

**BY ORDER OF THE COMMANDER
70TH INTELLIGENCE SURVEILLANCE
AND RECONNAISSANCE WING**

**70TH INTELLIGENCE SURVEILLANCE
AND RECONNAISSANCE WING
INSTRUCTION 31-401**



26 AUGUST 2014

Intelligence

70 ISR WING SECURITY PROGRAM

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: 70 ISRW/SO

Certified by: 70 ISRW/CC
(Col Kevin D. Dixon)

Pages: 18

This publication establishes the policies, procedures, and responsibilities that will promote the proper training, classification, and safeguarding of information and personnel within 70 ISRW that are vital to national security and allows for the continuous evaluation of unit personnel for trustworthiness and reliability. All 70 ISRW personnel must be familiar with and adhere to the policies listed in this instruction. Air Force units/organizations who are tenants within 70 ISRW buildings/installations must also be familiar with these policies. These policies implement and extend the requirements of the following Air Force Instructions: AFI 10-245, *Antiterrorism (AT)*; AFI 31-101, *Integrated Defense*; AFI 31-401, *Information Security Program Management*; AFI 31-501, *Personnel Security Program Management*; AFI 31-601, *Industrial Security Program Management*; AFI 10-701 *Operations Security*, ICD 705, *Sensitive Compartmented Information Facilities*.

Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional's chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>. Additionally, if your publication generates a report(s), alert readers in a statement and cite all applicable Reports Control Numbers in accordance with AFI 33-324.

(Applicability) This publication applies to all 70 ISRW units and personnel. This also applies to attached ANG and Reserve units and personnel. This does not apply to non-70 ISRW personnel that are not operationally or administratively attached to 70 ISRW.

1.	Responsibilities	2
2.	Protecting Classified Information	7
3.	Creation/Reproduction of Classified Information	9
4.	Antiterrorism (AT)	11
5.	Operations Security	12
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		16

1. Responsibilities

1.1. Each Group, Squadron, and Detachment Commander will appoint in writing a primary and alternate unit security manager (SM)/Security Representative (SR) [or Special Security Officer (SSO)], to ensure compliance with security directives for the protection of classified material per *AFI 31-401*.

1.2. Wing Security Officer (SO) will:

1.2.1. Be appointed in writing by the Wing Commander or their direct representative.

1.2.2. Be the primary point of contact within the Wing for all security matters relating to Personnel, Industrial, Physical, Antiterrorism and Information Security.

1.2.3. Develop and update Wing security operating instructions.

1.2.4. Advise Wing leadership on security issues pertaining to the Wing.

1.2.5. Work with Group Information Security Program Manager (ISPM)/Special Security Officers (SSOs) to ensure security guidance, policies and instructions are properly implemented and enforced.

1.2.6. Oversee the Wing Security Self-Inspection Program.

1.2.7. Assist the Wing and Group Commanders and Group ISPMs in monitoring security incident investigations.

1.2.8. Liaison with adjacent and higher headquarters and staffs on security issues unique to the Wing.

1.2.9. Coordinate with various Intelligence Community (IC) offices to ensure proper reporting and compliance of various security policies, guidelines and instructions.

1.2.10. Accomplish security tasks assigned by the Wing Commander.

1.2.11. Participate in and hold security education training and antiterrorism awareness training as required based on security training requirements, reviews of security incidents, self-inspections, Consolidated Unit Inspections (CUIs), etc.

- 1.2.12. Serve as Antiterrorism Officer (ATO) for 70 ISRW.
 - 1.2.13. Serve on the local installation Antiterrorism Working Group (ATWG).
 - 1.2.14. Serve on the local installation Threat Working Group (TWG).
 - 1.2.15. Assist the commander in implementing Joint, DoD, Ground Combatant Commander (GCC) and Air Force AT-related doctrine, policy and Tactics, Training and Procedures (TTPs).
 - 1.2.16. Serve on the local post Antiterrorism Executive Committee (ATEC).
 - 1.2.17. Review security incidents that occur to determine adequacy and effectiveness of current local security procedures.
 - 1.2.18. Ensure that additional security disciplines unique to 70 ISRW, such as Operations Security (OPSEC), Communications Security (COMSEC), TEMPEST, Intelligence Oversight (IO) and Information Assurance (IA) are fully incorporated into the Wing's overall Security plan.
 - 1.2.19. Respond to information/data requests from higher headquarters in a timely manner and ensure higher headquarters are kept aware of significant security issues or concerns within 70 ISRW.
- 1.3. Group Special Security Officer (SSO)/Information Security Program Manager (ISPM) will:
- 1.3.1. Be appointed in writing by the Commander.
 - 1.3.2. Be the primary point of contact within respective Group for all security matters relating to Personnel, Industrial, Physical, and Information Security [and Antiterrorism Awareness where applicable].
 - 1.3.3. Develop and update Group security operating instructions to ensure compliance with applicable higher headquarters instructions.
 - 1.3.4. Advise the Group Commander on security issues pertaining to the Group.
 - 1.3.5. Work with Group SSO Program Managers to ensure security guidance, policies and instructions are properly implemented and enforced [if applicable].
 - 1.3.6. Oversee the Group Security Self-Inspection Program and ensure internal semi-annual self-inspections are done by a disinterested party of their respective Programs and of the Group's respective Squadrons (if geographically feasible).
 - 1.3.7. Assist Group and Squadron Commanders in monitoring security incident investigations.
 - 1.3.8. Act as a liaison with Wing SO on security issues unique to the Group.
 - 1.3.9. Accomplish security tasks assigned by the Group Commander.
 - 1.3.10. Participate in and hold security education training, to include hosting ISPM-taught Security, Training, Education, and Motivation meetings (STEM).
 - 1.3.11. Manage Joint Personnel Adjudication System (JPAS) responsibilities within their Group.

- 1.3.12. Assist unit personnel in updating security clearances. Initiate Air Force (AF) Information Management Tool (IMT) 2583, **Request for Personnel Security Action**, to document a local files check, which is a review of locally available medical, personnel and security police records to determine if there is any unfavorable information.
 - 1.3.13. Validate/review change requests to the Unit Manning Document (UMD) relating to the Security Access Requirement (SAR) code.
 - 1.3.14. Brief personnel and maintain AF IMT 2583 in the SSO files on each individual requiring NATO access. Individuals must be debriefed by the Group ISPM (or Squadron Security Manager when the unit is not geographically located with the Group) by completing the AF IMT 2587, **Security Termination Statement**, when access is no longer needed (i.e., permanent change of station (PCS)/ permanent change of assignment (PCA)/temporary duty (TDY) 90 days or more).
 - 1.3.15. Complete AF IMT 2587 for every military or civilian member retiring or separating from the service. Additionally, civilian employees with special access terminating employment for more than 60 days need to complete AF IMT 2587.
 - 1.3.16. Issue courier authorization letters as required.
 - 1.3.17. Maintain documentation identified in Management Internal Control Toolset (MICT) checklists for respective security fields.
 - 1.3.18. Ensure this program governs the protection of classified defense information in the hands of government contractors doing business with the government.
 - 1.3.19. Request and receive visit authorization letters for all industrial contractors working within the unit and provide clearance verifications.
 - 1.3.20. Maintain liaison with all contractors, field representatives and the base industrial security personnel providing security support as required.
 - 1.3.21. Develop, implement and train a local Emergency Protection Plan in conjunction with unit SMs to help ensure site, facility and personnel security after an unplanned event, such as a fire, riot or earthquake.
 - 1.3.22. Ensure that a robust Antiterrorism program is in effect for all Group personnel to include assignment of Squadron ATOs/Antiterrorism Representatives (ATRs) and establishment of individual unit Random Antiterrorism Measures (RAMs) procedures are implemented and reported accordingly.
 - 1.3.23. Respond to information/data requests from higher headquarters in a timely manner and ensure higher headquarters are kept aware of significant security issues or concerns within their respective Group.
- 1.4. Squadron/Site Security Managers (SM) will:
- 1.4.1. Be appointed in writing.
 - 1.4.2. Receive training from the Group ISPM within 90 days of their appointment as Squadron/Site SM.
 - 1.4.3. Notify the Group ISPM in writing of a change in primary or alternate unit SM.

- 1.4.4. Develop and update a unit security operating instruction as required per AFI31-401.
- 1.4.5. Advise the unit commander on security issues pertaining to the unit.
- 1.4.6. Attend the Group ISPM-hosted STEM (if physically collocated with Group SSO, if not, receive material via e-mail from the Group SSO leading STEM training).
- 1.4.7. Update and remind personnel of security policies and procedures.
- 1.4.8. Oversee the unit information security self-inspection program and ensure internal semi-annual self-inspections are done by a disinterested party.
- 1.4.9. Report security incidents to the Group ISPM immediately, but no later than by the end of the first duty day.
- 1.4.10. Assist the unit commander and the Group ISPM in monitoring security incident Investigations.
- 1.4.11. Participate in and hold security education training at the local level on a quarterly basis, training records will be kept for one year to document training accomplished and personnel attending. This training is highly recommended to occur in a classroom environment or during one on one training sessions.
- 1.4.12. Manage JPAS within their organization.
- 1.4.13. Ensure sound physical security procedures are being adhered to, to include documentation of security containers, opening and closing of doors, locking of windows and security containers and logging off computer systems at the end of the work day via the Standard Form (SF) 701 Activity Security Checklist.
 - 1.4.13.1. SF 701s will be maintained for one year after completion for record purposes.
- 1.4.14. Develop a local Emergency Action Plan (EAP) and Emergency Protection Plan (EPP) in conjunction with the Group SSO.
- 1.4.15. Ensure this program governs the protection of classified defense information in the hands of government contractors doing business with the government.
- 1.4.16. Request and receive visit authorization letters for all industrial contractors working within the unit and provide clearance verifications.
- 1.4.17. Maintain liaison with all contractors, field representatives and the base industrial security personnel providing security support as required.
- 1.4.18. Assist unit personnel in updating security clearances.
- 1.4.19. Initiate Air Force (AF) Information Management Tool (IMT) 2583, **Request for Personnel Security Action**, as required; to document a local files check, which is a review of locally available medical, personnel and security police records to determine if there is any unfavorable information.
- 1.4.20. Squadron/Site Security Managers (SMs) are not required if the Group Special Security Office agrees to fulfill all obligations concerning security for the Squadron

Commander in addition to accomplishing all Group SSO functions; although it is recommended for Squadron Commanders to have their own Squadron SM.

1.4.21. Although SSOs can be found at some Squadron-level units, they shall adhere to instructions laid out in this OI to ensure information flow up the 70 ISRW chain of command.

1.4.22. Respond to information/data requests from higher headquarters in a timely manner and ensure higher headquarters are kept aware of significant security issues or concerns within the unit.

1.5. Flight Security Representatives [if applicable] will:

1.5.1. Meet all security requirements for individual unit members (Chapter 2.1).

1.5.2. Be available to assist unit SM in contacting personnel within their respective flights for Periodic Reinvestigation (PR) tracking purposes.

1.5.3. Administer quarterly STEM training to flight members and track their compliance.

1.5.4. Address security issues or concerns within the flight.

1.5.5. Notify unit SM of a projected absence and assign an alternate contact.

1.5.6. Ensure sound physical security procedures are being adhered to, to include documentation of security containers, opening and closing of doors, locking of windows and security containers and logging off computer systems at the end of the work day via the Standard Form (SF) 701 Activity Security Checklist.

1.5.7. Respond to information/data requests from higher headquarters in a timely manner and ensure higher headquarters are kept aware of significant security issues or concerns within their unit.

1.6. Unit Members will:

1.6.1. Know when they are due for their Security Scope Background Investigation-Periodic Reinvestigation (SSBI-PR) [every five years] and meet any suspense assigned by the SM for turning in required paperwork.

1.6.2. Contact the Group SSO to schedule a polygraph when it is due (every five years).

1.6.3. Complete the Electronic Questionnaires for Investigations Processing (EQIP) questionnaire to the best of their ability and take appropriate action when more information is needed (login required within 30 days of EQIP account creation).

1.6.4. Report intent to cohabituate or marry a non-U.S. citizen to the Group SSO.

1.6.5. Participate in security training as required.

1.6.6. Remain vigilant to possible security infractions and report security incidents to the unit SM as soon as they are realized or observed.

1.6.7. Report information which may have an adverse impact on continued security clearance eligibility up their respective security chain of command. Examples include, but are not limited to, adverse involvement with law enforcement agencies, including arrests for driving while under the influence and driving while intoxicated or traffic

violations of \$300.00 or more, credit judgments, Government Travel Card abuse, bankruptcy filing or repossession.

1.6.8. Ensure all foreign travel (official and unofficial) is reported to the member's respective Group SSO prior to departure and after return to ensure proper documentation is maintained of foreign travel.

2. Protecting Classified Information

2.1. Requirements for Access:

2.1.1. Access to classified information can only be given if three parameters are met by the member:

2.1.1.1. All members must have a valid-need-to know the classified material in question.

2.1.1.2. All members must have, at a minimum, the same security clearance annotated on the material(s).

2.1.1.3. All members must be properly trained in the storage and handling of classified materials.

2.2. Storage Requirements:

2.2.1. Classified materials will be received, handled, and stored in accordance with DoD 5200.1-R and AFI 31-401 for all AF owned security containers.

2.2.2. Store all classified material in lockable security containers utilizing X-07/08/09 series electromagnetic locks.

2.2.3. Every security container must have a primary and alternate safe custodian appointed in writing using the SF Form 700, **Security Container Information** (available through the Air Force Publications Distribution system or other like form), for each vault or secure room door and security container, to record the location of the door or container, and the names, home addresses, and home telephone numbers of the individuals who are to be contacted if the door or container is found open and unattended.

2.2.3.1. Applying classification marking to SF 700, Part 1, is not required when separated from Part 2 and 2a.

2.2.3.2. Affix the form to the vault or secure door or to the inside of the locking drawer of the security container. Post SF Form 700 to each individual locking drawer of security container with more than one locking drawer, if they have different access requirements.

2.2.3.3. The SF 700 contains Privacy Act information and must be safeguarded from casual view.

2.2.3.4. When SF Form 700, Part 2, is used to record a security container combination, it must be marked with the highest classification level of material stored in the security container; and stored in a security container other than the one for which it is being used.

2.2.4. Personnel opening/closing containers/vaults or secure rooms will use the Standard Form (SF) 702, **Security Container Check Sheet**, will check the exterior before opening, and interior after opening to determine evidence of forced entry or pilferage. If such evidence is found, the unit SM will be notified immediately. SF 702s will be maintained for one year after form is completely filled out.

2.2.5. If Sensitive Compartmented Information (SCI) material is involved, the Group SSO must be notified.

2.2.6. Combinations to containers/vaults/secure rooms will be changed when personnel with knowledge of the combination PCS, PCA, separate, retire, a compromise has occurred, when an individual no longer requires access but still has access to the area the container is stored in, or when maintenance is performed on the container/safe.

2.2.7. Classified material must be stored separately from unclassified material while in the same security container/safe to reduce the risk of accidental release or disclosure of classified information. Classified material must also be stored separately from funds, drugs, firearms, ammunition or other items of value to discourage theft.

2.2.8. Different levels of classified materials can be stored in the same security container/safe although it must be separated in some fashion to ensure that a user can tell the difference between the different classifications (such as envelopes or cardboard dividers). This will aid in removal of classified material in emergency situations.

2.2.9. Any maintenance conducted on a security container (does not include changing of lock combination) must be documented on a AFTO Form 36, **Maintenance Record for Security Type Equipment**. This document will be affixed to the interior of the container to remain with the container during its lifespan.

2.3. Information Systems Security:

2.3.1. Sharing accounts is not permitted.

2.3.2. Protect your password.

2.3.3. Use the computer screen lock when leaving the area.

2.3.4. Clearly label workstations (both monitors and CPUs) and media the highest classification level of material used on the device with appropriate classification labels "UNCLASSIFIED" (SF 710), "SECRET" (SF 707), "TOP SECRET" (SF 706) and/or "SCI" (SF 712).

2.4. Classified Waste:

2.4.1. Store paper waste that requires protection in a burn bag for destruction, these burn bags should be stored separately from unclassified waste receptacles to avoid the unintentional discarding of materials in the wrong container.

2.4.2. Store partially-filled burn bags in a locked container appropriate for the protection level of the classified material it contains.

2.5. Packaging and Wrapping Responsibilities:

2.5.1. When hand-carrying classified materials between controlled areas, double wrapping is required. The inner wrapper must be an opaque material and marked with

appropriate classification and handling instructions. The outer container must be an opaque material, will not bear classification or caveat markings, and will be labeled or tagged with instructions "Property of the U.S. Government, DO NOT OPEN" if found call: (###) ###-####".

2.5.2. When hand-carrying classified material within a controlled area, double wrapping is not required, but materials should be enclosed in an opaque container.

2.6. Removable Media:

2.6.1. Label all commercial CDs and disks with the following information:

2.6.1.1. Appropriate classification label.

2.6.1.2. Office who created the disc.

2.6.1.3. Phone number of office creating material.

2.6.2. All magnetic media introduced into a Secure Area/SCIF will be properly logged into the SCIF Magnetic Media Log.

2.6.3. Mark all information storage and removable media used to transfer unclassified data to classified systems "Classified" as soon as they are removed from the classified system and handle accordingly.

2.6.3.1. Only personnel whom are properly trained are authorized to transfer media between different classification system (i.e. Unclassified information onto a Classified network or vice versa).

2.7. Coversheets:

2.7.1. Coversheets are placed on top of documents to clearly identify the classification level of the document and protect classified and/or sensitive information for inadvertent exposure.

2.7.2. The coversheet classification forms include "CONFIDENTIAL" (SF 705), "SECRET", (SF 704), TOP SECRET" (SF 705). Although not a classification; sensitive but unclassified information should be protected by using a "PRIVACY ACT DATA Coversheet (SF-23-29).

3. Creation/Reproduction of Classified Information

3.1. Classified Creation/Reproduction:

3.1.1. Should be kept to the minimum required to accomplish the mission. All copies are subject to the same controls and safeguards as the original document and will follow rules found in *32 CFR Part 2001 and/or DOD 5200.01 vol 4*.

3.2. Required Markings are:

3.2.1. Overall classification markings will be placed on the top and bottom of every page of the document(s). Classification marking will always be fully spelled out unless an authorized abbreviation exists, will always be written all in capital letters and will include one of the following document classification labels:

3.2.1.1. Top Secret - Disclosure can cause exceptionally grave damage to the United States national security.

3.2.1.2. Secret - Disclosure can cause serious damage to the United States national security.

3.2.1.3. Confidential - Disclosure can cause identifiable damage to the United States national security.

3.2.2. Classification portion markings are used before titles or subjects, precede paragraphs and sub-paragraphs and can be shown in the following manner: (U) for Unclassified, (C) for Confidential, (S) for Secret or (TS) for Top Secret. Portion marks will always be in capital letters and inside parentheses.

3.2.3. Additional protection and handling markings may also be added to documents detailing specific requirements required to maintain the document in question. These are usually added to SCI documents. The SCI Control System is the system of procedural protective mechanisms used to regulate or guide each program established by the Director of Central Intelligence as SCI. These are placed at the end of overall classification and portion markings.

3.2.4. The Agency/Originator; otherwise known as Original Classification Authority (OCA), the reason designator for classification of the document and a declassify date (not to exceed 25 years of the original document classification) will be placed in the lower left hand side of the document.

3.3. Derivative Document:

3.3.1. Derivative documentation is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified. The newly developed material must be consistent with the markings of the source information.

3.3.2. A “Derived From/Declassify On” block is required in the lower right corner of the coversheet, coverpage, front page, and/or first slide of every classified document. The first line of the block will identify the creator of the document (ex. Classified by: John Doe, Director). The second line will identify the sources of classification used (ex. Derived From: Classification Guide 10-23). The third line will be the date of the original source, format is YYYYMMDD (ex. Dated: 20070108). The fourth line is the ‘declassify on’ date/event. If using a classification guide as a source, use the declassification instructions provided by the OCA (ex. guide states “declassify after 25 years,” add 25 years from the date of the creation of the new document). If the source is not a classification guide or does not have declassification instructions, add 25 years to the date of the source document for a declassification date. Legacy markings for declassification such as “MR” for Manual Review, or “OADR” for Originating Agency’s Determination Required, are obsolete and may no longer be used. For example:

Classified by: John Doe, 70 ISRW/SO
 Derived From: Department of Good Works
 Dated: 20130419
 Declassify On: 20380419 (usually 25 years later from source date of document)

3.4. Working Papers:

3.4.1. Are documents and material accumulated or created in the preparation of finished documents and material, such as drafts, talking papers, bullet papers, etc. Working papers must:

3.4.1.1. Be conspicuously marked "Working Paper" on the first page of the document in letters larger than the text.

3.4.1.2. Contain a creation date in ink.

3.4.1.3. Be marked with the highest classification of the information contained therein.

3.4.1.4. Be protected in accordance with assigned classification level.

3.4.1.5. Be destroyed when no longer needed.

3.4.1.6. If retained for more than 180 days from the date of origin, working papers must be accounted for, controlled and marked in the manner prescribed for a finished document of the same classification.

4. Antiterrorism (AT)

4.1. Purpose: AT is a command responsibility which must be thoroughly integrated into every unit mission. Additionally, an effective AT program requires participation from every member of the command. Each individual must remain aware of potential terrorist threats, practice personal security measures, and report suspicious activity.

4.2. Group/Squadron/Unit ATOs:

4.2.1. Units having 300 or more personnel assigned or under the operational control of a designated commander will appoint in writing a Level II certified ATO.

4.2.2. ATOs will be either a commissioned officer, non-commissioned officer (E-5 or above), or civilian staff officer of equivalent grade.

4.2.3. Contractors may not be appointed as primary or alternate ATO for government facilities.

4.2.4. Unit ATOs shall complete resident AT Level II training within 180 days of assignment as ATO.

4.2.5. Level II refresher training must be completed at least once every three years to maintain qualification as ATO/ATR.

4.2.6. Units with an authorized strength of 299 or fewer and separate flight/elements will appoint in writing a ATR by the unit commander or element chief.

4.2.6.1. Unit ATRs will hold a minimum grade of SSgt (E-5) or civilian equivalent.

4.2.6.2. Unit ATRs shall complete either resident AT Level II training within 180 days of formal assignment or complete the "AT Level II Refresher CBT" found on ADLS until they can attend a resident AT Level II course.

4.2.6.3. Level II refresher training must be completed at least once every three years to maintain qualification as ATO/ATR.

4.3. ATO/ATR Responsibilities/Duties:

4.3.1. Assist the commander in implementing Joint, DoD, GCC and Air Force AT-related doctrine, policy and TTPs. Make recommendations to the commander if supplemental policy and guidance is necessary to execute the commander's AT Program.

4.3.2. Provide AT considerations, to include real-world and exercise lessons learned, to assist the commander in developing realistic and relevant scenarios to exercise and validate the AT program.

4.3.3. Establish an effective Random Antiterrorism Measures Program that utilizes the Standards set forth in AFI 10-245, *Antiterrorism (AT)*, 21 September 2012.

4.3.3.1. The RAM Program is developed and implemented as an integral component of the overall AT program and guided by the principles outlined in the Antiterrorism Handbook.

4.3.3.2. RAMs will be implemented to mitigate and reduce risk for existing and potential vulnerabilities.

4.3.4. Ensure members of the command are aware of existing installation Force Protection Controls and any changes that are anticipated in the future.

4.3.5. Ensure that all relevant standards found in AFI 10-245, *Antiterrorism (AT)*, 21 September 2012 are adhered to.

4.3.6. Criticality Assessments (CAs) and Vulnerability Assessments (VAs) will be conducted by the unit ATO/ATR to cover facilities and assets that are included in that unit's mission. These CAs and VAs will be updated annually.

5. Operations Security

5.1. Purpose: The purpose of Operations Security or 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.

5.1.1. OPSEC awareness is an encompassing program that involves all Airmen, civilian, contractors and family members within 70 ISRW.

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

5.2.1. Identifying those actions that can be observed by adversary intelligence systems.

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

5.2.3. Selecting and executing measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

5.3. OPSEC Program Manager (PM):

5.3.1. OSPEC Program Manager will be appointed in writing at the Wing-level.

5.3.2. OPSEC PMs will be an O-3 or above, civilian equivalent, or an E-7 or above. 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).

5.3.3. OPSEC PMs will have accounts established on SIPRnet.

5.3.4. Completion of the Air Force Signature Management Course (SMC) is mandatory for OPSEC PMs below MAJCOM level.

5.3.4.1. Signature management utilizes a process of profiling day-to-day observable activities and operational trends at installations and each of its resident units. These profiles result in identified processes and details that can be used in efforts to defend or exploit operational profiles resident at a given military installation.

5.3.5. Completion of the Interagency OPSEC Support Staff's (IOSS) OPSE-2500 course, *OPSEC Analysis and Program Management Course* is required for all OPSEC PMs.

5.4. OPSEC Coordinators:

5.4.1. OPSEC Coordinators will be appointed in writing at subordinate Wing-level organizations, down to Squadron level.

5.4.2. OPSEC Coordinators can be officers, NCOs (E-5) and above or civilian equivalent of any grade. OPSEC Coordinators, at a minimum, will have a secret clearance.

5.4.3. Completion of the Interagency OPSEC Support Staff's (IOSS) OPSE 1300 course, *OPSEC Fundamentals* (course-based) or OPSEC-1301, *OPSEC Fundamentals* (computer-based).

5.5. OPSEC Program Managers and OPSEC Coordinators will:

5.5.1. Advise the commander on all OPSEC matters to include developing operating instructions, recommending guidance, and OPSEC measures.

5.5.2. OPSEC PMs and Coordinators will coordinate and integrate with host installation on any OPSEC or signature management initiatives and working groups.

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

5.5.4. Develop, implement, and distribute commander's OPSEC guidance memorandums to include Critical Information Lists (CILs).

5.5.4.1. CILs include 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. They also include areas, activities, functions, or other matters that a facility/organization considers most important to protect from adversaries.

5.5.5. Ensure procedures are in place to control critical information and associated indicators.

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

5.5.7. Review all OPSEC plans, CILs and memos on an annual basis.

5.5.8. Conduct quarterly OPSEC assessments.

5.5.9. Conduct the annual OPSEC program review.

5.6. Web Site Administrators, Webmasters, and anyone (superiors, public affairs specialist, OPSEC coordinators, PMs, Signature Management Officers (SMOs)/Signature Management Noncommissioned Officers (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 and Public Release Decisions* and OPSE-3500, *OPSEC and Internet Based Capabilities Course* are the training methods to fulfill this requirement.

5.7. OPSEC Assessments and OPSEC Program Reviews:

5.7.1. OPSEC 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. The annual OPSEC Program Review is a continual processes that involve combining data collected from Measures of Performance (MOP), measures of Effectiveness (MOE), exercise after action reports, lessons learned, operational readiness/compliance inspections, and annually conducted self-assessments/self-inspections.

5.7.2. OPSEC assessments will be conducted by OPSEC Coordinators and may be accomplished by utilizing the MICT OPSEC 4: OPSEC Program - (Below Wing Level Organizations checklist (for Group or lower OPSEC programs), OPSEC office walkthroughs to verify proper OPSEC procedures and implementation is proceeding accordingly and/or via OPSEC reviews of public domain unit websites/social media sites.

5.7.2.1. 70 ISRW OPSEC Coordinators will conduct OPSEC assessments, at a minimum, on a quarterly basis. At least two of these assessments must be by means other than utilizing the MICT OPSEC 4 checklist, such as utilizing OSPEC office walkthroughs and web site reviews. This is to ensure OPSEC Coordinators are proactively engaging with unit personnel on proper OPSEC procedures.

5.7.3. OPSEC PMs and OPSEC Coordinators will utilize the OPSEC risk assessment tool Operations Security Collaboration Architecture (OSCAR) to accomplish annual program reviews unless otherwise directed by Wing or MAJCOM direction. OPSEC program reviews are an opportunity to formally notify the chain of command of the overall status of a unit's OPSEC program

5.7.3.1. 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.

5.7.3.2. 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.

5.7.3.3. OSCAR accounts can be requested by going to the following link:
<https://register.dtic.smil.mil/wobin/WebObjects/RegLite?SiteID=OSCAR> on
SIPRnet.

KEVIN D. DIXON, Colonel, USAF
Commander

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

32 C.F.R. Part 200, *Classified National Security Information*.
AFI 10-245, *Antiterrorism (AT)*, 21 September 2012.
AFI 31-101, *Integrated Defense*, 08 October 2009.
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 10-701 *Operations Security*.
DoD 5200.1, Volume 1, *DoD Information Security Program: Overview, Classification, and Declassification*, 24 February 2012.
ICD 705, *Sensitive Compartmented Information Facilities*, 26 May 2010.

Adopted Form

AF Form 847, *Recommendation for Change of Publication*.

Abbreviations and Acronyms

70 ISRW—70 Intelligence, Surveillance and Reconnaissance Wing
ADLS—Advance Distribution Learning Service
ATEC—Antiterrorism Executive Committee
AFI—Air Force Instruction
AT—Antiterrorism
ATFP—Antiterrorism Force Protection
ATWG—Antiterrorism Working Group
ATO—Antiterrorism Officer
ATR—Antiterrorism Representative
CA—Criticality Assessment
CBT—Computer Based Training
CILs—Critical information Lists
CPU—Central Processing Unit
CUI—Consolidated Unit Inspections
DoD—Department of Defense
EAP—Emergency Action Plan

EPP—Emergency Protection Plan
EQIP—Electronic Questionnaire for Investigations Processing
FPCON—Force Protection Controls
GCC—Ground Combatant Commander
IA—Information Assurance
IC—Intelligence Community
IMT—Information Management Tool
IO—Intelligence Oversight
ISRG—Intelligence, Surveillance and Reconnaissance Group
ISPM—Information Security Program Manager
JPAS—Joint Personnel Adjudication System
MAJCOM—Major Command
MOA—Memorandums of Agreement
MICT—Management Internal Control Toolset
MOE—Measures of Effectiveness
MOP—Measures of Performance
OPSEC—Operations Security
OSCAR—Operations Security Collaboration ARchitecture
PM—Program Manager
RAMs—Random Antiterrorism Measures
RAMP—Random Antiterrorism Measures Program
PR—Periodic Reinvestigation
SAR Code—Security Access Requirement Code
SCIF—Sensitive Compartmentalized Information Facility
SF—Standard Form
SIPRnet—Secret Internet Protocol Router Network
SM—Security Manager
SMC—Signature Management Course
SMNCOs—Signature Management Noncommissioned Officers
SMOs—Signature Management Officers
SO—Security Officer
SR—Security Representative

SSBI—PR - Single Scope Background Periodic Reinvestigation

SSO—Special Security Officer (found at Group and/or Squadron level)

STEM—Security, Education, Motivation and Training Meetings

TTPs—Tactics, Training and Procedures

TWG—Threat Working Group

OCA—Original Classification Authority

UDM—Unit Deployment Manager

UMD—Unit Manning Document

VA—Vulnerability Assessment