BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-701

18 OCTOBER 2007

Operations

OPERATIONS SECURITY (OPSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A3O-CI
Certified by: AF/A3O (Maj Gen (S) Gibson)
Supersedes AFI10-701, 30 September 2005
Pages: 38

This publication implements Air Force Policy Directive (AFPD) 10-7, *Air Force Information Operations*, September 6, 2006; and DOD Directive 5205.02, *DOD Operations Security Program*, March 6, 2006, and Joint Publication 3-13.3, *Operations Security,* June 29, 2006. The reporting requirements in this publication are exempt from licensing in accordance with AFI 33-324 paragraph 2.11.1, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*. It applies to all Major Commands (MAJCOM), Field Operating Agencies (FOA), Direct Reporting Units (DRU), Air National Guard (ANG) units and Air Force Reserve Command (AFRC). Any reference to wing-level OPSEC program management applies to wing and wing-equivalent organizations such as agency directorates, tenant units, numbered Air Force units and centers of excellence. 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 IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through MAJCOM publications/forms managers. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, (will convert to 33-363) *Management of Records* and disposed of in accordance with the *Air Force Records Disposition Schedule (RDS)* located at **https://afrims.amc.af.mil/**. 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

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed.

Chapter 1

GENERAL

1.1. General:

1.1.1. 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 core military capabilities of psychological operations (PSYOP), OPSEC, military deception (MILDEC), counterintelligence (CI) operations, public affairs (PA) operations and counterpropaganda operations to affect behaviors, protect operations, communicate commander's intent and project accurate information to achieve desired effects across the battle space. OPSEC's desired affect 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 unit OPSEC program managers (PM) or coordinators will reside in the operations and/or plans element of an organization or report directly to the commander. For those units with no traditional operations or plans element, the commander must decide the most logical area to place management and coordination of the unit's OPSEC program while focusing on operations and the mission of the unit.

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 from 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 planning to ensure critical information and indicators are identified. The Air Force will integrate OPSEC into military strategy, operational and tactical planning and execution, military indoctrination, support activities, contingency, combat and peacetime operations and exercises, communications-computer architectures and processing, weapons systems Research, Development, Test and Evaluation (RDT&E), Air Force specialized training, inspections, acquisition and procurement, 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 OPSEC measures are required.

1.4.2. **Headquarters, United States Air Force (HQ/USAF).** The Deputy Chief of Staff for Operations, Plans and Requirements (AF/A3/5) is the office of primary responsibility (OPR) for implementing DOD OPSEC policy and guidance. This responsibility is assigned to the Director of Operations (AF/A3O). AF/A3O 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. Assigning a full-time AF OPSEC PM (O-4 or YA-03) and ensuring AF OPSEC forces are aligned with the AF IO Career Force Plan once it has been fully established.

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

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

1.4.2.1.4. Ensuring OPSEC surveys are conducted for subordinate commands and agencies at least once every three years in order to enhance mission effectiveness.

1.4.2.2. Develop Air Force Departmental publications to define policy, guidance, responsibilities, authorities and 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 J-3.

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

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

1.4.2.5. Provide oversight, advocacy and act 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 servants and to those contractors who have access to mission critical information.

1.4.2.7. Ensure government contract requirements properly reflect OPSEC requirements.

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

1.4.3. **The Secretary of the Air Force Office of Warfighting Integration and Chief Information Officer (SAF/XC):**

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

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

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

1.4.5. **The Assistant Secretary of the Air Force, Acquisition (SAF/AQ)** provides policy and guidance to ensure OPSEC is considered in AF acquisition and RDT&E.

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

1.4.7.1. Implement AF OPSEC policy 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.

1.4.7.2. Develop effective OPSEC programs IAW guidance issued by AF/A3O.

1.4.7.3. Designate an organization as the OPR for OPSEC and appoint a full-time OPSEC PM position (O-3/4 or YA-02/03) IAW the AF IO Career Force plan once it has been fully established. 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.

1.4.7.4. Ensure OPSEC PMs have at a minimum a secret clearance and access to SIPRNET, NIPRNET and organizational email accounts.

1.4.7.5. Develop policy and issue implementing supplements or other guidance as required.

1.4.7.6. Consolidate OPSEC requirements and submit them to the AF IO requirements and analysis working group for inclusion into the Air Force IO Capabilities Plan.

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

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

1.4.7.9. Ensure all subordinate units are controlling critical information and indicators.

1.4.7.10. Ensure all subordinate units plan, exercise and implement OPSEC measures as appropriate.

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

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

1.4.7.13. Ensure training of OPSEC PMs and planners at wing-level and above is accomplished as soon as possible upon being appointed.

1.4.7.14. All OPSEC PMs and planners will be assigned an OPSEC special experience identifier (SEI) when the AF IO Career Force is fully established. SEIs will drive future training allocations upon receipt of orders or upon assignment to units with SEI coded positions.

1.4.7.15. Develop and cultivate the intelligence and CI relationships necessary to support OPSEC programs.

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

1.4.7.17. Ensure OPSEC considerations are included in annual unclassified public web page reviews and in the approval process for posting new data to AF public and private web sites.

1.4.7.18. Ensure assistance is provided to wing public affairs (PA) office as needed to ensure OPSEC considerations are included in PA review and approval processes for publishing/releasing information to the public.

1.4.7.19. Forward annual self-assessment report for the fiscal year period of 1 Oct - 30 Sep, to the AF OPSEC PM (AF/A3O-CI) NLT 31 October each year (See **Attachment 2**)

1.4.7.20. Ensure OPSEC related briefings or presentations to be given outside the MAJCOM are coordinated through the Air Force OPSEC PM, AF/A3O-CI, prior to the presentation date.

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

1.4.8.1. 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.

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

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

1.4.8.4. Provide capabilities to meet Air Force OPSEC assessment requirements.

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

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

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

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

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

1.4.9.3. Integrate OPSEC into the AMC AOC construct.

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

1.4.9.5. Centrally program for MAF OPSEC capabilities.

1.4.10. **Air Force Material Command (AFMC) will:**

1.4.10.1. Ensure OPSEC is integrated into all RDT&E efforts. When critical information is involved ensure OPSEC is applied throughout the life cycle of all weapon systems.

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

1.4.11.1. 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.

1.4.11.2. 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.

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

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

1.4.11.5. Establish a validation process to ensure AF/A3O-CI, reviews all AETC OPSEC training materials used in accession and professional military education.

1.4.12. **Air Force Office of Special Investigations (AFOSI) will:**

1.4.12.1. Provide OPSEC PMs, coordinators and unit commanders with AFOSI local threat information.

1.4.12.2. Provide counterintelligence vulnerability support when possible for OPSEC assessments.

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 will:**

1.4.15.1. Issue policy and guidance 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 OPSEC measures. They must determine the balance between OPSEC measures and operational needs.

1.4.15.2. Appoint in writing a primary and alternate OPSEC PM or coordinator and forward to higher headquarters (HHQ) OPSEC PM. OPSEC PMs will be assigned for a minimum of 18 months. Organizations where an assignment is less than 18 months will request, in writing, a waiver through their MAJCOM OPSEC PM from AF/A3O-CI. Once the AF IO Career Force Plan has been fully established, OPSEC PMs, coordinators and planners will be assigned to manpower billets IAW the AF IO Career Force Plan.

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

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

1.4.15.5. Ensure OPSEC assessments are conducted to support operational missions.

1.4.15.6. Establish OPSEC working groups (OWG) at the wing-level and above. In addition, an ad-hoc OWG will be established for any large-scale operation or exercise. ***NOTE***: Refer to AFTTP 3-1.36*, Information Warfare Planning, Integration, and Employment Considerations (U), Attachment 5* for additional guidance to include OWG composition and responsibilities.

1.4.16. **OPSEC PMs:** Are assigned at the wing-level and above and will:

1.4.16.1. Manage the organization's OPSEC program.

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

1.4.16.3. Have at a minimum a secret clearance and access to SIPRNET, NIPRNET and organizational email accounts.

1.4.16.4. Develop, maintain, and monitor the execution of the organization's OPSEC program.

1.4.16.5. Ensure OPSEC is incorporated into organizational plans, exercises, and activities.

1.4.16.6. Develop and implement commander's OPSEC policy and critical information list.

1.4.16.7. Ensure OPSEC is integrated into IO, IFO and other supporting capabilities.

1.4.16.8. Ensure procedures are in place to control critical information and indicators to include compiling subordinate organization critical information for consolidation into command critical information lists.

1.4.16.9. Participate in annual multi-disciplinary web page review boards as outlined in AFI 33-129, *Web Management and Internet Use*, Para 3.9.1. ***Note:*** OPSEC PMs develop policy to be used by web page review boards. OPSEC PMs will answer questions concerning protecting critical information and when required will coordinate OPSEC reviews of public and/or restricted web pages.

1.4.16.10. Assist wing PA office as needed to ensure OPSEC considerations are included in PA review and approval processes for publishing/releasing information to the public; to include but not limited to printed and televised media. OPSEC PMs will develop policy to be used by PA and provide advice concerning protecting critical information.

1.4.16.11. Provide management, development, and oversight of appropriate OPSEC training and ensure training is provided to subordinate coordinators and OWG members.

1.4.16.12. Ensure unit deployment managers (UDM) add OPSEC awareness training as a mandatory UDM requirement for deploying personnel.

1.4.16.13. Ensure annual OPSEC self-assessments are conducted (See attachment 3) by subordinate units for the fiscal year period (1 Oct - 30 Sep) and results forward via annual self-assessment report through MAJCOM to reach AF/A3O-CI NLT 31 October each year. Annual self-assessment reports will be maintained on file for at least 1 year after the end of each fiscal year.

1.4.16.14. Chair OWG. The OWG will consist of representatives from the appropriate IO and security disciplines and applicable supporting organizations. ***NOTE***: Refer to AFTTP 3-1.36, Attachment 5 for additional guidance to include OWG composition and responsibilities.

1.4.16.15. Coordinate and facilitate OPSEC assessments such as surveys, annual self-assessments, and vulnerability assessments as listed in **Chapter 5**.

1.4.16.16. Serve as the focal point for OPSEC support capabilities as listed in **Chapter 5**.

1.4.16.17. Conduct Staff Assistance Visits (SAV) on subordinate units as required or requested.

1.4.16.18. Submit request for intelligence (RFI) information to the appropriate intelligence organization to ensure OPSEC PMs and planners receive timely intelligence threat briefings and/or updates to determine OPSEC implications.

1.4.16.19. Coordinate and integrate OPSEC initiatives with tenant unit OPSEC PMs/coordinators even though administrative oversight of the tenant unit's program still resides with their respective MAJCOM.

1.4.16.20. Serve on exercise evaluation teams (EET) to observe and evaluate mission profiles and signatures, as well as OPSEC measures of performance (MOPs) that assess the organizations ability to mitigate loss of critical information. OPSEC PMs will also evaluate how unit personnel execute OPSEC measures. Any deficiencies or best practices will be submitted in after action reports and to the AF lessons learned database (**https://afknowledge.langley.af.mil/afcks/**). 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*.

1.4.17. **OPSEC coordinators:** Are assigned in writing at each subordinate organization below the wing-level (MAJCOM, ANG, FOA, and DRUs also require coordinators within HQ directorates, as appropriate) and will:

1.4.17.1. Have at least a minimum secret clearance, possess a NIPRNET and access to an organizational email and SIPRNET accounts.

1.4.17.2. Advise commander on all OPSEC matters to include developing and recommending policy, guidance, instructions, and measures.

1.4.17.3. Tenant unit OPSEC coordinators will closely coordinate and integrate with host wing OPSEC initiatives and working groups. However, administrative oversight of the tenant unit's program still resides with their HHQ OPSEC PM. If the host wing has an OPSEC working group, the coordinator will seek representation in it.

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

1.4.17.5. Develop, implement, and distribute commander's OPSEC policy and critical information list. Review periodically for currency and update as necessary.

1.4.17.6. Ensure procedures are in place to control critical information and indicators and are reviewed periodically for effectiveness.

1.4.17.7. Utilize assessment results to correct discovered vulnerabilities and aid organization OPSEC awareness efforts.

1.4.17.8. Ensure OPSEC reviews are conducted on all organizational web pages prior to the information being posted, updated, or modified.

1.4.17.9. Conduct OPSEC reviews of information submitted for publication or release to the public. This could include, but is not limited to base newspapers, safety magazines, flyers, web pages, television interviews and information for news articles.

1.4.17.10. Coordinate with appropriate organizations and wing senior leadership to resolve/mitigate AF OPSEC assessment findings as required.

1.4.17.11. Provide management of unit's OPSEC training and ensure initial OPSEC awareness training is accomplished upon arrival of newly assigned personnel and annual refresher OPSEC training thereafter.

1.4.17.12. Coordinate, facilitate, and conduct OPSEC assessments such as surveys, annual self-assessments (See **Attachment 3**), and vulnerability assessments as listed in **Chapter 5**. Forward annual self-assessment reports for the period of 1 Oct through 30 Sep each fiscal year to HHQ OPSEC PM according to MAJCOM guidance.

1.4.17.13. Serve as the focal point for OPSEC support capabilities as listed in **Chapter 5**.

Chapter 2

OPSEC PROCESS

2.1. General:

2.1.1. OPSEC is accomplished using a five-step process: 1) Identify critical information; 2) Analyze threats; 3) Analyze vulnerabilities; 4) Assess risk; and 5) Apply OPSEC measures. Although these steps are normally applied in a sequential manner during deliberate or crisis action planning, dynamic situations may require any step to be revisited at any time.

2.2. Identify Critical Information:

2.2.1. Critical information is specific facts 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. OPSEC indicators are friendly detectable actions and open-source information that can be collected, interpreted or pieced together by an adversary to derive critical information. The product of the first step in the OPSEC process is a Critical Information List (CIL).

2.2.2. Critical information is best identified by the individuals responsible for the planning and execution of the unit's mission. An OWG 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.

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

2.3. Analyze Threats:

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

2.3.2. The primary sources to obtain threat information are your local intelligence and counterintelligence organizations.

2.3.3. 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.

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

2.4. Analyze Vulnerabilities:

2.4.1. An OPSEC vulnerability is a condition where friendly actions provide indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective adversary decision-making. The OWG or staff planning team must conduct the vulnerability analysis based on operational planning and current operating environment.

2.5. Assess Risk:

2.5.1. An OPSEC risk is a measure of the potential degree to which critical information and indicators are subject to loss through adversary exploitation. The OWG or staff planning team must conduct the OPSEC risk assessment and develop recommended OPSEC measures based on operational planning and current operating environment. A typical risk assessment will:

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

2.5.1.2. Determine potential OPSEC measures to reduce vulnerabilities with the highest risk. The most desirable OPSEC measures are those that combine the highest possible protection with the least adverse effect on operational effectiveness.

2.6. Apply OPSEC Measures:

2.6.1. OPSEC measures are the methods and means to gain and maintain essential protection of critical information. OPSEC measures may be both offensive and defensive in nature.

2.6.2. Potential OPSEC measures, among other actions are, cover, concealment, camouflage, deception, intentional deviations from normal patterns, and direct strikes against adversary collection.

2.6.3. The OWG or staff planning team will submit recommended OPSEC measures for commander approval through the operational planning process for employment.

2.6.4. OPSEC measures 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 OPSEC measures do not become unacceptable indicators themselves.

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

Chapter 3

OPSEC PLANNING

3.1. General. This chapter provides direction for planners at wings and AOCs 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 will assist unit planners to incorporate protection of critical information and indicators into supported OPLANS and supporting plans. They will also assist exercise planners in developing master scenario events listings (MSEL) and MOPs to train unit personnel in the application or execution of OPSEC measures (See AFDD 2, *Operations and Organizations,* for more information concerning MOPs and measures of effectiveness (MOE)s).

3.2. Operational Planning. OPSEC will be included in force presentation and deliberate and crisis action planning and execution segment (DCAPES) for the planning, deployment, employment, sustainment, redeployment and reconstitution of forces. DCAPES supports all phases of operations development and execution at the strategic, operational, and tactical levels. OPSEC will be included in all operational plans (OPLANs), concept plans (CONPLANs), functional plans (FUNCPLANs), and operation orders (OPORDS). 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. Threat(s) and vulnerability assessments will be used to identify applicable OPSEC measures to mitigate any unacceptable operational risks. MOP and MOE will be developed for each OPSEC measure.

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

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 scenarios will be included in the exercise MSELs with MOPs to assess the proficiency of functional planners to mitigate loss of critical information and unit personnel to execute OPSEC measures. Any deficiencies or best practices will be submitted to the AF lessons learned database (**https://afknowledge.langley.af.mil/afcks/**) and used to develop TIPs IAW AFI 10-204 and AFI 11-260.

3.4.1. OPSEC measures will also be employed during the exercise to minimize observation 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 AWARENESS EDUCATION AND TRAINING

4.1. 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 recurring annual OPSEC training. Standardized AF OPSEC awareness training located on the AF Advanced Distance Learning System (ADLS) is the baseline training required for all personnel. Unit 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, coordinators, and planners assigned to OPSEC positions require more in-depth training designed to ensure proper management, planning, and execution of organizational OPSEC programs.

4.2. All Personnel:

4.2.1. Awareness education will be provided to personnel upon initial entrance/accession into military service.

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

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

4.2.4. When government-provided OPSEC training is required by a contract, OPSEC PMs and/or OPSEC coordinators will provide OPSEC training or training materials to contract employees within 90 days of employees' initial assignment to the contract.

4.2.5. Unit OPSEC coordinators will track initial and annual awareness training and report training initiatives in their annual OPSEC self-assessment reports to their respective HHQ OPSEC PM. Wing, MAJCOM, FOA, and DRU OPSEC PMs are responsible for the tracking of command/wing staff personnel training initiatives.

4.3. OPSEC Program Managers, Coordinators, and Planners:

4.3.1. OPSEC Orientation Training. Personnel assigned as an OPSEC PM, coordinator, planner, or vulnerability assessment team member are required to complete OPSEC orientation training. Once developed, approved and deployed, the Air Force's OPSEC orientation training course will be the primary method used to satisfy this requirement. Until then, the Interagency OPSEC Support Staff's (IOSS) OPSE-1301 CBT course is the accepted method for completing OPSEC orientation training. Additionally, OPSEC training can be received from HHQ OPSEC PM. Training must be completed within 30 days of assignment to OPSEC duties.

4.3.2. Formal OPSEC training. Formal OPSEC training is required for all OPSEC PMs, planners assigned to OPSEC positions and those who conduct formal OPSEC surveys.

4.3.2.1. Training must be completed within 90 days of appointment through the next available Air Force Signature Management Course; IOSS OPSE-2500, OPSEC Analysis and Program Management Course; or OPSEC-2400, DOD OPSEC Course. The Air Force course is the preferred method.

4.3.2.1.1. If training cannot be obtained within 90 days of appointment, units must submit a request for waiver to AF/A3O-CI, through their HHQ OPSEC PM justifying an extension to the 90 day requirement. Waivers must contain confirmation that individual is scheduled for next available training course. Because training of traditional AF Reservists and ANG personnel differs from active duty Air Force, traditional AF Reservist and ANG personnel will be granted automatic waivers.

4.3.2.2. Wing, center and installation commanders will program unit funds for training attendance, however MAJCOM Military Deception program managers may fund MAJCOM training quotas. Request for training will be submitted through the wing OPSEC PM to their respective HHQ OPSEC PM.

4.3.3. Mission Readiness Training (MRT). Personnel working in the AOC require MRT that encompasses initial qualification training (IQT), mission qualification training (MQT), and continuation training (CT). IQT will consist of formal training and mission specific on the job training. 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.

Chapter 5

OPSEC ASSESSMENTS

5.1. General:

5.1.1. Assessments are performed to achieve two specific purposes: to provide information and data into the OPSEC risk analysis process and to gauge the overall effectiveness of the program (See **Table 5.1.** for OPSEC assessment types).

5.1.2. The Air Force provides several tools to assist OPSEC PMs, 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 protective measures which can mitigate or negate risk to operations.

5.1.3. Assessment of program effectiveness is accomplished through the development of MOP and MOE. MOPs are developed to assess the proficiency of unit personnel to protect critical information through the execution of OPSEC measures. Any deficiencies or best practices identified are documented in lessons learned and TIPs. IG inspections are also used to assess unit compliance, operational readiness, and nuclear surety. Submit TIPs IAW AFI 11-260.

5.1.4. OPSEC PMs will request external assessments via their respective HHQ OPSEC PMs.

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

5.2. OPSEC Program Self-Assessment:

5.2.1. Self-assessments are continual processes that involve combining data collected from MOP, MOE, exercise after action reports (AARs), lessons learned, nuclear surety, operational readiness/compliance inspections, and annually conducted self-assessments/self-inspections. This data is reported annually as a self-assessment report to the HHQ OPSEC PM and is outlined in **Attachment 2**.

5.2.2. OPSEC PMs and coordinators will conduct annual self-assessments to ensure the health of their program, evaluate compliance with applicable policies and to identify short-falls and vulnerabilities. **Attachment 3** contains a sample self-assessment checklist that can be modified for specific unit/activity needs. This data will be reported annually as outlined in **Attachment 2**.

5.3. Staff Assistance Visit (SAV):

5.3.1. SAVs may be conducted periodically by HHQ OPSEC PMs or other organization subject matter experts (SME) to assist units in repairing dormant, non-compliant, deficient programs or for any other reason deemed necessary by the commander. The unit 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/coordinators as required.

5.4. Survey:

5.4.1. An OPSEC survey is a collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function in light of the known collection capabilities of potential adversaries.

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

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

5.5. Support Capabilities:

5.5.1. Electronic Systems Security Assessment (ESSA) involves the collection and analysis of information transmitted via unsecured and unprotected communications systems (telephone, email, radio, web sites) to determine if these systems are being used to transmit critical, sensitive or classified information. ESSA helps in evaluating an organization's OPSEC posture and determine the amounts and types of information available to adversary collection entities. ESSA is accomplished only within certain legal parameters and may only be performed by authorized personnel.

5.5.2. Multi-Disciplinary Vulnerability Assessments (MDVA) are assessments combining network security, physical security, HUMINT, and ESSA. MDVAs are conducted to identify operations vulnerabilities, operational impacts, and exercise threat response procedures.

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

5.5.4. 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 is provided to assist in the performance of OPSEC risk assessments for blue forces to develop OPSEC measures to counter the threat based on vulnerabilities identified.

5.5.5. Field organizations will request support through their HHQ OPSEC PM to their respective MAJCOM OPSEC PM. MAJCOM OPSEC PMs will submit ESSA and MDVA requests to HQ ACC/A3I; HVA requests should be submitted IAW procedures of your local AFOSI detachment.

5.6. Annual Assessment Reporting:

5.6.1. Detailed results of OPSEC assessments conducted throughout the year are reported on an annual basis IAW **Chapter 1**; see **Attachment 2** for further guidance.

5.6.2. 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 it will be signed by the commander or their designated representative.

Table 5.1. OPSEC Assessment Types and Support Capabilities

Assessment Type	Purpose	Methodology	Frequency	Request Procedures	Reporting
Program Self-Assessment	-Program health -Policy compliance -Shortfalls	OPSEC PMs and coordinators evaluate the health of OPSEC programs, evaluate compliance with applicable policies and identify vulnerabilities	Annual	N/A	OPSEC PM/ coordinator reports to organization CC and up channel to HHQ PM
SAV	- Policy compliance - Shortfalls - Provide guidance	OPSEC PMs assess subordinate organizations (if collocated)	As requested or required	N/A	Report to subordinate organization CC and OPSEC PM or coordinator
OPSEC Survey	Assess organization's ability to apply the OPSEC methodology to operations.	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
ESSA	ID potential vulnerabilities	Collect and analyze communications	As requested or required	Organization CC requests through HHQ PM	Report to requesting organization
Multi-Disciplinary Vulnerability Assessment (MDVA)	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	Installation CC requests through MAJCOM OPSEC PM	Out-brief & report to installation CC

Chapter 6

AIR FORCE OPSEC ANNUAL AWARDS PROGRAM

6.1. General:

6.1.1. 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 award winners will be forwarded to compete for the IOSS National OPSEC Awards.

6.1.2. Air Force organizations wishing to compete for AF OPSEC annual awards must submit nominations through their respective MAJCOMs to reach AF/A3O-CI, NLT 31 Oct each year.

6.1.3. 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 its MAJCOM to reach AF/A3O-CI, NLT 15 November to meet the IOSS suspense. Go to **http://www.ioss.gov** for further descriptions of the awards and nomination criteria.

6.1.4. Policy and guidance for AF OPSEC awards are listed in AFI 36-2807, Chapter 12, *Headquarters United States Air Force Deputy Chief of Staff Operations, Plans and Requirements Annual Awards Program.*

CARROL H. CHANDLER, Lt Gen, USAF
DCS, Air Space and Information Operations, Plans and Requirements

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

National Security Decision Directive (NSDD) No. 298, *National Operations Security Program, 22 January 1988*

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

DODD 5230.9, *Clearance of DOD Information for Public Release, 9 April 1996*

DODR 5400.7/*AF Sup, Freedom of Information Act (FOIA), 24 June 2002*

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*

AFDD 2, *Operations and Organizations, 3 April, 2007*

AFDD 2-5, *Information Operations, 11 January 2005*

AFTTP 3-1.36, *IO Planning, Integration, and Employment Considerations (U), 1 June 2006*

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

AFJI 31-102, *Physical Security, 31 May 1991*

AFPD 31-4/AFI 31-401, *Information Security, 1 September 1998/1 November 2005*

AFPD 31-5/AFI 31-501, *Personnel Security* 1 August 1995/27 January 2005

AFPD 31-6, *Industrial Security, 1 April 2000*

AFPD 33-2, *Information Assurance (IA) Program, 19 April 2007*

AFPD 63-17, *Technology and Acquisition Systems Security Program Protection, 26 November 2001*

AFMAN 37-123, (will convert to 33-363) *Management of Records, 31 August 1994*

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

AFI 10-208, *Continuity of Operations (COOP) Program, 1 December 2005*

AFI 10-245, *Anti-Terrorism/Force Protection Program, 21 June 2002*

AFI 10-401, *Air Force Operations Planning and Execution, 7 December 2006*

AFI 10-403, *Deployment Planning and Execution, 5 August 2005*

AFI 10-404, *Base Support and Expeditionary Site Planning, 9 March 2004*

AFI 10-704, *Military Deception Program, 30 August 2005*

AFI 10-710, *Information Operations Condition (INFOCON), 10 August 2006*

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

AFI 13-1AOCv3, *Operational Procedures – Air and Space Operations Center (AOC), 1 August 2005*

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

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

AFI 31-601, *Industrial Security Program Management, 29 June 2005*

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

AFI 33-129, *Web Management and Internet Use, 3 February 2005*

AFI 33-202, Vole I, *Network and Computer Security, 3 February 2006*

AFI 33-203, Vole 1, *Emissions Security, 31 October 2005*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP), 1 May 2006*

AFI 33-332, *Privacy Act Program, 29 January 2004*

AFI 35-101, Chapter 15 and 18, *Public Affairs Policies and Procedures, 29 November 2005*

AFI 38-101, *Air Force Organization, 4 April 2006*

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

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

AFPAM 14-118, *Aerospace Intelligence Preparation of the Battlespace, 5 June 2001*

Abbreviations and Acronyms

AFOSI—Air Force Office of Special Investigations

AOC—Air and Space Operations Center

CAF—Combat Air Forces

CI—Counterintelligence

CIL—Critical Information List

DCAPES—Deliberate and Crisis Action Planning and Execution Segment

DOD—Department of Defense

DODD—Department of Defense Directive

FAA—Functional Area Analysis

FNA—Functional Needs Analysis

FSA—Functional Solutions Analysis

HHQ—Higher Headquarters

HUMINT—Human Intelligence

IFO—Influence Operations

IG—Inspector General

IO—Information Operation

MAF—Mobility Air Forces

MOE—Measures of Effectiveness

MOP—Measures of Performance

OPSEC—Operations Security

OWG—Operations Security Working Group

PA—Public Affairs

PM—Program Manager

RDT&E—Research, Development, Test and Evaluation

SEI—Special Experience Identifier

TIP—Tactics Improvement Proposal

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.

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, or foreign persons, or international terrorist activities.

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.

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

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 evaluation of the organization's compliance with OPSEC plans and programs and appraises the OPSEC posture. Commanders may choose to conduct assessments with a small team of experts from within the organization. This team at a minimum should be composed of the OPSEC Program Manager, a representative from each security discipline and at least one representative from the operations and intelligence staff sections.

OPSEC Coordinator—Acts as an interface to direct and manage all relevant OPSEC matters below the wing-level and reports to the wing-level 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—Anything, which effectively negates or mitigates an adversary's ability to exploit vulnerabilities.

OPSEC Program Manager—Focal point for all OPSEC related matters at the wing-level or higher. Ensures OPSEC requirements are in compliance as directed and reviews operations plans to ensure OPSEC is appropriately considered.

OPSEC Planner—Planners conduct OPSEC planning for AOCs.

OPSEC Survey—An OPSEC survey is a collection effort by a team of subject matter experts to reproduce the intelligence image projected by a specific operation or function in light of the known collection capabilities of potential adversaries.

OPSEC Working Group—A (normally formal) designated body representing a broad range of line and staff activities within an organization that provides OPSEC advice and support to leadership and all elements of the organization.

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—An OPSEC process of evaluating the risks of information loss based on an analysis of threats to, and vulnerabilities of, a system, operation or activity.

Sensitive Information—Information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (NSTISSI 1997).

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—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.

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—An evaluation (assessment) to determine the vulnerability of an installation's application of influence operations and security processes to determine specific vulnerabilities. Identifies areas of improvement to withstand, mitigate, or deter acts of violence, terrorism, sabotage or espionage.

Attachment 2

ANNUAL OPSEC PROGRAM REPORT

NOTE: Annual reports will provide information relating to the following areas:

A2.1. Executive Summary: Full-time OPSEC PM appointed, budget plan developed, level of importance within the organization.

A2.2. OPSEC Initiatives/Projects/Successes: How is the commander making OPSEC a priority? (Policy and guidance, web site reviews, etc.)

A2.3. OPSEC Training and Awareness: How is OPSEC awareness education and training conducted in the organization? (Commander's call, unit newsletter, incorporating OPSEC into exercises)

A2.4. 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)

A2.5. Assessment: What has the organization done to determine the overall effectiveness of the unit's OPSEC program? (i.e., surveys, exercises, measures of effectiveness for implemented OPSEC measures, nuclear surety, operational readiness, and compliance inspections)

SAMPLE REPORT

1 October 2006

MEMORANDUM FOR AF/A3O-CI

FROM: ABCD/CV
69 KY Street
Randolph AFB TX 78150

SUBJECT: HQ ABCD Annual OPSEC Program Report (1 October 2005 – 30 September 2006)

The following is the consolidated annual OPSEC program report which includes input from the 12 FTW, 14 FTW, 17 TRW, 47 FTW, 56 FW, 59 MDW, 81 TRW, 82 TRW, 97 AMW, 149 FW, 325 FW, and 16 SOW. **NOTE**: *This sample report is an accumulation of information provided by AETC and AFSOC as an example of the type of information and structure required within the Annual OPSEC Program Report.*

1. Executive Summary

A full-time OPSEC Program Manager (PM) is assigned at the command-level and two full-time PMs assigned at the 16th Special Operations Wing (SOW). Each HQ directorate and organization under wing-level has a primary and alternate OPSEC Coordinator assigned as additional duty.

Funding for the command's OPSEC program has been requested through normal POM channels and through the command's FY10-35 Strategic Planning process (CAD, FSA, FAA and FNA). To date, none of these efforts have resulted in any significant funding. The command received some funding from HQ AF for FY06, but the late release (May 06) of funds greatly impacted spending. Additional travel funding is provided from AFSOC/A3, but neither Information Operation (IO) nor OPSEC has a dedicated funding line. The wing receives approximately $15K from the wing commander to operate its Information Operations Office of which the OPSEC program is part.

2. OPSEC Initiatives/Projects/Successes:

a. AETC/A3 assigned new command OPSEC PM, to replace former contractors. AETC is conducting a course resource estimate for the future OPSEC manager formal course, results expected in Dec.

b. The following initiatives are ongoing at AETC and AFSOC Wings:

(1) The 12 FTW developed and implemented Wing OPSEC Computer Based Training tailored to each unit insuring high training rates; CC approved new CIL; scrutinized exercise OPSEC vulnerabilities, led to weakness identification and fix. Wing OPSEC training at 97%; Wing OPSEC training conducted monthly; OPSEC managers formally trained.

(2) The 14 FTW units conduct monthly web pages reviews and reports to Wing PM; Annual OPSEC conducted by unit CC call primarily; Wing PM conducts initial OPSEC training to all newcomers. OPSEC measures included in all wing plans; OPSEC procedures reviewed during exercises; surveys completed by unit personnel annually

(3) The 17 TRW appointed two GS employees to serve as OPSEC PMs in hopes of continuity and future experience base; OPSEC focused on roles and responsibilities through quarterly XP newsletter; Initial training conducted through newcomers process, annual training conducted across wing by 28 Feb; Wing PM reviewed all wing web pages for OPSEC indicators; reduced deployment indicators by changing deployment line process.

(4) The 47 FTW maintains a robust webpage with many links to program guidance and related information; established an OPSEC library to centralize available media materials; OPSEC awareness is given at newcomers; tailored initial and annual training conducted by each unit; Plans are assessed during the review cycle ensuring OPSEC principles implemented/included; Self assessment and random observations employed to gauge program effectiveness.

(5) The 56 FW CC signed new policy letter stressing OPSEC practice for mission effectiveness; updated CIL to include BRAC issues; MDVA scheduled, was not accomplished due to manning/funding issues; PM are active members of TWG, Readiness Review Board, and Battle Staff, able to make OPSEC a priority consideration for security driven decisions; Approximately 12 Battle Staff Directives addressing OPSEC awareness to all personnel; Final OPSEC review of all plans conducted prior to signature; Gathered threat information from OSI, and assisted security forces conducting Anti-Terrorism base vulnerability assessment.

(6) The 59 MDW requested/received survey from DOD Joint Information Operations Center, results pending; Partnered with 37 TRW OPSEC PM to align programs and initiatives; Used wing newsletter to publish OPSEC indicators, threat, and countermeasures awareness; All PMs formally trained; Initial and Annual training accomplished across wing utilizing group level CC calls; No OPSEC findings reported from ORI.

(7) The 81 TRW significantly modified training program after Hurricane Katrina and AFI 10-701, utilizing newcomers and First Term Airman's Center awareness training and commander's calls; Developing a Computer Based Training module to further assist initial and annual training objectives; Developed "OPSEC Guide for the Family" to assist family awareness and protection; Developing intranet

one stop shop for all Unit OPSEC Coordinators' needs; IOSS products have been made available for training; Newcomers OPSEC training is this year's most successful program.

(8) The 82 TRW formalized program management with new PM appointment. A wing CIL has been accomplished; Wing PM accomplishes weekly vulnerability spot inspections on random units, attempting to gather critical information from unit based on that units CIL and reports vulnerabilities to unit commander; OPSEC awareness incorporated into First Term Airmen Center Program and Base Newcomers Briefing; All base plans reviewed for OPSEC indicators and vulnerabilities; Wing SAVs conducted at all group/squadron programs by wing OPSEC PM.

(9) The 97 AMW underwent a Vulnerability Assessment by HQ AETC Team 1-4 May 2006. Concluding findings are: Altus OPSEC program "exceeds DOD standards"; CIL established and monitored; Suspicious requests for mission or personal information are being forwarded to AFOSI; Recommendation-continue on course. The 97 AMW successfully accomplished 100% annual training reports; conducts initial training through in-processing; Reviews and monitors all media releases for OPSEC indicators; Commanders are aware and supportive of OPSEC focus; OPSEC slide provided in weekly wing staff meetings; OPSEC reviews conducted in all base-level exercises.

(10) The 149 FW requested and received assistance from AFWIC conducting aggressor operations against the wing: Vulnerabilities and corrective initiatives briefed to commanders; Updated awareness training implemented within quarterly "Commander's Newcomer Briefing"; Annual training is provided during Aug 06 UTA mass briefing to the 149 FW: OPSEC refresher briefing airs on closed circuit network at varying times during UTA weekends.

(11) The 325 FW OPSEC PM attends meetings of the Regional Domestic Security Task Force sharing in OPSEC/threats/intelligence/criminal and terrorist information with local authorities; Conducts OPSEC WG periodically; Maintains OPSEC library resource; Developed OPSEC familiarization course with hotlinks and placed it on the installation intranet; PM and Plans officer are same; All plans are developed and reviewed from OPSEC perspective; Conducted surveys and exercises to observe and monitor OPSEC; conducted annual OPSEC vulnerability assessment and briefed vulnerabilities to senior leadership.

(12) The command PM worked with the newly formed Electronic Systems Security Assessment Center (ESSAC) – Special Operations Forces (SOF) to integrate their OPSEC supporting capabilities into the command's operations. This has resulted in an operation-level impact with senior leadership on the importance of practicing good OPSEC and COMSEC at all times. ESSA-SOF has become the AF lead in developing and testing new applications, resources, equipment and methods for the ESSA community in supporting operational-level OPSEC.

3. OPSEC Training and Awareness:

a. AETC has turned to IOSS for training some of our wing level program managers. All wing PMs, except one newly assigned, have been formally trained. Command PM has not been formally trained at this time.

b. OPSEC articles have been written for base newspapers and TV networks to promote OPSEC awareness at all AETC wings bases.

c. Both the command and wing PMs have developed an AF Knowledge Now, Community of Practice (CoP) to provide PMs and Coordinators a one-stop-shop for threat information, alerts, general news, training materials and opportunities, and other reference materials.

d. Created and published AFSOCI 10-701, *Operations Security* and the AFSOC OPSEC Plan to provide guidance for the command's PMs and Coordinators.

e. Initial OPSEC training is conducted bi-monthly for first-term airman at the Commando Airman's Pride Center. This briefing is designed to introduce airman to the world of OPSEC and Special Operations.

4. OPSEC in Operational Planning:

a. Wing OPSEC PMs reviewed all base program plans, exercise plans and deployment plans for OPSEC considerations. Most OPSEC PMs in AETC are also Wing XP personnel monitoring plans from conception through execution with an OPSEC perspective.

b. OPSEC Working Groups conducted at all Wings to ensure OPSEC is incorporated into all base activities. Lessons learned from exercises were briefed to unit OPSEC Managers during workings groups.

c. The 16 SOW OPSEC PMs have developed a functional access database that analyzes mission critical areas, and generates a vulnerability assessment report for planning purposes. Vulnerabilities are assessed on a numerical scale 1-5, to determine risks associated with various phases of wing operations. Significant areas are highlighted and briefed to wing leadership for countermeasure execution to mitigate any associated OPSEC risks.

d. Both the command and wing review information for publication on the web, AF Portal, the base newspaper, and other periodicals.

5. Assessment:

a. HQ AETC OPSEC Program Manager conducted no formal Staff Assistance Visits (SAVs), due to funding and manpower.

b. Multidisciplinary Vulnerability Assessment (MDVA) was planned for 56 FW at Luke AFB AZ, but was cancelled due to limited resources and BRAC related issues.

c. HQ IG Inspections were conducted on OPSEC programs at the 17 TRW, 97 AMW, 59MDW, 12 FTW, and 82 TRW, with no significant findings.

d. Transforming the OPSEC mindset from awareness to process and execution will be the program emphasis for FY07

e. The 92 IWAS conducted an OPSEC survey for the 16 SOW on the base's deployment plan. The outside look enabled the wing to correct vulnerabilities and indicators that were present.

f. The 16 SOW PMs are members of the Hurlburt Exercise and Evaluation Team (HEET), allowing them to incorporate OPSEC into the wing IG exercises and to inspect for compliance

g. The wing OPSEC PMs have integrated themselves into the Force Protection, Anti-Terrorism, Intelligence and AFOSI Counterintelligence communities allowing them to not only provide OPSEC support to these areas, but facilitating an interface between these communities to better support OPSEC efforts for the wing.

MARK O. POLO, Maj Gen, USAF
Vice Commander

Attachment 3

SAMPLE OPSEC SELF-ASSESSMENT CHECKLIST

NOTE: This is only an example to be used to develop your own inspection checklists based on your particular organizational level and/or OPSEC requirements IAW this instruction.

1 – Organizations Below Wing-Level				
ITEM	**YES**	**NO**	**NA**	**REMARKS**
1. Has a primary and alternate OPSEC coordinator been appointed in writing? (AFI 10-701, Para **1.4.15.** and **1.4.17.**)				
2. Has the commander signed and issued unit policy and a critical information list? (AFI 10-701, Para **1.4.15.1.**)				
3. Is the policy periodically reviewed for currency and updated as necessary? (AFI 10-701, Para **1.4.17.5.**)				
4. Are procedures to control critical information and indicators in place? (AFI 10-701, Para **1.4.17.5.**)				
5. Is OPSEC integrated into organizational plans, exercises and activities? (AFI 10-701, Para **1.4.17.4.**)				
6. Is there an awareness and training program in place? (AFI 10-701, Para **1.4.17.11.**)				
7. Are all newly assigned personnel trained upon arrival as part of unit in-processing? (AFI 10-701, Para **1.4.17.11.**)				
8. Do all personnel receive awareness training annually? (AFI 10-701, Para **1.4.17.11.**)				
9. Does the OPSEC coordinator have a secret clearance and access to NIPRNET and organizational email accounts? (AFI 10-701, Para **1.4.17.1.**)				
10. Does the OPSEC coordinator provide guidance and ensure OPSEC reviews are conducted on all unit web pages? (AFI 10-701, Para **1.4.17.9.**)				
11. Has an annual OPSEC self-assessment been conducted for the FY period (1 Oct-30 Sep) and results forwarded to HHQ OPSEC PM? (AFI 10-701, Para **1.4.17.12.**)				

2 – Wing-Level Organizations NOTE: Operational Planning Staff list also applies.				
ITEM	**YES**	**NO**	**NA**	**REMARKS**
1. Has a Primary and alternate wing OPSEC PM been appointed in writing? (AFI 10-701, Para **1.4.15.2.**)				
2. Has the commander established and signed OPSEC command policy, guidance and a critical information list? (AFI 10-701, Para **1.4.15.1.**)				
3. Are OWGs established and meet periodically (AFI 10-701, Para **1.4.15.6.**)				
4. Have all OWG members been trained? (AFI 10-701, Para **1.4.16.11.**)				
5. Is senior leadership actively involved in the OPSEC program? (AFI 10-701, Para **1.4.15.1.**)				
6. Have coordinators been assigned in writing IAW with command policy? (AFI 10-701, Para **1.4.15.2.**)				
7. Does OPSEC PM assist PA officer to ensure OPSEC considerations are included in PA reviews of info released to the public? (AFI 10-701, Para **1.4.16.10.**)				
8. Are procedures in place to control critical information and indicators? (AFI 10-701, Para **1.4.16.8.**)				
9. Does OPSEC PM have a SIPRNET, NIPRNET and access to organizational email accounts? (AFI 10-701, Para **1.4.16.3.**)				
10. Does the OPSEC PM have a budget plan? (AFI 10-701, Para **1.4.7.11.**)				
11. Are all newly assigned personnel trained upon arrival as part of unit in-processing? (AFI 10-701, Para **1.4.17.11.**)				
12. Has a copy of the last annual self-assessment been sent to the MAJCOM OPSEC PM? (AFI 10-701, Para **1.4.16.13.**)				

3 - Operational Planning Staff				
ITEM	**YES**	**NO**	**NA**	**REMARKS**
1. Is training provided and documented for newly assigned personnel upon assignment to planning staff? (AFI 10-701, Para **4.3.1.**)				
2. Are OPSEC principles integrated into all operational, support, exercise, crisis action and acquisition plans? (AFI 10-701, Para **3.1.**)				
3. Are critical information and OPSEC indicators identified from all functional areas requiring protection? (AFI 10-701, Para **3.2.**)				
4. Are OPSEC measures implemented to correct vulnerabilities? (AFI 10-701, Para **3.2.**)				

4 – MAJCOM-Level Organizations **NOTE: Organizational Planning Staff list also applies.**				
ITEM	**YES**	**NO**	**NA**	**REMARKS**
1. Has a full-time MAJCOM OPSEC PM position been established? (AFI 10-701, Para **1.4.7.3.**)				
2. Has the commander established and signed command policy and guidance? (AFI 10-701, Para **1.4.7.1.**)				
3. Has AF policy and guidance been implemented throughout the command? (AFI 10-701, Para **1.4.7.1.**)				
4. Are all newly assigned OPSEC personnel trained upon assignment? (AFI 10-701, Para **1.4.7.13.**)				
5. Are OPSEC measures implemented to correct vulnerabilities? (AFI 10-701, Para **1.4.17.7.**)				
6. Does the OPSEC PM chair and periodically convene an OWG? (AFI 10-701, Para **1.4.16.4.**)				
7. Have OPSEC requirements been consolidated/ submitted to AF IO requirements and analysis working group for inclusion in AF IO Capabilities Plan? (AFI 10-701, Para **1.4.7.6.**)				
8. Have funds been programmed through the established budget and requirements process? (AFI 10-701, Para **1.4.7.11.**)				
9. Has a copy of the last annual self-assessment been sent to AF OPSEC PM? (AFI 10-701, Para **1.4.7.19.**)				
10. Is a copy of the last annual report on hand? (AFI 10-701, Para **1.4.16.13.**)				
11. Are plans reviewed periodically for currency and updated when required? (AFI 10-701, Para **3.1.**)				

5. AF-Level				
ITEM	YES	NO	NA	REMARKS
1. Has an AF OPSEC PM been appointed? (DODD 5205.02, Para 5.3.1.1)				
2. Has the Commander established and signed AF policy? (DODD 5205.02, Para 5.3.1)				
3. Has the Commander's policy been distributed to the Air Force? (DODD 5205.02, Para 5.3.1)				
4. Have funds been programmed through the established budget and requirements processes? (DODD 5205.02, Para 5.3.1)				
5. Are all newly assigned personnel trained? (AFI 10-701, Para 4.2.)				
6. Have support capabilities been established to provide for? (DODD 5205.02, Para 5.3.1.2):				
6.1. Program Development				
6.2. Program Planning				
6.3. Operational Planning				
6.4. Training				
6.5. Assessment and survey capabilities				
6.6. Readiness training				
7. Has an annual review of the AF OPSEC program been accomplished and submitted to USD(I)? (DODD 5205.02, Para 5.3.1.4)				
8. Are procedures in place for conduct of OPSEC surveys every three years? (DODD 5205.02, Para 5.3.1.5)				
9. Has support been provided to other DOD OPSEC program as needed? (DODD 5205.02, Para 5.3.1.6)				
10. Has guidance been issued regarding the techniques, training and procedures for conducting vulnerability assessments and OPSEC surveys? (DODD 5205.02, Para 5.3.2)				

5. AF-Level				
ITEM	**YES**	**NO**	**NA**	**REMARKS**
11. Is OPSEC integrated into the every day mission activities? (DODD 5205.02, Para 5.3.3)				
12. Is critical information identified and updated as missions change? (DODD 5205.02, Para 5.3.4)				
13. Are appropriate levels of OPSEC training established and provided? (DODD 5205.02, Para 5.3.5)				
14. Are AF OPSEC forces aligned with the AF IO Career Force? (AFI 10-701, Para **1.4.2.1.1.**)				
15. Has guidance been provided to ensure government contract requirements properly reflect OPSEC responsibilities? (AFI 10-701, Para **1.4.2.7.**)				