DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AIA RECURRING PERIODICAL 31-1

2nd Quarter 2001

Security

THE SHIELD

NOTICE: This publication is available digitally on the AIA website at: http://pdc.aia.af.mil.

OPR: HQ AIA/SOCD (MSgt Guy Woodbury) Certified by: HQ AIA/SOC (Mr. Robert Eddy)
Pages: 6
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, ACC, 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.

Table 1. JGUBY Messages.

JGUBY 01-08	271926 Feb 01	AIA Form 95
JGUBY 01-09	012024 Mar 01	Clarification of Labeling SCI AIS
JGUBY 01-10	092125 Mar 01	Defense Travel Briefing
JGUBY 01-11	141526 Mar 01	Classification of U-2 SIGINT Capabilities
JGUBY 01-12	211604 Mar 01	Classified Title
JGUBY 01-13	292117 Mar 01	Cellular Telephones Inside AIA Managed SCIFs
JGUBY 01-14	041844 Apr 01	NSA Entry Criteria
JGUBY 01-15	090808 Apr 01	Document Accountability
JGUBY 01-16	192023 Apr 01	Data Call-Operational Failures Mas-Hamilton Locks
JGUBY 01-17	021257 May 01	Clarification NSA Entry Criteria
JGUBY 01-18	031643 May 01	Security Information File and For Cause Data
JGUBY 01-19	041543 May 01	Sentinel Key Operations
JGUBY 01-20	081332 May 01	SSBI and TS PR Workload Transfer to OPM
JGUBY 01-21	242007 May 01	SSBI-PR
JGUBY 01-22	011525 Jun 01	Reporting of Intelligence Security Incidents
* Note:	JGUBY messages	are posted on AIA's products and services homepage on INTELINK

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

Table 2. NOSIZ Messages.

NOSIZ 01-04	011458 Mar 01	USAF SCI Security Management Course (20-22 Mar)
NOSIZ 01-05	062141 Mar 01	Physical Security Seminar Class Announcement
NOSIZ 01-06	031808 Apr 01	USAF SCI Security Management Course (24-26 Apr)
NOSIZ 01-07	251927 Apr 01	Physical Security Seminar Class Announcement
NOSIZ Unnum-bered	111535 May 01	Cancelled SCI Management Course Jun 01
NOSIZ 01-08	221718 May 01	USAF SCI Security Management FY 02 Course Schedule

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

Table 3. ROXAD Messages.

ROXAD 01-01	021749 Mar 01	Classified In Public Media/ Open Source

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

Table 4. AIG 8551 Messages.

AIG 8551 01-02	031901 Apr 01	AIG 8551 Recapitulation 01/ 01 of AIG Eight Five Five One
AIG 8551 01-03	041440 Apr 01	Security Office Digest, First Quarter 2001

1.2. PROPER USAGE OF THE "FOR OFFICIAL USE ONLY" CAVEAT **by MSgt William McCredden, HQ AIA/SOCI**

The purpose of this article to help clarify the proper use of the For Official Use Only (FOUO) caveat. The most common misconception about the FOUO caveat is it is some watered-down form of "classification" people can use to protect information they deem is sensitive but cannot justify as classified. Using the FOUO caveat in this way is NOT acceptable according to Executive Order 12958.

The definition of FOUO as per DoD Regulation 5400.7-R, DoD Freedom of Information Act [FOIA] reads:

"Information that has not been given a security classification pursuant to the criteria of an Executive Order, but may be withheld from the public for one or more of the reasons cited in FOIA exemptions 2 through 9 shall be considered as being For Official Use Only. No other material shall be considered or marked "For Official Use Only" as it is not authorized as an anemic form of classification to protect national security interests." You must justify marking information FOUO using these above named exemptions.

The marking of FOUO material is fairly straightforward. If the document is unclassified, mark the bottom of the front cover, back cover, and the page(s) that actually contain FOUO information. Also portion mark the FOUO material. If FOUO is contained in a classified document, mark page(s) according to the highest classification but portion mark to identify FOUO. Information to be declassified must be reviewed for FOUO material and, if any is found, marked as such on the front cover at the bottom.

Transmitting FOUO can be by any means including unclassified LANs, Nets, and facsimiles. It can be sent by these unclassified electronic means if the material is properly marked and identified as FOUO, and the person receiving the message is the intended recipient and has a "need to know." FOUO can also be transmitted by secure means (STU-III, SIPRNet, etc.) if these same rules are followed. FOUO may be mailed 1st class or parcel post. Bulky shipments may be sent by 4th class mail. These above rules are for transmission purposes only! FOUO may not be posted on any unclassified web sites.

Destruction of FOUO must be accomplished so the material cannot be reconstructed in any manner. Any method authorized for classified material may be used for FOUO. FOUO may be recycled if it can be protected from unauthorized access/disclosure.

I hope this article has helped clear up the proper use of the FOUO caveat. If you have any questions you can check DoD Regulation 5400.7-R. If further clarification is still needed please feel free to contact the HQ AIA FOIA Office at DSN 969-2979 or HQ AIA/SOCI at DSN 969-2011.

2. PERSONNEL SECURITY:

2.1. OPM STEPS UP TO THE BACKLOG PLATE by SMSgt Danny Shine, HQ AIA/SOP

The Department of Defense (DoD) has been working several initiatives to clear the security clearance backlog which has plagued the government for some time. While progress has been made due to some cases being transferred from the Defense Security Service (DSS) to the Office of Personnel Management (OPM), now radical steps have been taken to transfer more cases to OPM. These changes should provide welcome relief to the situation and further reduce the backlog.

Starting 1 May 01, all single scope background investigations (SSBI) and Top Secret Periodic Reinvestigations (PR) are to be sent to OPM. This will include investigations and PRs for both civilians and military personnel and does include cases that have overseas leads. Contractors' SCI/SSBI cases will be sent to OPM as well.

Procedures have been developed to expedite this process. Many authorized requestors have experience sending in PRs and SSBIs to OPM and can advise you on the simplest way to fill out the requested forms.

Cases already in the works at DSS will remain there. Please note after 21 May 01, DSS will not process any case received by them that should have been sent to OPM. Due to resource considerations, DSS will not return misrouted electronic personnel security questionnaires (EPSQ), signed releases, or fingerprint cards to the sender, nor will they be forwarded to OPM.

Personnel security specialists must ensure submissions for SSBIs and Top Secret PRs are now sent to OPM, rather than DSS.

This article is an excerpt from AIA JGUBY date time group 081332Z May 01. This and all JGUBY messages are available for viewing and or downloading on Intelink at the following URL: http://www.aia.ic.gov/products.

2.2. New Data Fields in Sentinel Key by Mrs. Jane Radigan, HQ AIA/SOP

In February 2001, new data fields were added to Sentinel Key (SK) to indicate the date any investigation was transmitted to DSS or OPM. All authorized SK users should fill these fields out when submitting all investigation requests, particularly Periodic Reinvestigations. If you need further information, please refer to the SK web site.

3. PHYSICAL SECURITY

3.1. Portable Electronic Devices in AIA Managed SCIFs by MSgt Timothy Taylor, HQ AIA/SOXX

What is a Portable Electronic Device? According to the Joint DoDIIS/Cryptologic SCI Information Systems Security Standards (JDCSISSS), dated 31 March 2001, portable electronic devices, or PEDs for short, are "cellular telephones, two-way pagers, palm-sized computing devices, two-way radios, audio/video/data recording equipment, personal digital assistants, palm tops, laptops, notebooks, data diaries, and watches with communications software and synchronization hardware, that may be used to telecommunicate".

Our primary concern is focused on the use of palm-sized computing devices, laptops, notebooks, and personal digital assistants. These devices present a degree of risk for compromise of classified or sensitive information. The following guidance is taken from Chapter 15 of the JDCSISSS.

Can government-owned PEDs be brought into the SCIF? Presently, government-owned devices are allowed controlled access into the SCIF. By controlled, we mean incoming PEDs are accounted for

by make, model, and serial number. In addition, only personnel authorized in writing and approved by the SSO are allowed to introduce and remove these items from the SCIF.

Government-owned PEDs must meet certain requirements according to the JDCSISSS. These include:

Government PEDs, associated hardware/software, and media must be controlled

Operation in the SCIF is prohibited unless approved and accredited by the appropriate SCIF accrediting agency

Users and their supervisors must sign a statement acknowledging understanding of restrictions

Connection to any government system must be approved in writing by the unit Information Systems Security Manager (ISSM)

PEDs with wireless, radio frequency (RF), infrared (IR), and voice recording capability will not be used unless these features are turned off or physically disabled

Under certain conditions, government-owned PEDs can be approved for processing classified and approved for connection to government systems. If approved for classified use, these devices and their associated media require transportation and storage that affords protection from the possibility of compromise, sabotage, theft, or tampering.

How about Contractor/Business-owned PEDs? These devices must meet the same requirements as government PEDs. In addition, these PEDs must support specific government contract and be documented in support of the contract prior to entry into the SCIF.

How about Personally-owned PEDs? Currently, personally-owned PEDs are not allowed in our SCIFs, pending further guidance from DIA/DAC-2. If authorized, personal devices will be required to meet the same requirements as government PEDs, but will not require accreditation. Connection of personal PEDs to any information system within the SCIF will be prohibited.

What's the bottom line? Government-owned PEDs are allowed with certain restrictions and must be controlled.

Contractor/business-owned PEDs are allowed with the restrictions, must be controlled, and must be documented in the contract.

Personally-owned PEDs are currently not allowed.

4. FORCE PROTECTION

4.1. THREAT IDENTIFICATION FOR FACILITY AND SITE DESIGN PROCESS by MSgt Donald Shea

Identification and characterization of terrorist threats are the first steps in developing an Antiterrorism Force Protection Program. Once commanders understand the threat, they can assess their facilities' ability to survive an attack. The threat assessment is an essential element in the force protection planning process as it defines the parameters on which effective protective systems are based. Threat identification is the first element within a threat assessment that relates to installation facility planning and design.

4.1.1. THREAT IDENTIFICATION: Identifying the threat focuses on three components (1) Aggressors; (2) tools, weapons, and explosives; and (3) tactics.

Aggressors: Aggressors generally perform hostile acts against people, facilities, and equipment. Their objectives include (1) inflicting injury or death on people; (2) destroying or damaging facilities, property, equipment, or resources; (3) stealing equipment, material, or information; and (4) creating publicity for their cause. Aggressors may use the first three objectives to accomplish the fourth.

Tools, Weapons, and Explosives: To achieve their objectives, aggressors use the following:

Tools such as forced entry tools, vehicles, and surveillance tools

Weapons, such as incendiary devices, small arms, antitank weapons and mortars, and nuclear, biological and chemical agents (also called weapons of mass destruction)

Explosives, such as homemade bombs, hand grenades, and vehicle bombs

Tactics: Tactics refer to the offensive strategies employed by aggressors, reflecting their capabilities and objectives. Some of the more common tactics include:

Moving-vehicle bomb: The moving-vehicle bomb is a suicide attack where an explosive-laden vehicle is driven into a facility, and detonated.

Stationary vehicle bomb: This type of bomb may be detonated by time delay or remote control

Exterior attack: This attack is at close range of a facility or exposed asset. Using clubs, rocks, improvised incendiary devices, hand grenades, or hand-placed bombs, the aggressor attempts to inflict destruction and death**.**

Standoff weapons attack: These attacks are executed using military or improvised direct-and indirect-fire weapons, such as antitank weapons and mortars.

Ballistic attack: Using small arms at varying distances, the aggressor attempts to inflict death.

Covert entry: The aggressor attempts to enter the facility covertly using false credentials. The aggressor may attempt to carry weapons or explosives into the facility.

Mail bombs: Small bombs or incendiary devices are incorporated into envelopes or packages that are delivered to the targeted area.

Supply bombs: Bombs or incendiary devices, generally larger than those found in mail bombs, are incorporated into various containers and delivered to facilities or installations.

Airborne contamination: The aggressor uses chemical or biological agents to contaminate the air supply of a facility or installation.

Waterborne contamination: The aggressor uses chemical, biological, or radiological agents to contaminate the water supply of a facility or insulation.

As outlined in DOD 0-2000.12-H the Department of Defense has identified four factors to establish information analysis and collection of information from all sources concerning the terrorist threat. Look for these four factors in the next Shield.

JIMMY R. JONES
Chief of Security