

**BY ORDER OF THE COMMANDER,
AVIANO (USAFE)**

**401 AIR EXPEDITIONARY WING
INSTRUCTION 31-401**

20 FEBRUARY 2004

Security

INFORMATION SECURITY



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: 401 AEW/CCEA (TSgt Marvin Strange)

Certified by: 401 AEW/CCE
(Maj Kenneth A. Wong)

Pages: 5

Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 31-401, *Information Security*, and provides guidance from DoD 5200.1-R, *Information Security Program*; AFI 31-401, *Information Security Program Management* and USAFEPAM 31-402, *Conducting Security Incident Inquiries and Investigations*. This instruction provides guidance on implementing an effective information security program within the 401 AEW staff and all subordinate units. 401 AEW units will send proposed changes and corrections to this publication to the 401 AEW/CCEA for review and inclusion. Maintain and dispose of records created as a result of prescribed processes in accordance with Air Force Manual (AFMAN) 37-139, *Records Disposition Schedule*.

1. POLICY:

1.1. All 401 AEW staff members must be personally responsible for providing proper protection of the classified information within their respective custody.

1.1.1. With the exception of Sarajevo, all detachments possess classified capability in one form or another and will handle and process classified information according to established regulatory guidance.

1.2. All officials within the 401 AEW have specific, non-delegable responsibilities for implementation and management of Information Security Programs within their units. Our presence in a foreign country and our peacekeeping mission present increased security risks; all unit members will give utmost care and attention to classified information to ensure it is protected.

1.3. Classified information will be protected at all times, either by storage in a GSA approved container or facility, or by the personal observation and control of an authorized individual.

2. PROCEDURES:

2.1. The 401 AEW Staff and each unit within the 401 AEW will appoint, in writing, an Information Security Program Manager (**Attachment 2**). Each unit Security Manager will keep signed copies of **Attachment 2** on file. It is his/her responsibility to ensure all deployed persons are fully aware of proper procedures for custody and care of classified information. Unit commanders and Security Managers will ensure that the security inprocessing briefing (**Attachment 1**) is provided to all incoming personnel. Furthermore, the Program Manager will ensure proper procedures are followed in the event of a compromise of classified information.

2.2. Unit commanders shall permit classified information access only if individuals, (1) possess a valid and appropriate security clearance, (2) have signed the appropriate non-disclosure agreement, and (3) have a valid need for access to information in order to perform a lawful and authorized government function. Everyone bears responsibility to ensure that these requirements are met.

2.3. 401 AEW units shall have a system of control measures that ensures access to classified information is limited to authorized personnel. Control measures shall be appropriate for both the environment where access occurs and the nature and volume of information. The system shall include technical, physical and personal control measures. Administrative control measures (which may include records of internal distribution, access, generation, inventory, reproduction and disposition) shall be required when technical, physical and personal control measures are insufficient to detect and/or deter access by unauthorized persons.

2.4. Classified information, discussed in telephone conversations or over computer information systems, must be discussed only over secure communication circuits approved for transmission of information at the specific level of classification.

2.5. Meetings and conferences involving classified information present special vulnerabilities to unauthorized disclosure. Adequate security procedures to minimize risk to classified information must be developed and implemented. Classified sessions will be segregated whenever possible. Access to meetings, conferences or specific sessions at which classified information will be discussed or disseminated will be limited to persons who possess an appropriate security clearance and need-to-know.

2.6. Commanders will establish procedures to ensure prompt and appropriate management actions are taken in case of (1) compromise or potential compromise of classified information, (2) improper classification of information, (3) violation of the provisions of this operation instruction and, (4) for incidents that may put classified information at risk of compromise.

2.6.1. Any person who becomes aware of the possible compromise of classified information will immediately report it to their supervisor or the unit security manger. If the person believes that the immediate supervisor or security manager may have been involved in the incident, he/she may report it to authorities at the next level of command or supervision. Unit commanders will advise 401 AEW/CC and 401 AEW/IM as soon as possible when there is a security incident.

2.6.2. If a compromise occurs, damage to U.S. interests will be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise. When possible, action should be taken to regain custody of documents or material that was compromised.

2.6.2.1. The unit commander will initiate an investigation by appointing an investigating official. The investigating official will immediately inquire into the incident to determine when, where and how it occurred, and if classified information was compromised.

2.6.2.2. For information on how to conduct an inquiry or formal investigation consult USAFEPAM 31-402, *Conducting Security Incident inquiries and Investigations*. This pamphlet explains who to notify and provides guidance on whether to conduct an inquiry or a formal investigation and how to conduct them. Given the transitory nature of personnel within the 401 AEW, it is imperative that inquiries are completed expeditiously.

2.6.2.3. Action will be taken to identify the source and reason for actual or potential compromise and remedial action taken to prevent recurrence.

2.6.2.4. All 401 AEW personnel must understand that they are subject to sanctions if they knowingly, willfully, or negligently disclose classified information to unauthorized personnel. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, and loss or denial of access to classified information. UCMJ action may also be taken for violations of the code and any applicable criminal law.

JOSEPH A. ABBOTT, Colonel, USAF
Commander

Attachment 1

401 AEW SECURITY INPROCESSING BRIEFING

Welcome to the 401 AEW! Our presence in a foreign country and our high intensity peacekeeping mission requires every AEW member to place a significant emphasis on information security. The compromise of classified information could prove detrimental to our mission and it is everyone’s responsibility to ensure classified information is protected from unauthorized disclosure. Please read through this short briefing and become familiar with your responsibilities to the AEF mission and national security.

KNOW YOUR UNIT SECURITY MANAGER:

- The wing level security manager is _____, DP 632-_____.
- The unit level security manager is _____, DP _____.

RESOURCE PROTECTION/PHYSICAL SECURITY:

- Ensure building doors, file cabinets and locks are secured at the end of the duty day
- In a friendly manner, challenge unfamiliar faces or personnel who look like they may need help
- After duty hours secure valuables and personal information in a lockable desk or file cabinet
- Report lost or stolen building keys or gate keys to the unit security manager
- Report lost or stolen Restricted Area Badges, if applicable, to the unit security manager
- Report any suspicious personnel/activity to Security Forces

COMPUTER SECURITY:

- Do not process classified information on your computer unless it is approved for classified
- Use alphanumeric passwords at least 8 characters in length and change them every 90 days
- Do not share your password, but if you have to, change it as soon as possible

INFORMATION SECURITY:

- Read and become familiar with the 401AEWI 31-401, *Information Security*.
- Maintain positive control of classified material while it is in your possession
- Classified material must have a cover sheet
- Classified material that is to be removed from your workcenter must be double wrapped
 - Classification markings and OPR/address on inside wrapper/outer wrapping contains OPR/address and NO classification markings
 - Refer to DoD 5200.1-R if you have any questions
- Transmit classified information via secure means (secure facsimile, STEE or STU-III)
- Never leave classified documents unattended in your work area

This is to certify I have received my initial security briefing and understand the contents herein and that I will read the 401 AEWI 31-401. If I have any questions, I will contact my unit Security Manager.

PRINTED NAME

SIGNATURE

DATE

Attachment 2**SAMPLE APPOINTMENT OF INQUIRY OFFICIAL****(Use 401 AEW Letter Head)**

DATE

MEMORANDUM FOR _____, SSN: _____

FROM: UNIT/CC

SUBJECT: Appointment of Inquiry Official

1. Under the provisions of DoD 5200.1-R and AFI 31-401, you are appointed to conduct a preliminary inquiry into security incident # ____ reported on (date). The security incident involved the handling of classified items or equipment by uncleared persons, or possible compromise.
2. The purpose of this inquiry is to determine whether a compromise of classified information occurred and to categorize the incident in accordance with DoD 5200.1-R and AFI 31-401. You are authorized to interview those persons necessary to complete your findings. You are further authorized access to all records and files, to include those classified up to and including SECRET/NATO SECRET, which are pertinent to this inquiry.
3. Conducting this inquiry will be your primary duty until it is completed. Immediately contact 31 SFS/SFAI, 632-7155, for a briefing on your responsibilities and the conduct of any limitations of this inquiry. You will forward your written report to me within 10 duty days of this letter. As a minimum, the report must contain the following:
 - a. A statement that a compromise or probable compromise did/did not occur
 - b. Category of the security incident
 - c. Causal factors and responsible person(s)
 - d. Recommended corrective action(s)
4. Notify me immediately if you determine a compromise has occurred. You are encouraged to obtain technical assistance from the 31 SFS/SFAI or 401 AEW/JA offices during the course of this inquiry, as necessary.

Full Name, Rank, USAF

Commander

cc:

31 SFS/SFAI

401 AEW/SF

This is protected under the Privacy Act of 1874.