BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-1105

19 MAY 1994

Operations

PORT SECURITY INSTRUCTIONS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: HQ USAF/XOXT
(Lt Col Richard F. Shroy)
Supersedes AFR 55-32 (S), 1 June 1988.

Certified by: HQ USAF/XO
(Maj Gen Larry L. Henry)
Pages: 4
Distribution: F

This instruction implements AFPD 10-11, *Operations Security* and Department of Defense (DoD) Directive 5100.78, *United States Port Security Program*, August 25, 1986. It assigns Air Force functions and responsibilities for supporting the US Navy in its role as the DoD Port Security Executive Agent. As a part of the Air Force Operations Security Program, it provides additional instructions for controlling critical information and operations security (OPSEC) indicators from foreign vessels admitted into US ports and territorial waters. Reference AFI 10-1101, *Operations Security Instructions* and AFMAN 10-1106, *OPSEC Surveys,* for additional instruction on how to *deny* mission critical information to an adversary.

SUMMARY OF REVISIONS

This is the initial publication of AFI 10-1105. It aligns the instruction within the Air Force Operations Security Program under AFPD 10-11 and changes the office of primary responsibility (OPR) from HQ AFOSI/IVOB to HQ USAF/XOXT. It also tells Air Force commanders to implement OPSEC as the first line of defense against the exploitation threat presented by foreign vessels transiting their area of responsibility. ***Note:*** The instructions presented in this AFI are **UNCLASSIFIED.**

1. Background Information. Foreign ships that are in US ports or transiting coastal waterways and territorial seas provide ideal opportunities for hostile intelligence collection over a wide spectrum of activities. It is DoD policy to take all feasible steps to reduce our vulnerability to this collection effort along coastal shipping lanes and in or near US port areas. This policy extends to sensitive Air Force activities, operations and defense systems within reach of these collection agents, thereby eliminating or reducing the foreign exploitation of information.

1.1. The use of merchant, research, and fishing vessels by foreign nations to collect information of intelligence value has been well documented by the US and allied naval intelligence organizations.

Foreign vessels are excellent collection platforms and can provide safe havens for intelligence gathering personnel.

1.2. These commercial and private ships in port may complement foreign reconnaissance satellites, dedicated intelligence collection ships, and shore electromagnetic intercept sites. Ships in port can intercept signals which are not available to other collection platforms. Electro-magnetic signals associated with research, development, test and evaluation are prime targets. Government telephone and other communications are also prime targets since they use unchanging commercial land and satellite microwave channels.

2. Service Relationships. The following relationships are established for Air Force interaction with other DoD organizations:

2.1. The Secretary of the Navy is the DoD Executive Agent for the United States Port Security Program. A Navy Staff member acts as the DoD Member for Operations on the US Port Security Committee to handle matters arising from the administration of the program. The Navy also provides a port security vulnerability assessment program for determining the sensitivity and vulnerability of Defense facilities in or near port areas under the jurisdiction of the United States.

2.2. The Director, National Security Agency, designates a point of contact to assist the DoD Executive Agent.

2.3. The Secretaries of the Army and the Air Force each designate an organization to respond to the DoD Executive Agent in the conduct of the port security vulnerability assessment program and other needs of the Port Security Program.

3. Controlled Access to US Ports. There are US policies in place that control the access of *some* foreign countries to *some* US ports:

3.1. The following five US ports are open to the Former Soviet Union (FSU) Republics on a *7-day request* regime *subject to denial* for security reasons:

- San Diego, CA.
- Port Hueneme, CA.
- Kings Bay, GA.
- Port Canaveral, FL.
- New London/Groton, CT.

3.2. The following US ports are open to the FSU Republics on a *3-day notification* regime:

- Charleston, SC.
- Pensacola, FL.
- Portsmouth, NH.
- Port St. Joe, FL.
- New London/Groton, CT.
- Panama City, FL.
- Honolulu, HI.
- Hampton Roads, VA.

3.2.1. The twelve independent FSU Republics are: Armenia, Azerbaijan, Byelarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Turkmenistan, Ukraine, and Uzbekistan.

3.3. Countries **not** currently **permitted access** to US ports are Cambodia, Cuba, Iran, Iraq, Libya, North Korea, Syria, and Vietnam.

4. Responsibilities:

4.1. Concerned Air Force Commanders will:

4.1.1. Institute effective OPSEC programs and measures (according to AFI 10-1101) that control mission critical information and OPSEC indicators from the foreign collection and exploitation effort referred to in paragraph **1.1.**

4.1.2. Request a cognizant naval authority to provide their units with timely notifications of FSU requests to visit ports (according to paragraphs **3.1.** and **3.2.**) or transit coastal waters within their specific area of concern.

4.1.3. Develop procedures to ensure their units are notified of FSU vessel visits as soon as possible such that appropriate OPSEC actions can be implemented as necessary.

4.1.4. Monitor vulnerabilities and institute OPSEC measures as needed.

4.1.5. Maintain a staff member of primary responsibility (POC) for managing the Port Security Program.

4.1.6. Request (through appropriate channels) HQ USAF/XOXT (1480 Air Force Pentagon, Washington DC 20330-1480; DSN 227-3050) to notify cognizant naval authorities when FSU visits to ports should be denied or delayed Be prepared to justify such requests in writing.

4.2. Deputy Chief of Staff, Plans and Operations (HQ USAF/XO) through the Technical Plans Division (HQ USAF/XOXT) will:

4.2.1. Maintain an OPR for managing the Port Security Program.

4.2.2. Assist and cooperate with the Executive Agent for DoD participation in the US Port Security Program.

4.2.3. Coordinate major command and field operating agency requests to deny or delay special interest vessel visits to specified port areas with the DoD Executive Agent.

4.3. The Air Force Information Warfare Center will accomplish OPSEC surveys to support Air Force missions and support naval port security vulnerability assessments as requested by concerned facility managers in coordination with HQ USAF/XOXT.

4.4. The Air Force Office of Special Investigations will support Air Force OPSEC surveys and naval port security vulnerability assessments conducted under the auspices of the US Port Security Program.

5. Terms and Definitions:

5.1. Critical Information. Specific facts about friendly intentions, capabilities, limitations, 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. (Joint Pub 1-02)

5.2. Operations Security (OPSEC) Indicator. Friendly detectable actions and open-source information that can be interpreted or pieced together by an adversary to derive critical information. (Joint Pub 1-02)

5.3. Operations Security Measures. Methods and means to reduce or eliminate OPSEC vulnerabilities by controlling critical information and OPSEC indicators of that critical information. The following categories apply:

- **Action Control.** Methods to eliminate or prevent detection of OPSEC indicators. Examples are adjusting schedules and activities and delaying information releases. First, plan activities necessary to conduct and support an operation. Then, control the conduct (timing, place, etc.) of those activities to eliminate or substantially reduce OPSEC indicators.
- **Countermeasures.** Methods to disrupt adversary information gathering *sensors* and *data links* or preventing an adversary from obtaining, detecting or recognizing OPSEC indicators. Examples are jamming, interference, diversions and force. The objective is to disrupt effective adversary information gathering, analysis, and distribution. Use units, system designs, and procedures to create diversions, camouflage, concealment, jamming, threats, police powers, and force against adversary information gathering, processing, and distribution capabilities.
- **Counteranalysis.** Methods to affect the observation and/or interpretation of adversary intelligence analysts. Examples are military deceptions and covers. The objective is to prevent accurate interpretations of OPSEC indicators during adversary data analysis. This is done by confusing the adversary analyst through deception techniques.
- **Protective Measures.** Methods to create closed information systems to prevent adversaries from gaining access to information and resources. Examples include crypto-logic systems and standardized security procedures.

LARRY L. HENRY, Maj General, USAF
Acting DCS/Plans and Operations