BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 14-3

1 MAY 1998

Intelligence

CONTROL, PROTECTION, AND DISSEMINATION OF INTELLIGENCE INFORMATION

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ USAF/XOIIS (Ms Elizabeth Hall) Certified by: HQ USAF/XOII (Mr Dennis Alvey)
Supersedes AFPD 14-3, 10 June 1993. Pages: 6
Distribution: F

This policy directive provides guidance for protecting intelligence information. It defines authority lines, roles, and responsibilities for oversight and implementation of programs and procedures to ensure proper controls and protection in preserving the integrity of intelligence collection systems.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

Establishes requirement for AF development of automated systems for efficiency of SCI security management. Designates HQ USAF/XOIIS as Cognizant Security Authority for SCI. Designates HQ USAF/XOIIS, Intelligence Security Division as SCI Security Policy Team, chartered to establish SCI control and release programs for AF. Establishes one Base, one SSO policy. Establishes HQ AIA/SO as OPR for compilation and submission of quarterly intelligence information compromise and security education training reporting. Discontinues requirement for HAF-IN(Q) 9327, Results of Security Management Inspection Report.

1. Intelligence information is crucial to an effective Air Force fighting force. It must be controlled and protected to preserve the integrity of the intelligence collection system. Some intelligence information designated as Sensitive Compartmented Information (SCI) requires additional control and protection. This Directive establishes policy for the control, protection, and dissemination of Air Force intelligence information.

2. The Air Force will maintain effective control of the dissemination of intelligence information among US intelligence community components, US forces outside the intelligence community requiring the information, foreign nationals, foreign governments, and contractors.

3. Intelligence information will be secured, handled, and disseminated only by properly designated users.

3.1. The Air Force will validate organizations authorized to receive and handle SCI, indoctrinate personnel for access to SCI, and train them to protect against unauthorized disclosures. In addition, the

Air Force will maintain SCI facilities and communications capabilities certified to support SCI handling.

3.2. The Air Force will develop automated systems to sustain efficiency of intelligence security management.

3.3. The Air Force will develop procedures to report compromises of classified intelligence information or serious failures to comply with the provisions of security regulations which are likely to result in compromise.

4. This directive establishes the following responsibilities and authorities:

4.1. Director of Intelligence, Surveillance and Reconnaissance, DCS/Air and Space Operations, is the Air Force Senior Official of the Intelligence Community (SOIC), responsible for intelligence information security for the Air Force.

4.2. HQ USAF/XOII (Associate Director for Intelligence) is the Air Force authority for issues involving the release of intelligence information.

4.2.1. HQ USAF/XOIIS is the Air Force Cognizant Security Authority (CSA) for SCI, the single principal designated by the SOIC to serve as responsible official for SCI security program management.

4.2.2. HQ USAF/XOIIS will establish intelligence security control and release programs and oversee Major Command (MAJCOM), Field Operating Agency (FOA), and Direct Reporting Unit (DRU), intelligence security programs. In addition, they will represent the Air Force in national and Department of Defense (DoD) intelligence security forums.

4.3. Air Force activities will control intelligence information in accordance with governing directives and report intelligence information security violations to HQ Air Intelligence Agency Security Office (AIA/SO).

4.3.1. Air Force activities will conduct quarterly security awareness training with emphasis on reducing or preventing recurrence of violations. MAJCOM SSOs will report number of personnel receiving security education training per quarter to HQ AIA/SO. HQ AIA/SO will use training satistics to identify and document correlations between security violation trends and the conduct security education training.

4.4. The host Major Air Command (MAJCOM) for an installation will ensure SCI communications and security management are provided as necessary to support any Air Force unit mission on that installation. The host command may contract with a tenant organization to provide SCI communications and SCI security management oversight at an Air Force installation for the host command. Tenant organizations will work with the host MAJCOM to ensure there is only one AF SSO per installation. The Air Force Office of Special Investigations will retain a separate SSO to support its counterintelligence and force protection responsibilities.

4.5. Commanders/Senior Intelligence Officers (SIO) will ensure facilities where intelligence information is used meet security requirements and that personnel are trained to protect the information. Commanders/Senior Intelligence Officers may enter into agreements (Memorandums Of Agreement) with other United States security organizations to provide or receive security services. The sharing or consolidation of security resources and skills required to meet the needs of the participant's individual governing directives is encouraged.

4.6. HQ USAF/XOIIS will establish objectives and requirements for the electronic exchange and dissemination of security and intelligence information through automated security management systems.

5. This policy applies to all Air Force activities and personnel who produce, receive, or disseminate intelligence information.

5.1. Air Force Service Cryptologic Elements will also comply with National Security Agency directives. Conflicts will be resolved by the Cognizant Security Authorities.

6. This policy directive implements Director of Central Intelligence Directive (DCID) 1/7, Security Controls on the Dissemination of Intelligence Information; DCID 1/14, Personnel Security Standards and Procedures Governing Eligibility for Access to SCI; DCID 1/16, Security Policy on Intelligence Information in Automated Systems and Networks; DCID 1/19, Security Policy for Sensitive Compartmented Information; DCID 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities; and National Telecommunications and Information Systems Security Instruction, (NTSSI) No. 7000.

7. This policy directive interfaces with DoD S-5105.21-M-1, Sensitive Compartmented Information Administrative Security Manual; AFPD 31-4, Information Security; AFI 14-302, Control, Protection, and Dissemination of Sensitive Compartmented Information; and AFI 14-303, Release of Collateral Intelligence to US Contractors.

8. See attachment 1 for measures used to assess compliance with this policy.

F. WHITTEN PETERS
Acting Secretary of the Air Force

Attachment 1

MEASURING AND DISPLAYING POLICY EFFECTIVENESS

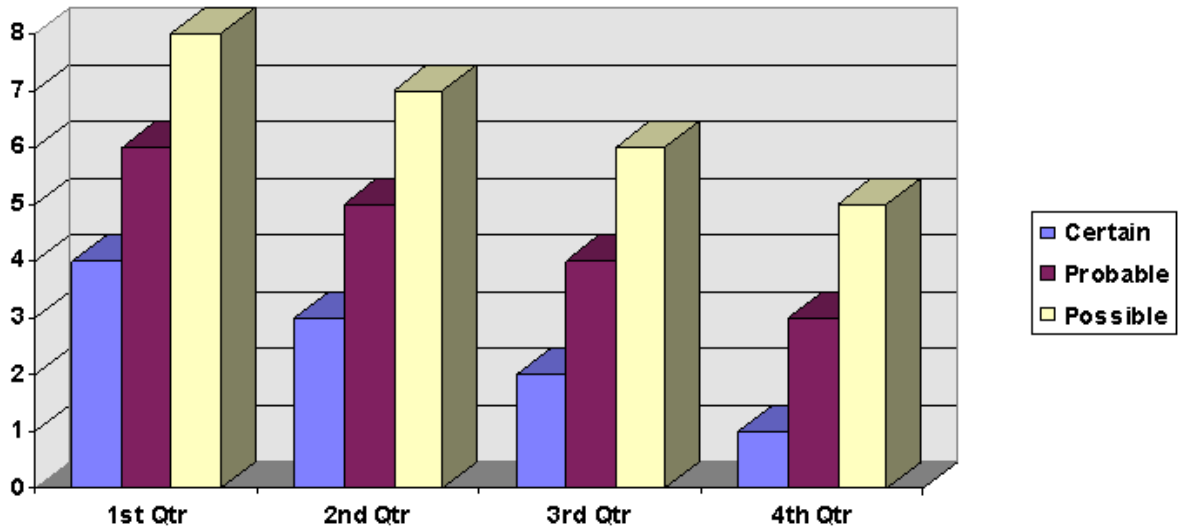
A1.1. The Air Force will measure the success of controlling, protecting, and disseminating intelligence information by evaluating the number of intelligence information compromises occurring quarterly . The data will be displayed on bar charts that show the number of certain, probable, or possible compromises and the category of each compromise. Analysis will focus on identifying trends in categories of compromise. The objective is to reduce the number of intelligence information compromises.

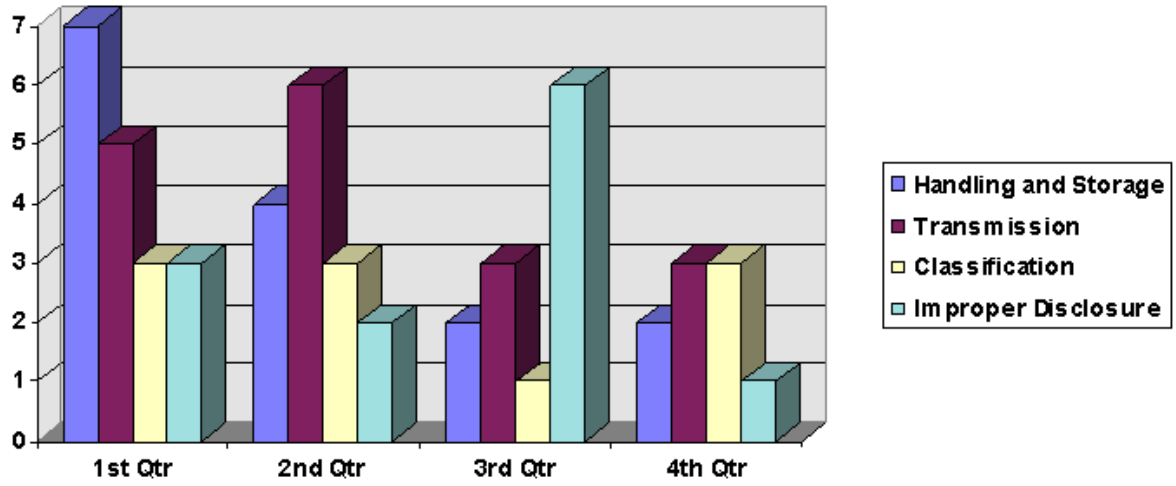
A1.2. MAJCOMs, FOAs, and DRUs will report all SCI security violations as defined in DoD S5102.21-M-1, Sensitive Compartmented Information Administrative Security Manual, and AFMAN 14-304, The Security, Use, and Dissemination of Sensitive Compartmented Information.

A1.3. HQ AIA/SO will provide a two-part quarterly report, RCS: HAF-XO(Q) 9326, that identifies trends in security violations and the impact of security education and training programs on security violation trends. Part I: Compiled data from initial and follow-up security violations reports received from MAJCOMs, FOAs, and DRUs. Part II: Compiled data reflecting number of individuals receiving security education training. Submit quarterly Intelligence Information Compromise and Security Education Report to HQ USAF/XOIIS. This report is designated emergency status code D. Immediately discontinue reporting data requirements during emergency conditions.

Figure A1.1. Sample Metric of Number of Security Incidents.

Number of Intelligence Information Compromises





One set of graphs would reflect SCI incidents and another would reflect Collateral Intelligence Information incidents. (The collateral metrics would be caveated to indicate that compromises reflected will be included in reporting required by AFPD 31-4)

Figure A1.2. Sample Metric of Number of Individuals Receiving Security Education Training.

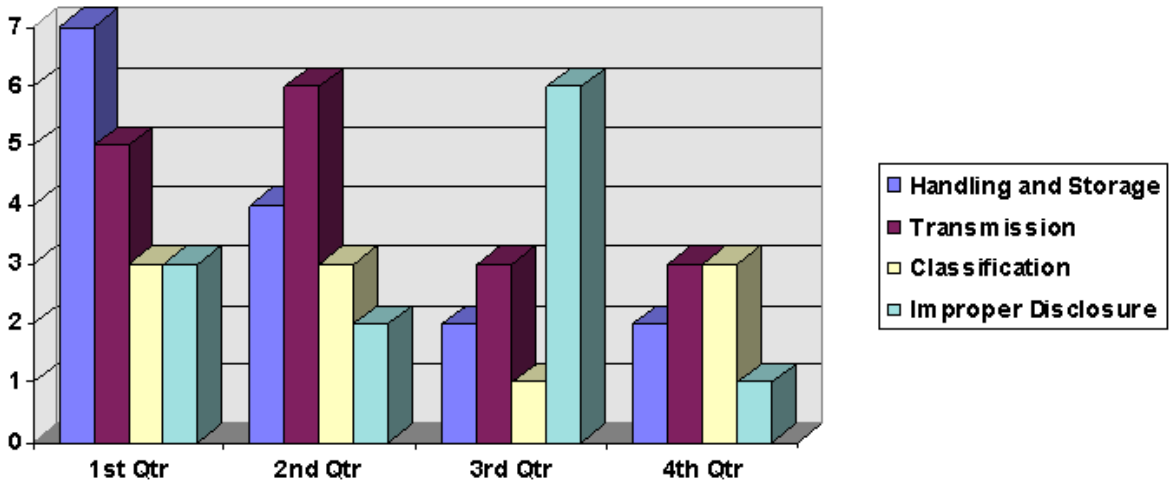


Chart will depict compilation of quarterly security education training received. The categories here mirror the categories assigned to security incidents. Actual training reported will not always be one of these categories by name. The specific training conducted will be assigned the category it best serves.