| 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<br>-Policy compliance<br>-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<br>- Shortfalls<br>- 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.

7.1.2. (ACC) ACC units will submit award nominations through USAFWC, 1 AF, 9 AF, or 12 AF to arrive at ACC/A3I by 15 October 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.

7.1.3. (ACC) ACC units wishing to compete for the National OPSEC Multimedia Achievement Award will submit the nomination through their wing and C-NAF/Center to ACC/A3I by 15 Oct each year.

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.

7.1.4. (ACC) Requirements for AF OPSEC awards are listed in AFI 36-2807, *Headquarters United States Air Force Deputy Chief of Staff, Operations, Plans and Requirements Annual Awards Program*, Chapter 12. These are separate from the IO awards found in Chapter 23.

## 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.

**8.1. (ACC) General:** AFI 10-701, Chapter 8 establishes requirements for “the organization” to include contract requirements. ACC adds these responsibilities to the MAJCOM, C-NAF, DRU, FOA, wing, and GSU group commanders that have responsibility to establish and maintain an OPSEC program/SM office and to his PM/SMO. The commander may designate, in writing, one or more individuals to perform these roles for him but the responsibility remains with the commander. In the absence of assigning the contractual requirements to another office, the OPSEC PM/SMO will be the office responsible for carrying out the commander’s guidance on the Chapter 8 contractual requirements.

#### 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.

8.2.2. 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).

8.2.8. **(Added-ACC)** Unit commanders should ensure OPSEC PM and/or Coordinators work with the contracting officers when writing contract documents such as Requests for Proposal and Statements of Work. Critical information should not be included in unclassified contract documents to reduce the vulnerability of that information being released. Contracting officers should have all unit CILs and will compare their unclassified documents to those lists to ensure critical information is not included. Commanders are responsible for their critical information. Unit OPSEC PM or Coordinator will review the documents before release.

**Chapter 9 (Added-ACC)****INFORMATION COLLECTIONS, RECORDS, AND FORMS**

**9.1. (Added-ACC) Information Collections.** No additional information collections are created by this supplement. The reporting requirements in the parent publication are exempt from licensing IAW AFI 33-324, *The Information Collections and Reports Management Program: Controlling Internal, Public, and Interagency Air Force Information Collections*, paragraph 2.11.1.

**9.2. (Added-ACC) Records.** OPSEC Status Reports and OPSEC Survey Reports are retained IAW T10-07, rules 01.00 – 06.00, of the AFRIMS (<https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>).

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

**ACC**

GILMARY M. HOSTAGE III, General, USAF  
Commander

## 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*, 30 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)

**Attachment 1 (ACC)****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFTTP 3-1.1, *General Planning* (U), 15 June 2007

AFI 10-404, *Base Support And Expeditionary (Bas&E) Site Planning*, 11 October 2011

AFI 36-2807, *Headquarters United States Air Force Deputy Chief of Staff, Operations, Plans and Requirements Annual Awards Program*, 18 July 2007

AFI 33-324, *The Information Collections and Reports Management Program: Controlling Internal, Public, and Interagency Air Force Information Collections*, 1 June 2000

AFI 90-1601, *Air Force Lessons Learned Program*, 25 September 2010

CJCSM 3122.03C, *Joint Operation Planning and Execution System Volume II, Planning Formats and Guidance*, 17 August 2007

***Adopted Forms***

DD Form 2757, *Welding Examination Record*

AFTO Form 781A, *Maintenance Discrepancy and Work Document*

AFTO Form 95, *Significant Historical Data*

AF Form 1800, *Operator's Inspection Guide and Trouble Report*

***Abbreviations and Acronyms***

AAR—After-Action Reports

ABW—Air Base Wing

ACC—Air Combat Command

ACOMS—Air Communications Squadron

ACW—Air Control Wing

ADPE—Automated Data Processing Equipment

AETC—Air Education and Training Command

AFFOR—Air Force Forces

AFI—Air Force Instruction

AFMC—Air Force Materiel Command

AFOSI—Air Force Office of Special Investigations

AFOTEC—Air Force Operational Test and Evaluation Center

AFRIMS—Air Force Records Information Management System

AFSOC—Air Force Special Operations Command

AFTTP—Air Force Tactics, Techniques, and Procedures

AFWC—Air Force Warfighting Center

AG—Airlift Group

AGOW—Air-Ground Operations Wing

ALSA—Air, Land, Sea, Application

AOC—Air and Space Operations Center

AOG—Air Operations Group

ARW—Air Refueling Wing

ASOS—Air Support Operations Squadron

Attch—Attachment

BPP—Base Profiling Process

BW—Bomb Wing

CCW—Command and Control Wing

CIC—Compliance Inspection Checklist

CIL—Critical Information List

CM—Countermeasure

C-NAF—Component Numbered Air Force

CONOP—Concept of Operations

CoP—Community of Practice

CRL—Custody Receipt Listing

Det—Detachment

DLA—Defense Logistics Agency

DRMO-- Defense Reutilization and Marketing Office

DRU—Direct Reporting Unit

ECG—Electronic Combat Group

Est—Estimated

EWG—Electronic Warfare Group

FOA—Field Operating Agency

FW—Fighter Wing

GSU—Geographically Separated Unit

HHQ—Higher Headquarters  
HQAF—Headquarters Air Force  
HOAB—Heartland of America Band  
IAW—In accordance with  
IG—Inspector General  
IMT—Information Management Tool  
IOG—Information Operations Group  
IOSS—Interagency OPSEC Support Staff:  
JBLE—Joint Base Langley-Eustis  
JCTD—Joint Concept Technology Demonstration  
JEPAC--Joint Electronic Protection for Air Combat  
MAJCOM—Major Command  
MICT—Management Internal Control Tool  
MILDEC—Military Deception  
MFR—memo for record  
MOA—Memorandum of Agreement  
MOE—Measure of Effectiveness  
MOP—Measure of Performance  
NAF—Numbered Air Force  
NAOC—National Airborne Operations Center  
NLT—Not later than  
NOS—Network Operations Squadron  
OI—Operating Instruction  
OL—Operating Location  
OPR—Office of Primary Responsibility  
OPSE 2500—IOSS course designator for the OPSEC Analysis and Program Management Course  
OPSEC—Operations Security  
OSI—Office of Special Investigations  
PCA—Permanent Change of Assignment  
PCS—Permanent Change of Station  
PM—Program Manager  
RAPCON—Radar Approach Control

RQG—Rescue Group  
RRP—Rapid Reaction Program  
RW—Reconnaissance Wing  
SAV—Staff Assistance Visit  
SEI—Special Experience Identifier  
SM—Signature Management  
SMC—Signature Management Course  
SMNCO—Signature Management Non-Commissioned Officer  
SMO—Signature Management Officer  
SPTS—Support Squadron  
STOS—Strategic Operations Squadron  
STRATCOM—[United States] Strategic Command  
TES—Test and Evaluation Squadron  
TG—Test Group  
TRS—Training Squadron  
TRSS—Training Support Squadron  
TSS—Training Support Squadron  
USAFWC—United States Air Force Warfare Center  
TTP—Tactics, Techniques, and Procedures  
WG—Wing  
WR-ALC—Warner Robins Air Logistics Center  
WSMR—White Sands Missile Range

## Attachment 2 (Added-ACC)

OPSEC PROGRAM MANAGER FOR ACC C-NAF AND DRUS APPOINTMENT  
LETTER TEMPLATEDEPARTMENT OF THE AIR FORCE  
HEADQUARTERS AIR COMBAT COMMAND  
JOINT BASE LANGLEY-EUSTIS VA

[Use your unit letterhead]

[date] 2012

MEMORANDUM FOR ACC/A3IF

SUBJECT: [your HQ C-NAF, DRU] Operations Security (OPSEC) Program Managers (PMs)

1. The following individuals are appointed as the OPSEC PMs for [your HQ.] IAW AFI 10-701. (Note, specify all units that the Program covers. i.e. "...for HQ 12AF, 612 AOC, 612 AFFOR, 612 ACOMS, and TOG." ACC recommends you have one program for the entire HQ but if the entire command is not covered under the one program then appoint other PMs to ensure the entire command has an OPSEC program]. These individuals meet all the requirements for rank and retainability as required in AFI 10-701 and the ACC supplement, and will be trained within 90 days of this appointment letter. (If individual will not be retained for two years attach the waiver request to this appointment letter. See **Attachment 6 Sample Waiver Memo** for format.)

| <u>Position</u> | <u>Name/Rank</u> | <u>Off</u><br><u>Symbol</u> | <u>Duty</u><br><u>Phone</u> | <u>Clearance</u> | <u>Est PCS/PCA/</u><br><u>Ret date</u> |
|-----------------|------------------|-----------------------------|-----------------------------|------------------|--|
|-----------------|------------------|-----------------------------|-----------------------------|------------------|--|

Primary  
Alternate

2. This letter supersedes all previous letters, same subject.

Name, Rank, USAF  
Commander

Atch: (if needed) Waiver to SMO retainability requirement request. (see **Attachment 6 Sample Waiver Memo**)

## Attachment 3 (Added-ACC)

## OPSEC PLAN FORMAT

## [unit] OPERATIONS SECURITY PLAN FORMAT

## TABLE OF CONTENTS

Table A3.1. OPSEC Plan Format.

| CONTENTS  | PAGE       |
|---|------------|
| SECURITY INSTRUCTIONS/RECORD OF CHANGES/RECORD OF REVIEWS                 | i          |
| PLAN SUMMARY  | Ii         |
| TABLE OF CONTENTS   | Iv         |
| BASIC PLAN  | 1          |
| ANNEX A, TASKED ORGANIZATIONS   | A-1        |
| ANNEX B, INTELLIGENCE THREAT  | B-1        |
| ANNEX C, OPERATIONS   | C-1        |
| APPENDIX 1. OPSEC WORKING GROUP (OWG or SMWG)                             | C-1-A-1    |
| APPENDIX 2. OPSEC TRAINING PROGRAM  | C-1-A-2    |
| TAB A. SAMPLE APPOINTMENT LETTER  | C-1-A-2-A1 |
| TAB B. CONTINUITY BOOK TABLE OF CONTENTS                                  | C-1-A-2-B1 |
| APPENDIX 3 TO ANNEX C, OPSEC PROCESS                                      | C-1-A-3    |
| TAB A. IDENTIFICATION OF CRITICAL INFORMATION                             | C-1-A-3-A1 |
| TAB B. ANALYSIS OF THREATS  | C-1-A-3-B1 |
| TAB C. ANALYSIS OF VULNERABILITIES  | C-1-A-3-C1 |
| EXHIBIT 1, OPSEC INDICATORS   | C-1-C-1-1  |
| TAB D. ASSESSMENT OF RISK   | C-1-D-1    |
| TAB E. APPLICATION OF APPROPRIATE OPSEC COUNTERMEASURES                   | C-1-E-1    |
| APPENDIX 4 TO ANNEX C, OPSEC PROGRAM MANAGEMENT TOOLS                     | C-4-1      |
| TAB A, APPOINTMENT LETTER TEMPLATE  | C-4-A-1    |
| TAB B. CONTINUITY BOOK TABLE OF CONTENTS                                  | C-4-B-1    |
| TAB C. CRITICAL INFORMATION LIST TEMPLATE                                 | C-4-C-1    |
| APPENDIX 5 TO ANNEX C, OPSEC ASSESSMENT PROGRAM                           | C-5-1      |
| APPENDIX 6 TO ANNEX C, OPSEC PLANNING                                     | C-6-1      |
| TAB A. "APPENDIX 3 TO ANNEX C TEMPLATE, OPERATIONS SECURITY"              | C-6-A-1    |
| TAB B," SAMPLE TAB A TO APPENDIX 1 TO ANNEX C, CRITICAL INFORMATION LIST" | C-6-B-1    |
| ANNEX Y, OPSEC RELATED DEFINITIONS  | Y-1        |
| ANNEX Z, DISTRIBUTION   | Z-1        |
| REFERENCES  | Z-2        |



## Attachment 4 (Added-ACC)

## SIGNATURE MANAGEMENT APPOINTMENT LETTER TEMPLATE



**DEPARTMENT OF THE AIR FORCE  
HEADQUARTERS AIR COMBAT COMMAND  
JOINT BASE LANGLEY-EUSTIS VA**

[Use your unit letterhead]

[date]

MEMORANDUM FOR ACC/A3IF

SUBJECT: [wing/GSU group] Signature Management Appointment Letter

1. The following individuals are appointed as the Signature Management Officer(s) (SMOs)/NCOs (SMNCOs) for [wing/Geographically Separated Unit (GSU) group]. The SMOs/SMNCOs will assume the duties of the OPSEC PM, SMO, and MILDEC Officer/NCO and be responsible for all program requirements directed in AFI 10-701 and AFI 10-704 and their ACC supplements.

Primary SMO/SMNCO:

NAME:

RANK:

CLEARANCE:

UNIT MAILING ADDRESS:

OFFICE SYMBOL:

DSN/STE:

CLASSIFIED FAX (DSN):

UNCLASSIFIED FAX (DSN):

OFFICE CELL (Commercial):

HOME PHONE (Commercial):

NIPR EMAIL ADDRESS:

SIPR EMAIL ADDRESS:

TRAINING STATUS: Signature Mgmt Course – [date]; OPSE 2500 OPSEC Analysis and Program Management Course – [date]

PROJECTED PCS/PCA/Ret Date (waiver request attached if less than two years from appointment date (see Attachment 6 Sample Waiver Memo):

Alternate SMO/SMNCO:

NAME:

RANK: 1

CLEARANCE:

UNIT MAILING ADDRESS:

OFFICE SYMBOL:

DSN/STE:

CLASSIFIED FAX (DSN):

UNCLASSIFIED FAX (DSN):

OFFICE CELL (Commercial):

HOME PHONE (Commercial):

NIPR EMAIL ADDRESS:

SIPR EMAIL ADDRESS:

TRAINING STATUS: Signature Mgmt Course – [date]; OPSE 2500 OPSEC Analysis and Program Management Course – [date]

PROJECTED PCS/PCA/Ret Date (waiver request attached if less than two years from appointment date):

2. These individuals meet all the requirements for rank and retainability as required in AFI 10-701 and AFI 10-704 and their respective ACC supplements, and will be trained within 90 days of this appointment letter.
3. The Signature Management Concept at the installation/GSU unit level combines both OPSEC and MILDEC under one office with a primary and alternate POC appointed in writing by the unit's commander. The unit SMO/SMNCO is responsible for the requirements set forth in both AFI 10-701 and AFI 10-704 and their respective ACC supplements.
4. This letter supersedes all previous letters, same subject.

Name, Rank, USAF  
Commander [wing/GSU Group]

Atch: (if needed) Attach minimum rank or two-year retainability waiver request(s), as required (See **Attachment 6 Sample Waiver Memo**).

## Attachment 5 (Added-ACC)

**OPSEC COORDINATOR/SMWG MEMBER APPOINTMENT LETTER TEMPLATE  
FOR BELOW WING LEVEL AND HQ DIRECTORATES**



**DEPARTMENT OF THE AIR FORCE  
HEADQUARTERS AIR COMBAT COMMAND  
JOINT BASE LANGLEY-EUSTIS VA**

[Use your unit letterhead]

[date]

MEMORANDUM FOR [your HHQ PM/SMO's office symbol]

SUBJECT: [your group, squadron, directorate or division] Operations Security (OPSEC) Program Coordinators and/or Signature Management Working Group (SMWG) member

1. The following individuals are appointed as the OPSEC Program Coordinators and/or SMWG member (designate below which role(s)) for [your dir. or div.] IAW AFI 10-701 OPSEC.

| <u>Position</u> | <u>Name/Rank</u> | <u>Off<br/>Symbol</u> | <u>Duty<br/>Phone</u> | <u>Clearance</u> | <u>Est PCS/PCA/<br/>Ret date</u> |
|-----------------|------------------|-----------------------|-----------------------|------------------|----------------------------------|
| Primary         |                  |                       |                       |                  |                                  |
| Alternate       |                  |                       |                       |                  |                                  |

2. This letter supersedes all previous letters, same subject.

Name, Rank, USAF  
Chief, [your directorate, division, group, squadron]

cc:

Attachment 6 (Added-ACC)  
SAMPLE WAIVER MEMO



DEPARTMENT OF THE AIR FORCE  
HEADQUARTERS AIR COMBAT COMMAND  
JOINT BASE LANGLEY-EUSTIS VA

[Use your unit letterhead]

{Date}

MEMORANDUM FOR HQ ACC/A3I

FROM: {Unit}/CC

SUBJECT: Request for Waiver to Signature Management Officer (SMO) [Signature Management NCO (SMNCO); OPSEC Program Manager (PM)] Retainability Requirement

1. AFI-10-701, Operations Security and AFI 10-704, Military Deception both require the SMO [SMNCO, PM] to have two years retainability from the date of appointment. This requirement is driven by training costs, return on investment, as well as health of the program since high turnover negatively affects the programs' effectiveness.
2. I am unable to appoint a SMO [SMNCO or PM] that meets the retainability requirement for the following reasons: [include rank, name of individual to be appointed with this waiver, expected date of departure, reason for departure, why another individual cannot be appointed that can meet the retainability requirement, and any other pertinent information.]
3. Request a waiver be granted to [unit requesting waiver] for [rank, name] until [estimated date]. At that time I intend to meet the requirement by [state corrective actions that will bring the units program into compliance].

[Signature]  
[Grade], USAF  
Commander

cc:

**Attachment 7 (Added-ACC)**

**STANDARDIZED ACC UNIT SM/OPSEC CONTINUITY BOOK**

**STANDARDIZED ACC UNIT SM/OPSEC CONTINUITY BOOK**

**TABLE OF CONTENTS**

**Note:** Electronic continuity books are authorized and encouraged. The overall structure (folder hierarchy) of the e-book should match this attachment. At the PM/SMO's discretion, hard copies of critical sections may be maintained. A hard-copy showing the network path/route to the e-book is mandatory. (For example: \\lfi-cs-fas01\shared\myopsecprogram\best%20continuity%20binder%20ever)

**Note:** If the file is not actually put in the continuity book (either hard copy or electronic continuity book) then specify at the appropriate Tab the location of the file. This could be because of the large size of the file/document or because its classification precludes including in the unclassified book/e-book. Example for a hard copy file location might be "IV 2 Threat Assessment (S) found in Safe #3, Drawer 2, OPSEC folder, documents 2-5". An example of an electronic file might be "IV 2 Threat Assessment (S) found in XP sharedrive O-- \\lfi-cs-fas01\shared\XP\OPSEC\Threat assessment."

**Note:** A unit Coordinator should have a continuity book also but it does not need to contain all of the same content. Items below marked with an asterisk should be in a unit Coordinator continuity book.

**TAB   DESCRIPTION**

\*I.     SM/OPSEC Appointment Letters and Approved Waivers

(ACC) 1. SMO/SMNCO or OPSEC PM/Alt PM (See **Attachment 4 Signature Management Appointment Letter Template** or **Attachment 2: OPSEC Program Manager for ACC C-NAF and DRUs Appointment Letter Template**.)

(ACC) 2. SM Working Group (SMWG) or OPSEC WG (OWG) (See **Attachment 5 (Added): OPSEC Coordinator Appointment Letter Template for Below Wing Level and HQ Directorates**)

3. SM/OPSEC Training Certificates and Approved Waivers (if applicable) (see **Attachment 6 Sample Waiver Memo**)

(ACC) a. Unit commander orientation briefing completion.

\*b. SM/PM Training certificates

\*c. OWG/SMWG training completion.

\*II.    SMO/SMNCO or OPSEC Coordinator's Authorization Letter (See ACC Supplement to AFI 10-704 for letter format)

III.    SMWG/OWG Roster (See **Attachment 9 SMWG Master Roster**)

\*IV.    OPSEC/BPP Products

- (ACC) 1. The unit's operational Critical Information List (proposed and final)
- (ACC) 2. Unit Threat Analysis documents (AFOSI, OSCAR, Cyber Threats, Other) (S)
- (ACC) 3. A list of your unit/installation's Vulnerabilities and Indicators.
- (ACC) 4. A Risk Analysis of your unit's vulnerabilities (before and after proposed countermeasures are implemented)
- (ACC) 5. A list of proposed Countermeasures, the costs of implementing those CMs, and those CMs that are chosen to implement.
- (ACC) 6. Measure(s) of Performance and Effectiveness for each countermeasure
- 7. Requests for Intelligence (RFIs) and other reports needed to assess the MOPs/MOEs.
- (ACC) 8. Assessments of the countermeasures as determined from Intelligence and OSI reports, and periodic wing exercises.
- 9. A list of major wing/installation activities/missions (see **paragraph 2.3.3.1. and Table 2.1 Standard ACC Wing Activities for Base Profiling**)
- 10. A detailed flow chart of each major wing/installation activity/mission
- 11. A master checklist of all wing/installation activities/missions. See **Attachment 11: Signature Management Execution Checklist.**
- V. SMO/OPSEC Position Description / Roles and Responsibilities (See AFI 10-701, AFI 10-704 and respective ACC supplements)
- VI. Phase I Operational Readiness Exercise (ORE) Report [Last Inspection]
- VII. Phase I Operational Readiness Inspection (ORI) Report [Last Inspection]
- VIII. Compliance Inspection Report [Last Inspection]
- IX. SM/OPSEC Local Exercise After-Action Reports (See
- X. SM/OPSEC Local Exercise Lessons Learned
- XI. Program Self-Assessment Documents
- (ACC) 1. Staff Assistance Visit Reports
- (ACC) 2. E-SAV Results
- (ACC) 3. Self-Inspection Checklist (See ACC Checklist found at the ACC OPSEC Community of Practice Page or SharePoint page.
  - 4. Self-Inspection Report (see **Attachment 13 Self-Inspection Report**)
- XII. Memorandum of Understanding between Host and Tenant Units (as applicable) (See **Attachment 8: Host Tenant Relationships for ACC Units** for applicability)
- XIII. SM (OPSEC/MILDEC) TDY Orders/Paid Travel Vouchers
- XIV. Current SM Execution Checklist (See **Attachment 11: Signature Management Execution Checklist**)

- XV. (Wing level (SMO) only) Unit SM (OPSEC and MILDEC) Annual Report(s)
- XVI. (Wing level (SMO) only) USAF MILDEC Security Classification / Declassification Guide (FOUO)
- XVII. AFTTP 3-1, Information Operations, OPSEC Chapter 9 (OPSEC TTPs) (S)
- \*XVIII. Air Force Instructions
- (ACC) 1. AFI 10-701, Operations Security
  - 2. (Wing level (SMO) only) AFI 10-704, Military Deception Program (S), SM Chapter only.
- \*XIX. ACC Supplements
- (ACC) 1. AFI 10-701, ACC Supplement Operations Security
  - 2. (Wing level (SMO) only) AFI 10-704, ACC Supplement Military Deception Program (S)
- XX. Current Copy of Unit Base Support Plan (Classified and/or unclassified Versions, as applicable)
- \*XXI. Current Unit Threat Assessment Documents (AFOSI, OSCAR, Cyber Threats, Other) (S)
- XXII. SMWG/OWG Meeting Minutes/attendance rosters
- XXIII. SM/OPSEC Master File Plan (including archive)
- XXIV. Current Unit ADPE Listing of SM equipment (i.e. FAX, Laptop, Desktop computer, Printer, etc.)
- XXV. Current Unit Custodian Authorization (CA)/Custody Receipt Listing (CRL) of SM equipment (i.e. STE, Safe)
- XXVI. (Wing level (SMO) only) OPSEC and MILDEC Annual Awards Package (AF Form 1206, biography, and commander's nomination letter)
- XXVII. Current DOC Statement for each subordinate unit assigned (S)
- XXVII. Copies of past Operational Event Logs (See **Attachment 12 SIGNATURE MANAGEMENT EVENT LOG** for example)
- XXIX. Copies of AF IMT 310, Document Receipt and Destruction Certificate; and AF Form 12 Accountable Container Receipts
- XXX. Current ACC SM/OPSEC Network Roster
- XXXI. ACC E-Grams

Notes:

Content may require two or more volumes to the continuity book.

Additional tabs may be needed for unit specific needs. Add the tabs to the end of the standard format.

## Attachment 8 (Added-ACC)

## HOST TENANT RELATIONSHIPS FOR ACC UNITS

Table A8.1. Host Tenant Relationships for ACC Units.

| INSTALLATION                            | HOST UNIT<br>(M) Denotes Host<br>ACC Unit MOA<br>Required | TENANTS (ACC)<br>(P) Denotes ACC Unit Should<br>Have Its Own SM/OPSEC<br>PM Effort | TENANTS (NON-ACC)<br>IF ACC UNIT IS THE HOST UNIT<br>Consider These Units When Establishing a MOA (Assess for<br>applicability)<br>This is not an all inclusive list. |
|---|---|--|---|
| Beale AFB                               | 9RW (M)(P)  |  | 940th Air Refueling Wing (AFRC)   |
| Davis-Monthan AFB                       | 355WG (M) (P)   | [HQ 12 AF, 612 AOC/AFFOR,<br>612 ACOMS, 612 SPTS,<br>612 TOG] (P)                  | 214 RQG   |
|   |   | 943RQG (P)   | 162 FW (ANG)  |
|   |   | 563RQG (P)   | Aerospace Maintenance and Regeneration Group (AMARG) (AFMC)   |
|   |   | 55ECG (P)  |   |
| Dyess AFB                               | 7BW (M) (P)   |  | 317 AG (AMC)  |
| Eglin AFB                               | 96 ABW (Host)<br>(AFMC)                                   | 53WG (P)   | Non-ACC host  |
| Ellsworth AFB                           | 28BW (M) (P)  |  | 82nd Civil Support Team   |
|   |   |  | Det 8, AETC   |
| Hill AFB                                | 75 ABW (Host)<br>(AFMC)                                   | 388FW (P)  | Non-ACC host  |
| Holloman AFB                            | 49WG (M) (P)  |  | 46 Test Group   |
|   |   |  | 417th Weapons Squadron  |
|   |   |  | Army Air Division   |
|   |   |  | Det 1, 53D Test and Evaluation Group  |
|   |   |  | Det 1, 82nd Aerial Target Squadron  |
|   |   |  | Det 1, 21st Operations Group German Air Force Flying Training Center  |
|   |   |  | National Range Operations – WSMR  |
|   |   |  | 746th Test Squadron   |
|   |   |  | 4th Space Control Squadron  |
|   |   |  | 586th Flight Test Squadron  |
|   |   |  | 846th Test Squadron   |
|   |   |  | Corps Of Engineers  |
|   |   |  | Defense Automated Printing Services   |
|   |   |  | Det 4, Air Force Weather Agency   |
|   |   |  | M1 Support Services   |
|   |   |  | National Geospatial Intelligence Agency   |
|   |   |  | New Mexico Technology Group   |
| OL-AB, Air Force Research Lab           |   |  |   |
| OL-AC, Air Force Research Lab           |   |  |   |
| Physical Science Laboratory             |   |  |   |
| Hurlburt Field                          | 1st SOW (Host)<br>(AFSOC)                                 | 505 CCW (P)  | Non-ACC host  |
| Joint Base Langley-<br>Eustis<br>(JBLE) | 633ABW (M) (P)  | 1FW (P)  | 192FW   |
|   |   | HQ ACC (P)   | WR-ALC, Det 1   |
|   |   |  | 710 Combat Ops Squadron   |
|   |   |  | AF Element vehicle and equipment and support office   |

|                     |                      |  |                                       |
|---------------------|----------------------|--|---------------------------------------|
|                     |                      |  | NASA                                  |
|                     |                      |  | Civil Air Patrol                      |
|                     |                      |  | 71 <sup>st</sup> Aerial Port Squadron |
|                     |                      |  | 372 TRS Det 218                       |
|                     |                      |  | 512 AW Mission Support                |
| Moody AFB           | 23 WG (M) (P)        | 93AGOW (P)                                     |                                       |
| Mountain Home AFB   | 366FW (P)            |  |                                       |
| Nellis/Creech       | 99 ABW (M) (P)       | AFWC (P)                                       | JEPAC                                 |
|                     |                      | 432WG (P)                                      | 763d Maintenance Sq                   |
|                     |                      | 57 WG (P)                                      |                                       |
|                     |                      | NTTR (P)                                       |                                       |
|                     |                      | USAF AMMOS                                     |                                       |
|                     |                      | AF Weapons School                              |                                       |
|                     |                      | 232d Operations Squadron                       |                                       |
|                     |                      | 505 TES  |                                       |
|                     |                      | 53 EWG OL-                                     |                                       |
|                     |                      | 563 RQG (P)                                    |                                       |
|                     |                      | 58 RQG (P)                                     |                                       |
|                     |                      | 66th RQG (P)                                   |                                       |
| Det 8 ACC TSS       |                      |  |                                       |
| Offutt AFB          | 55WG (M) (P)         | Det 10, ACC TRSS                               | NAOC                                  |
|                     |                      |  | 625 STOS                              |
| Robins AFB          | 78 ABW (Host) (AFMC) | 461 ACW (P)                                    | Non-ACC host                          |
| Seymour Johnson AFB | 4FW (M) (P)          |  | 916 ARW                               |
| Shaw AFB            | 20FW (M) (P)         | [HQ USAFCENT/AOC Det 1, AFFOR/ACOMS / 9AF] (P) |                                       |
| Tinker AFB          | 72 ABW (Host) (AFMC) | 552 ACW (P)[HQ]                                | Non-ACC host                          |
| Tyndall AFB         | 325FW (Host) (AETC)  |  | Non-ACC host                          |

**Note: Changes in org will not drive a change to the ACC Supp. Do not assume you have no requirements if your org is not specifically mentioned. Contact ACC PM for requirements.**

**Attachment 9 (Added-ACC)**  
**SMWG MASTER ROSTER**

**A9.1. Note:** The SMWG roster that starts on the next page is a list of typical flying wing's subject matter experts (SMEs) that should be considered as part of the unit SMWG. Although the list is based on a flying unit, ACC unit SM personnel need to remember to identify, train, and exercise SMWG personnel from all non-flying support units and functions within the wing as well to ensure a complete wing SM capability. Remember that the example list is not all-inclusive and may need to be amended to suit your particular unit location, mission, or organizational structure. You may not need to use each and every functional area SME for a particular SM exercise/operation, but you should try to work through the lower echelon group and squadron commanders to have them appoint someone as a SMWG member. The SMWG roster should also include tenant units assigned on the host installation. Where the ACC unit is tenant on a non-ACC base, the ACC unit's SM personnel must include the host unit SM personnel as part of the ACC units SMWG. The SMWG master roster will be maintained as a FOUO document when filled in with personnel data. The following privacy act statement must be added to the roster when filled in with personal data. **“This document contains FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Privacy Act and AFI 33-332.”**

Column A – Enter functional area title

Column B – Enter functional area office symbol

Column C - Enter SMWG member's last name

Column D - Enter SMWG member's first name

Column E – Enter SMWG member's middle initial

Column F - Enter SMWG member's rank

Column G - Enter SMWG member's work phone number

Column H - Enter SMWG member's cell phone number

Column I - Enter SMWG member's home phone number

Column J - Enter SMWG member's email address

Column K - Enter SMWG member's initial or refresher training date

Column L - Enter whether the SMWG member is the primary or alternate appointee



**Attachment 10 (Added-ACC)**  
**EXERCISE PROPOSAL FORMAT**

**All material will be dated and include classification and declassification instructions.**



**DEPARTMENT OF THE AIR FORCE**  
**HEADQUARTERS AIR COMBAT COMMAND**  
**JOINT BASE LANGLEY-EUSTIS VA**

[Use your unit letterhead]

[date]

MEMORANDUM FOR HQ ACC/A3IF

FROM: (Your Wing)

Subject: (Signature Management Training Exercise Supporting Exercise Camel Jockey) or  
 (Signature Management Quarterly Training Exercise, FY 12/1) (U)

1. (Classification) Overall Situation: This paragraph will contain a brief synopsis of the actual exercise taking place that SM will support. List the objective(s) of this exercise (objectives are those of the actual exercises, not the SM objectives).
2. (Classification) Critical Information: List the critical information associated with the supported exercise (if no supporting exercise, critical information associated with the Wing that requires SMC support).
3. (Classification) SM Collaboration: This paragraph will identify the tactics, techniques and procedures that will be used to protect the critical information. (i.e. Hangar four will hide/cover the identity of the deploying force, face to face communications will protect the coordination process for the deploying force or uniforms will be changed to hide actual identity of forces (patches/hats).
4. (Classification) Base Threat Assessment: List the current threats that are present in the area that possibly collect information on your base. Data of this type may be found in the Base Threat Assessment published by OSI at the following website:  
[Http://www.afosi.af.smil.mil/threatcenter/](http://www.afosi.af.smil.mil/threatcenter/)
5. (Classification) SM Working Group (Trusted Agent) Composition: List all members with a working knowledge of the protective or exploitation measure(s) and those that will be used to portray events to assist the plan.

6. (Classification) Exercise Overview: Discuss how you envision the SM scenario to unfold, (i.e. cover story presented, backstopping done to reinforce the cover story). Attach a draft/working copy of the developed SM execution checklist.
7. (Classification) Feedback. Develop Measures of Performance (MOP). List the Measures that will be used to judge the performance of the SM execution checklist. (i.e. Was the Hangar guard posted at the exact time indicated on the checklist?)
8. (Classification) After Action Report (AARs): Will include an evaluation of all of the above and any ideas for improvement. MOPs should be evaluated as to if an action item was to happen at a certain time or location, and did it take place, and as planned. AARs will be submitted within 15 days following termination of the exercise.
9. Cost estimates, if any, will include specific US dollar amounts for each person that directly supports the SM activity (i.e. per diem, travel, rental vehicles, lodging, etc.)



## Attachment 12 (Added-ACC)

## SIGNATURE MANAGEMENT EVENT LOG

Table A12.1. Signature Management Event Log.

| SIGNATURE MANAGEMENT EVENT LOG |  |                  |                 |          |                       |                               |                    |
|--------------------------------|--|------------------|-----------------|----------|-----------------------|-------------------------------|--------------------|
| [Current Date]                 |  |                  |                 |          |                       |                               |                    |
| Event #                        | Event (Brief Explanation)  | Start Time Local | Start Time Zulu | Date     | OPR                   | Individual                    | OPR Contact Number |
| 001                            | Prepare to Deploy Order message received                                       | 0630             | 0030            | 6 Dec 11 | WOC                   | SMSgt Widget                  | 734-1900           |
| 002                            | SMO recalled by Wing Operations Center as part of Battle Staff Recall          | 0635             | 0035            | 6 Dec 11 | WOC                   | SMSgt Widget                  | 734-1900           |
| 003                            | SMO notifies SMNCO   | 0640             | 0040            | 6 Dec 11 | SMO                   | Capt Anderson                 | 869-6977           |
| 004                            | SMO and SMNCO arrive at the WOC  | 0700             | 0100            | 6 Dec 11 | SMO                   | Capt Anderson and MSgt Franks | 869-6977           |
| 005                            | SMO meeting with Wing/CC and CV  | 0730             | 0130            | 6 Dec 11 | Battle Staff Director | Lt Col Babski                 |                    |
| 006                            | Wing/CC gives vector on SM Courses of Action                                   | 0730             | 0130            | 6 Dec 11 | WOC                   | Col Wingman                   |                    |
| 007                            | Wing/CC and SMO discuss plausible/believable/verifiable/consistent cover story | 0900             | 0300            | 6 Dec 11 | WOC                   | Col Wingman                   |                    |
| 008                            | SMO depart WOC   | 1000             | 0400            | 6 Dec 11 | SMO                   | Capt Anderson and MSgt Franks | 869-6977           |
| 009                            | SMO arrive back at office  | 1030             | 0430            | 6 Dec 11 | SMO                   | Capt Anderson and MSgt Franks | 869-6977           |
| 010                            | SMO convenes SMWG  | 1200             | 0600            | 6 Dec 11 | SMO                   | Capt Anderson and MSgt Franks | 869-6977           |

## Attachment 13 (Added-ACC)

## SELF-INSPECTION REPORT



**DEPARTMENT OF THE AIR FORCE  
HEADQUARTERS AIR COMBAT COMMAND  
JOINT BASE LANGLEY-EUSTIS VA**

[Use your unit letterhead]

{Date}

MEMORANDUM FOR HQ ACC/A3IF

FROM: {Unit}/CC

SUBJECT: SM (OPSEC/MILDEC) Self-Inspection Report

1. Listed below are the individual deficiencies checked/marked as "NO" on the SM / MILDEC self-inspection checklist conducted on [date].

Checklist Item Number: [enter checklist item number]

Restate Item Question: [restate item number question from the self-inspection checklist]

Deficiency POC (Rank / Name): [enter individual responsible for correcting the finding]

Projected Corrective Action(s): [enter corrective measures that will be taken to correct the deficiency]

Established Corrective Closeout Date For This Item: [enter suspense/closeout date for deficiency]

Checklist Item Number: [enter checklist item number]

Restate Item Question: [restate item number question from the self-inspection checklist]

Deficiency POC (Rank / Name): [enter individual responsible for correcting the finding]

Projected Corrective Action(s): [enter corrective measures that will be taken to correct the deficiency]

Established Corrective Closeout Date For This Item: [enter suspense/closeout date for deficiency]

[Repeat for each deficiency.]

2. [Unit]'s POC is [Rank, Name, contact information]

[Signature]  
[Grade], USAF  
Commander