DEPARTMENT OF THE AIR FORCE *AIA RECURRING PERIODICAL 31-1*

4th Quarter 2000

Security

THE SHIELD

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil.

OPR: HQ AIA/SOCD (MSgt Guy Woodbury) Certified by: HQ AIA/SOC (Mr. Robert Eddy)
Pages: 7
Distribution: F

FOREWORD This recurring publication is published quarterly to assist security managers administer unit security training and education programs. It supports the Air Intelligence Agency (AIA) Security Training, Education, and Motivation (STEM) Program governed by AIA Supplement 1 to AFI 31-401, *Managing The Information Security Program*. The contents are for information and training purposes only. Articles presented herein do not represent a change of policy or requirements unless officially incorporated into Air Force or Agency instructions.

We solicit your suggestions for articles or other ideas for publication. We are very interested in "cross-feeding" improved methods, effective procedures, quality enhancements, or other publications and training aids in this publication. Please forward any articles or suggested topics to the Information Security Division, Disclosure Branch, HQ AIA/SOCD, 102 Hall Blvd, Suite 257, San Antonio TX 78243-7026 or e-mail: guy.woodbury@lackland.af.mil.

1. INFORMATION SECURITY:

1.1. MESSAGES TO THE FIELD by MSgt Steve Kramer, HQ AIA/SOCD:

The following messages are from the past quarter and contain policy or guidance from HQ AIA/SO and others. They are intended for use throughout the Agency and supported element security offices; however, some apply only to the Wings, Groups, and Centers. If your organizations is not in receipt of, or on distribution for a below message, forward your inquiry to Mrs. Darleen Benware at DSN 969-2888 or darleen.benware@lackland.af.mil.

1.1.1. JGUBY MESSAGES: Used to disseminate security information to AIA units.

JGUBY 00-11, 311800Z Aug 00, EPSQ Updates

JGUBY 00-12, 061459Z Sep 00, Classification of Operational use of Chinese, Korean, and Russian Languages at NSA Headquarters and the RSOC's

JGUBY (Unnumbered), 061501Z Sep 00, AIA Visual Aids Available

JGUBY 00-13, 141934Z Sep 00, Personnel Security Clearance Investigations

JGUBY 00-14, 111504Z Oct 00, HQ AIA SCIF Database Update Request

JGUBY 00-15, 272027Z Oct 00, AFTAC General Subjects Security Classification Guide

1.1.2. NOSIZ MESSAGES: Used to disseminate security training information.

NOSIZ 00-09, 232023Z Aug 00, USAF SCI Security Management Course Info

NOSIZ 00-10, 031201Z Oct 00, USAF SCI Security Management Course Info

1.1.3. ROXAD MESSAGES: Used to disseminate updates and clarification of policy to the field.

ROXAD 00-04 (AIA-ROXAD-04-00), 181222Z Oct 00, AIA Security Publications and Visual Aids

1.1.4. AIG 8551: Used to disseminate information to AIA Security Forces.

AIG 8551 00-10, 211518Z Aug 00, Recapitulation 02/00 of AIG Eight Five Five One

AIG 8551 00-11, 162128Z Aug 00, New AIA Security Publication

AIG 8551 00-12, 302118Z Aug 00, 2000 USAF Security Forces Awards Program

AIG 8551 00-12, 311521Z Aug 00, Interim Change 00-01 to AFI 31-401

AIG 8551 00-13, 181549Z Sep 00, Combating Terrorism Training

AIG 8551 00-14, 041233Z Oct 00, Security Forces Craftsman Course L3ACR3P071-003

AIG 8551 00-15, 111540Z Oct 00, USAF Foreign Disclosure Training Class

AIG 8551 00-16, 272027Z Oct 00, Security Forces Civilian Plus-up

AIG 8551 00-17, 272037Z Oct 00, Training Information for AIA Security Forces Personnel/Officials

1.2. FOREIGN DISCLOSURE by Mr. George Stapleton, HQ AIA/SOCD

Before you disclose any classified information to authorized foreign visitors, clear the information with your unit Foreign Disclosure Officer. He, or she will insure the information is specified in the visit request, the visitors are appropriately cleared, the information is properly classified, and approved for release. I am the newly appointed Foreign Disclosure Officer for AIA and I am looking forward to working with all of you. If you have any questions feel free to call Mr. George Stapleton, DSN 969-2011.

1.3. LINGUISTS, BEWARE! by SMSgt John Cohorn, HQ AIA/SOC

The National Security Agency (NSA) recently released a new security classification decision stating that “the fact that an NSA/CSS employee is a linguist in a specific foreign language except for Russian, Korean, and Chinese is SECRET.” But, please be careful with this. The operational use of these languages anywhere except at NSA or the Regional SIGINT Operations Centers (RSOC) is still SECRET. So, basically this means that if you’re a Russian linguist at NSA or an RSOC, you can tell your mom. But, if you’re anywhere else in the world, this fact is SECRET.

1.4. SIGNALS INTELLIGENCE CLASSIFICATION REMINDER by SMSgt John Cohorn, HQ AIA/SOC

Although NSA has declassified many details of its mission, many of the old, more restrictive rules still apply to our field sites. For example, NSA declassified the association of a signals intelligence (SIGINT) mission with NSA headquarters, the RSOCs, and the service cryptologic element (SCE) headquarters. However, the association of a SIGINT mission with ANY specific AIA unit (other than HQ AIA because it's a SCE headquarters) is classified at least CONFIDENTIAL.

2. PERSONNEL SECURITY:

2.1. FOR CAUSE PROCESS by Lenny Martin, HQ AIA/SOPS

Did you know...the Air Force's Senior Officer of the Intelligence Community (SOIC) must approve "For Cause" actions (discharge or court martial) taken against people who have had access to Sensitive Compartmented Information (SCI) within the last three years. The request is used to determine the person's depth and breadth of knowledge of the SCI he, or she has been exposed, to what the damage would be to national security if the information were to be disclosed, and ultimately, whether or not the person will continue to protect that information. To determine this, a myriad of information is gathered and forwarded through your local Special Security Office (SSO) to your MAJCOM SSO and SSO USAF.

Personal data is collected – usually by the Orderly Room (CCQ). Access and, or clearance data is provided by the SSO. A depth of access – what EXACTLY does the person know, and to what degree – is provided, usually, by the supervisor. CCQ or Commander provides details of the "For Cause" action – the reason for the "For Cause" action, authorizing paragraph, worst characterization of discharge, and the Commander's recommended characterization of discharge. The supporting legal office determines whether the proposed actions are legally sufficient. The Commander provides an evaluation of the information to which the person has been exposed. Further, using the questions listed in AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information,* an assessment of the person is conducted and it is ultimately determined whether or not the person will continue to protect the information to which exposed.

Once all the information is collected, it is forwarded to the MAJCOM SSO who ensures all necessary information has been included in the request and conducts another damage assessment. MAJCOM SIOs have the authority to approve those cases when the damage is considered likely to be "minimal." If determined "serious," the MAJCOM SIO provides a recommendation to the SOIC who is the approval authority. SSO USAF sends approval to the MAJCOM SSO, which is then forwarded to the unit.

How long does it take to obtain approval? Approval for "minimal" cases can usually be obtained between 1–30 days – dependent upon the completeness of the request and MAJCOM SIO's schedule (leaves, TDYs, illness, etc.). "Serious" cases, on the other hand, can take up to two months for approval, depending on the completeness of the request, the schedule of the MAJCOM SIO and SOIC.

A few things can be done to speed up the process at the local level. First, obtain as much of the information needed for the "for cause" request as far in advance as possible – legal sufficiency is not needed to obtain personal data, depth of access, commander's assessment or commander's evaluation.

Next, proofread the request prior to sending it out. Common errors include another person's name in the text, vague details of incident, depth of access does not cover the last three years of access or is not in-depth enough, incorrect authorizing paragraph for discharge, incomplete commander's assessment

and a courtesy copy of the message was not addressed to the right office (should be SSO USAF/INSDM). Any omission of the above will result in the local SSO having to retransmit the request. Last but not least, as soon as legal sufficiency has been obtained, forward the request to the MAJCOM SSO.

As you can see, the process to discharge a person who has been indoctrinated for SCI is slightly more complicated and lengthy compared to those who have not been indoctrinated. By working together as a team, the commander, security office, supervisors, base legal office and orderly room can help ensure less than desirable people are removed from the Air Force as quickly and smoothly as possible.

2.2. Classified Briefings and Sessions by TSgt Ed Santulan, HQ AIA/SOPS

When selecting a location or facility for classified sessions you must ensure it can provide physical control, storage, protection, and a means for dissemination of classified information. This normally means a facility under the security control of an U.S. Government agency or a contractor having an appropriate facility security clearance. Do not use base theaters and other facilities that are normally open to uncontrolled access for classified meetings **unless:**

- There is no secure facility available

- Unauthorized personnel do not have physical access and can be prevented from hearing or seeing the proceedings of the meeting

As a general rule ensure you confirm the clearance and need-to-know of all attendees. Planning ahead in a timely manner ensures the success of your sponsored meetings. Before the start of the session, brief all attendees note taking and electronic recording is prohibited during classified sessions. Unless previous arrangements for handling classified notes have been made. As the sponsor of a meeting, you must ensure all aspects of security are covered and adhered to before, during and after every session. SECURITY is no laughing matter!

3. PHYSICAL SECURITY

3.1. UNDERSTANDING THE PHYSICAL SECURITY DEVIATION PRO GRAM by MSgt Lauren P. Barboza, HQ AIA/SOXS

The physical security deviation program formalizes security program risk acceptance. The inability to meet minimum DoD and Air Force Installation Security Program requirements results in a higher security program risk. Commanders must implement the physical security deviation program where resources are not protected at the assigned protection level.

The purpose of the physical security deviation program is to provide a management tool for installations and MAJCOMs to review, monitor, plan, and program for corrections to deviations from requirements. The governing directive for The Physical Security Deviation Program is AFI 31-101, *The Air Force Installation Security Program.*

Physical Security deviations can be described in one of three categories: Permanent Deviations (Exceptions), Temporary Deviations (Waivers), or Technical Deviations. Permanent deviations should be requested when a security-threatening condition can not be corrected or when correcting the problem would result in an exorbitant cost. Permanent deviations are granted for no more than 3 years. Conditions approved as permanent deviations require compensatory measures.

Units request a temporary deviation when a correctable, security-threatening condition exists. Conditions approved as temporary deviations require compensatory measures. Grant temporary deviations for no more than 1 year.

Units request a technical deviation when a condition exists that does not threaten security but technically differ from established requirements. Conditions approved as technical deviations do not require compensatory measures or corrective actions. Approve technical deviations for an indefinite period of time.

The host SF documents deviations on AF Form 116, **Request for Deviation from Security Criteria**, and submits each deviation for formal approval. The important thing to remember is coordination between the host security forces official, and MAJCOM/SF. The Installation Security Council is an integral part of the process to ensure required deviations are identified and implemented. AFI 31-101, Chapter 6, addresses the deviation program in greater detail.

4. FORCE PROTECTION

4.1. TERRORISM THREAT LEVEL METHODOLOGY OVERVIEW by MSgt Donald M. Shea, HQ AIA/SOXX

This article provides a brief overview of the new DoD Terrorism Threat Level Methodology effective 1 October 2000. This methodology, approved by the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD SO/LIC), was generated by suggestions from both the Intelligence Community and operators in the field to more clearly describe the terrorist threat. The significant changes in the new terrorism threat level methodology include:

Table 1. Terrorism Threat Level Methodology.

A. Reduction of the terrorism threat levels from five to four
B. Focus on terrorist group activity
C. Assessment of terrorist tactics
D. Consideration of DoD presence
E. Incorporation of terrorism warning into methodology

The new system assesses the threat to DoD posed by a terrorist group using the factors of Operational Capability, Intentions, and Activity against the operating environment of the country. These factors are used to identify the collection and analysis of information from all sources concerning terrorist threat. The threat level is set by assessing the Operational Capability, Intentions, Activity, and Operating Environment in sequence, and then reviewing the threat level definitions and applying the one that best describes the situation in a given country. If there is more than one group in the country, each one is assessed and the highest overall threat level is used for the country.

Each factor is scaled within a general guideline from low to high. The assessment of each factor, against the backdrop of the country being rated, actually produces the final threat level. Keep in mind the "Operational Capability" factor determines the "baseline" threat level from which all other factors are influenced. The new terrorism threat levels defined below were developed to reduce uncertainty and misinterpretation at the operational level by clearly describing the terrorist threat.

Table 2. Terrorism Threat Levels.

High:	Anti-US terrorist group is operationally active and uses large casualty producing attacks as their preferred method of operation. There is a substantial DoD presence and the operating environment favors the terrorist.
Significant:	Anti-US terrorist group is operationally active and attack personnel as their preferred method of operation or a group uses large casualty producing attacks as their preferred method and has limited operational activity. The operating environment is neutral.
Moderate:	Terrorist groups are present but there is no indication of anti-US activity. The operating environment favors the host nation/US.
Low:	No group is detected or the group activity is non-threatening.

The analytical approach described above, used by all DoD components, is an essential step in determining the threat level prior to issuing a threat warning. When terrorist groups are operationally active and specifically targeting US interests, a terrorist warning report will be issued. The DoD Terrorism Warning report is part of the methodology and emphasizes the threat, but is not a level itself. When a warning report is issued, the requirement is for a short duration and an automatic expiration of the warning will remain.

4.2. DUPLICATE PROTECTION LEVEL TERMINOLOGY by MSgt Donald M. Shea, HQ AIA/SOXX

The term "Protection Level" is used by separate functions for different purposes. Knowing these differing purposes can prevent confusion and enhance your security posture.

DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems (IS),* identifies five protection levels used when accrediting Information Systems (IS). The concept of Protection Levels within IS applies only to confidentiality. Once you have verified an IS will maintain, process, or transmit intelligence information and its Level of Concern for confidentiality is High, the Designated Accreditation Authority (DAA) must ascertain the appropriate Protection Level for the IS. The DAA will base his decision on the required clearance(s), formal access approval(s), and need-to-know of all direct and indirect users who receive information from the IS without manual intervention and reliable human review. It indicates an implicit level of trust that is placed in the system's technical capabilities. The DAA is responsible for assigning a protection level to each information system that is to be accredited. DCID 6/3, Table 4.1, presents the criteria for determining which of the five protection levels is appropriate for the IS being accredited.

AFI 31-101, *The Air Force Installation Security Program,* identifies specific Air Force resources you must secure and the level of security dedicated to those resources by assigning one of four protection levels. Protection Levels provide the basis for programming security manpower and equipment. Appropriate Air Staff offices review recommendations for permanent protection level designations and concur or non-concur. On the basis of the review, HQ USAF, Directorate of Security Forces, Deputy Chief of Staff for Air and Space Operations (HQ USAF/XOF) assigns or re-designates the protection level.

AFI 31-101, Chapter 17, prescribes security forces, physical security, and special procedures for securing Sensitive Compartmented Information (SCI) Facilities and Intelligence Production Systems

the AF has designated as protection level resources. AFI 31-101, Figure 17.1, identifies protection levels for SCI resources.

The Protection Levels identified in DCID 6/3 is independent from and has no correlation to the protection levels identified in AFI 31-101. Individuals should be cognizant of the differing protection level terminology and apply the level accordingly.

JIMMY R. JONES
Chief of Security