

**BY ORDER OF THE COMMANDER  
910TH AIRLIFT WING**

**910TH AIRLIFT WING INSTRUCTION  
10-701**



**19 JULY 2011**

**Operations**

**OPERATIONS SECURITY**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

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

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: 910 OSS/OSX

Certified by: 910 OG/CC  
(Col Craig Peters)

Pages: 10

---

This instruction implements Air Force Policy Directive (AFPD 10-7), *Information Operations* and Air Force Instruction (AFI) 10-701, *Operations Security (OPSEC)*. It establishes responsibilities and guidelines for conducting the 910th Airlift Wing (910 AW) Operations and Security (OPSEC) Program. It applies to all base operating support (BOS) contractors and units assigned or attached to Youngstown Air Reserve Station (YARS). Refer recommended changes and questions about this publication to 910th Operations Support Squadron (910 OSS/OSTX), Youngstown Air Reserve Station (ARS) using the Air Force Form (AF) 847, *Recommendation for Change of Publication*; route AF 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 the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afirms/afirms>

**SUMMARY OF CHANGES**

This is the initial publication of 910th Airlift Wing Instruction 10-701

**1. The Goal of OPSEC.** The goal is to identify information, primarily unclassified that relates to the 910 AW daily and wartime operation which could give an adversary an advantage if exploited. In conjunction with this identification process is determining the threat against this critical information and the ways in which this information could be exploited. In assessing the level of damage that would occur if this information is successfully exploited of the acceptable or not level of damage (Risk management) must be determined. If this level of damage is not acceptable then finding ways of preventing the adversary from exploiting the information and

applying the countermeasures of denying them this advantage. OPSEC is a continuous process. It is a process which should be used in all operational activities and the planning of those activities.

## **2. General Guidelines.**

2.1. OPSEC should be closely coordinated with the security disciplines in the Wing to include Computer Security (COMPUSEC), Communications Security (COMSEC), Emissions Security (EMSEC) and Information Protection (IP).

2.2. Commanders at every level in the Wing must take an active role in the program to ensure its success.

2.3. Coordinating with the BOS to ensure all contractors and civilian employees review good OPSEC procedures upon commencing activities initially and periodically when tasked.

2.4. All OPSEC Unit Coordinators must continuously review their programs and critical information lists to mitigate the dispersion of unclassified information that could affect the unit's mission or personnel.

## **3. Wing Program Manager (PM).**

3.1. The 910 AW Commander will appoint an OPSEC Program Manager and an alternate.

3.1.1. The Program Manager will attend the Signature Management Course within 90 days of appoint.

3.2. The 910 AW PM will:

3.2.1. Develop the wing's OPSEC procedures and guidelines, and ensure compliance of these directives.

3.2.1.1. Update the 910 AWI 10-701 as required incorporating any changes submitted.

3.2.2. In coordination with Information Protection Management Office and the Exercise Evaluation Team (EET) evaluate the wing's vulnerability during exercises.

3.2.2.1. Utilize OPSEC Surveys and assessments with the working groups assistance in updating the units Critical Information Lists (CILs) in mitigating this information.

3.2.3. Advise the 910 AW Commander on OPSEC issues and manage the integration of OPSEC measures into daily operations and exercises to increase the wings' operational effectiveness.

3.2.4. Chair the OPSEC working group meetings and provide minutes from those meetings.

3.2.5. Annually review and update the wing's critical information list and indicators.

3.2.6. Provide training to the contractor managers and provide assistance to all the OPSEC Unit Coordinators with their programs. All new Unit Coordinators will be trained within 90 days of their appointment.

3.2.7. Ensure newly assigned personnel receive training within 90 days of arrival as a part of their Newcomer's Briefing.

- 3.2.8. Complete the wing OPSEC self-inspection checklist annually.
- 3.2.9. Annually submit the 910 AW OPSEC Program Report to HQ AFRC/A3XX and 22 AF/A3V.
- 3.2.10. Update the 910 AW Program Manger Continuity Book.
- 3.2.11. Update and distribute information through the 910 AW OPSEC COP to the Unit Coordinators.
- 3.2.12. Order and update OPSEC training materials from the Interagency OPSEC Support Staff (IOSS).

#### **4. The 910 AW Unit Coordinators (UC).**

- 4.1. The OPSEC Unit Coordinator and their alternate will be appointed by the unit commander in writing. Either the primary or alternate will be an Air Reserve Technician (ART) within the unit. This individual must be thoroughly familiar with day to day operations of the unit.
- 4.2. The UC will:
  - 4.2.1. Advise the unit commander and their staff on OPSEC issues.
  - 4.2.2. Ensure their unit is complying with all OPSEC directives.
  - 4.2.3. Ensure annual refresher training is accomplished in conjunction with Information Protection Computer Based Training (IP CBT) on the Advanced Distributed Learning Services (ADLS).
  - 4.2.4. Provide periodic good OPSEC reminders throughout the year for unit members.
  - 4.2.5. Update and review their unit's CIL annually and post any updates on the unit's bulletin boards and on the 910 AW OPSEC Community of Practice (CoP).
  - 4.2.6. Assist in any OPSEC surveys and assessments which affects the unit.
  - 4.2.7. Forward any OPSEC issues to the wing program manager and the OPSEC working group.
  - 4.2.8. Complete the unit OPSEC self-inspection checklist annually.
  - 4.2.9. Each September provide the wing program manager an assessment of their program to include annual training accomplished.
  - 4.2.10. Maintain their unit's continuity book.

#### **5. Civil Engineering Contracting.**

- 5.1. The Program Unit Coordinator and their alternate will:
  - 5.1.1. Be appointed by letter. They must be in position which allows them to oversee their sections which play a role in the daily and wartime operations of the wing (i.e. contracting projects, etc)
  - 5.1.2. Pass any recommendations it may have to the appropriate wing, group or unit agency.
  - 5.1.3. Be a member of the 910 AW OPSEC Working Group.

- 5.1.4. Provide OPSEC awareness training annually to their employees.
- 5.1.5. Provide reminders throughout the year for members to practice good OPSEC.
- 5.1.6. Train all new fulltime Civilian Civil Engineer (CE) personnel on OPSEC practices and thoroughly brief them on the 910 AW Critical Information List and counter measures.
- 5.1.7. Assist in any OPSEC surveys or assessments which affect the CE contracting.
- 5.1.8. Complete an OPSEC self-inspection checklist annually.

## **6. Public Affairs (PA).**

- 6.1. The 910 AW Public Affairs Office has a unique position in protecting Critical Information while at the same time complying with the Department of Defense (DoD) Principles of Information, the PA core competencies as well as PA's role in Information Operations. Open communication between the OPSEC Program Manager and the Chief of Public Affairs must be maintained to have an effective OPSEC Program.
- 6.2. Public Affairs will appoint a primary and alternate OPSEC representative in writing to help protect Critical Information during the day-to-day operations.
- 6.3. Public Affairs will inform the OPSEC Program Manager of higher headquarters policy and guidelines (PAG) on critical information approved for release to the public and the media.
- 6.4. The PA OPSEC representative will ensure media releases do not contain Critical Information outside of the scope of information approved for release by higher headquarters as outlined in 6.3. The Chief of Public Affairs will consult with the Wing OPSEC Program Manager prior to release of critical information, not included in 6.3. The protection Of Critical Information is always important and risk management must be utilized when the release of Critical Information is vital to the mission.
- 6.5. The OPSEC "5 Step Process" will be used to mitigate risk.
- 6.6. Public Affairs has specific and current guidance pertaining to information releasable to the public. It is paramount to the OPSEC program that other 910 AW personnel continue protecting Critical Information as published. Critical Information is released only under the 910 AW Commander's discretion.

## **7. EAST Corporation Manager (BOS).**

- 7.1. The Program Unit Coordinator and their alternate will:
  - 7.1.1. Be appointed by letter. The manager must be in position which allows them to oversee their sections which play a role in the daily and wartime operations of the wing (i.e. base operations, transportation.etc)
  - 7.1.2. Pass any recommendations it may have to the appropriate wing, group or unit agency.
  - 7.1.3. Be a member of the 910 AW OPSEC Working Group.
  - 7.1.4. Provide OPSEC awareness training annually to their employees.

7.1.5. Provide reminders throughout the year for BOS members to practice good OPSEC.

7.1.6. Train all new fulltime BOS personnel on OPSEC practices and thoroughly brief them on the 910 AW Critical Information List and counter measures.

7.1.7. Assist in any OPSEC surveys or assessments which affect the BOS contractor.

7.1.8. Complete an OPSEC self-inspection checklist annually.

**8. OPSEC Working Group.**

8.1. The OPSEC working group will be appointed by memorandum from the installation commander. The working group will meet semi-annually; during initial planning phase of any 910 AW exercises, deployments, and major events; or as directed by the installation commander. It is the wing's forum for OPSEC issues. In addition, the working group will:

8.2. Periodically review the wing's critical information list.

8.3. Assist in any OPSEC surveys or assessments.

STEPHEN J. LINSENMEYER, Col, USAFR  
Commander

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

Joint Pub 3-54, *Joint Doctrine for Security Operations*

AFPD 10-7, *Information Operations*

AFI 10-701, *Operations Security (OPSEC) Instructions*

AFI 33-106, *Managing High Frequency Radios, Personal Wireless Communication Systems, and the Military Affiliate Radio System*

***Abbreviations and Acronyms***

**910 AW**—910th Airlift Wing

**AFI**—Air Force Instruction

**ADLS**—Advanced Distributed Learning Services

**AFPD**—Air Force Policy Directive

**AFMAN**—Air Force Manual

**ART**—Air Reserve Technician

**CE**—Civil Engineer

**CILs**—Critical Information Listings

**COMSEC**—Communications Security

**COMPUSEC**—Computer Security

**CoP**—Community of Practice

**DoD**—Department of Defense

**EMSEC**—Emission Security

**EET**—Exercise Evaluation Team

**HQ AFRC/A3XX**—

**IP**—Information Protection

**IP CBT**—Information Protection Computer Based Training

**OPSEC**—Operations Security

**PA**—Public Affairs

**PAG**—Policy and Guidelines

**PM**—Program Manager

**UC**—Unit Coordinators

**YARS**—Youngstown Air Reserve Station



## Attachment 2

## CRITICAL INFORMATION ITEMS GUIDANCE

Table A2.1. Critical Information.

<p><b>NOTE:</b> This table provides general guidance concerning 910 AW Critical Information items. Individuals should review and familiarize themselves with the following listing and their unit-specific Critical Information items. Each Unit/Group OPSEC Coordinator should develop specific Critical Information listings for their organization.</p>		
CRITICAL INFORMATION	INDICATORS	COUNTERMEASURES
Specific location of core facilities, key personnel and their activities	<p>Commander's daily schedule</p> <p>Upcoming events calendar</p> <p>Protocol calendars and schedules</p> <p>CE and Readiness minutes and notes</p> <p>Work Orders/Unfunded requirement documentation</p> <p>Using insecure communications nodes such as blackberry</p>	<p>Limited distribution of documents/100% policy of old documents/use Encrypted e-mail and verifier receivers need to know. Use Computer network access protections (firewall, password, etc.)</p> <p>Disseminate reminders of secure communications to avoid OPSEC violations. Request secure nodes of communication when risk is determined unacceptable</p>
Specific mission itineraries, objectives and status	<p>Contents of exercises/EET scenarios after action reports</p>	<p>Limit distribution - Do not share information (phone, E-mail) unless you verify receiver's need-to-know. Use Encrypted e-mail</p>
Status of implementing conditions (INFOCON, DEFCON, FPCON, weather)	<p>CAT/ ICC/EOC communications.</p> <p>Threat working Group discussion and findings</p> <p>Emergency actions and response.</p>	<p>Limit ICC EOC and TWG on strict need-to-know basis - Computer network access protections (firewall, other network software employed, passwords, etc.) - Do not leave documents in open public view or unprotected in the office - Properly dispose of (e.g. shred) when obsolete - Do not share information (phone, E-mail) unless you verify receiver's need-to-</p>

		know. Use Encrypted e-mail
Computer program passwords and user IDs	Hard copy information	Do not leave documents in open public view or unprotected in the office - Properly dispose of (e.g. shred) when obsolete - Do not share information (phone, E-mail) unless you verify receiver's need-to-know. Use Encrypted e-mail
Specific mobility requirements	Reporting Instructions, OPORDS, SPINS	Do not leave documents in open public view or unprotected in the office - Properly dispose of (e.g. shred) when obsolete - Do not share information (phone, E-mail) unless you verify receiver's need-to-know. use Encrypted e-mail
Privacy ACT FOUO	Civilian and Military Orders, 40A's, travel vouchers recall rosters, Alpha rosters key personnel lists	Do not leave documents in open public view or unprotected in the office - Properly dispose of (e.g. shred) when obsolete - Do not share information (phone, E-mail) unless you verify receiver's need-to-know
Accident/Mishap details	Exercise and Evaluation Team exercises, ICC/EOC communications, Battle Staff Directives	Limit ICC EOC and TWG on strict need-to-know basis - Computer network access protections (firewall, other network software employed, passwords, etc.) - Do not leave documents in open public view or unprotected in the office - Properly dispose of (e.g. shred) when obsolete - Do not share information (phone, E-mail) unless you verify receiver's need-to-know  Do not leave documents in open public view or unprotected in the office - Properly dispose of (e.g.

		shred) when obsolete - Do not share information over the phone unless you verify receiver's need-to-know
Significant Issues/Problems (military related) that are getting media attention	Newspaper and TV coverage of Political DV visits, Air show /Open House	Ensure all media information is approved through Public Affairs prior to release