INTERNET DOCUMENT INFORMATION FORM

A . Report Title: Air Force Policy Directive 31-4 Information Security

B. DATE Report Downloaded From the Internet 3/17 /98

Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): Secretary of the Air Force

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: UM **Preparation Date**: 3/18/98

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 31-4

1 AUGUST 1997

Security

INFORMATION SECURITY

OPR: HQ USAF/SFI
(Ms Deborah Ross)
Supersedes AFPD 31-4, 1 March 1995.

Certified by: HQ USAF/SFI
(Mr Eugene J. White Jr)
Pages: 6
Distribution: F

This directive provides Air Force policy for protecting sensitive Air Force information. It also assigns responsibility for implementing and managing the Information Security Program. This directive implements national policies in the Executive Order 12958, *Classified National Security Information*, 20 April 1995, and Federal Register Part VI, Office of Management and Budget, 32 CFR Part 2001, Information Security Oversight Office; *Classified National Security Information*; Final Rule, 13 October 1995. It interfaces with various other security publications such as DoD 5200.1-R, *DoD Information Security Program Regulation*; AFPD 31-5, *Air Force Personnel Security Program*; AFPD 31-6, *Air Force Industrial Security Program*; and AFI 31-401, *Information Security Program Management*. Policy for classified information designated Sensitive Compartmented Information is managed under the provisions of Director, Central Intelligence Directive 1/19, *Security Policy for Sensitive Compartmented Information*, 19 February 1987, and USAFINTEL 201-1, *The Security, Use, and Documentation of Sensitive Compartmented Information (SCI)*, 1 May 1990. (Copies of these publications are available from the supporting Special Security Office.) Compliance with these policies is mandatory for all Air Force military and civilian personnel.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

1. Air Force personnel must identify and protect classified information as required by national policies.

2. All Air Force activities that classify and/or maintain classified holdings will identify and review classified information that is more than 25 years old and has been determined to have permanent historical value under Title 44, United States Code.

3. The Office of the Secretary of the Air Force (SAF/AA) is designated the Air Force Senior Security Official responsible for ensuring implementation of the Information Security Program.

4. The Air Force Director of Security Forces (HQ USAF/SF) is responsible for policy, resource advocacy, and oversight of this program.

5. Commanders of major commands (MAJCOM), direct reporting units (DRU), field operating agencies (FOA), and installations are responsible for establishing Information Security Programs, identifying requirements, and executing their programs to comply with this policy.

6. The Chief of Security Police, senior security police official or Director/Chief of Acquisition Security is designated the Information Security Program Manager (ISPM) at all levels of command. ISPMs manage Information Security Program implementation and provide oversight within their commands.

7. Each unit commander or head of staff office will appoint a security manager to manage the Information Security Program. Appointing officials will ensure security managers receive required training.

8. See Attachment 1 for ways to measure compliance with this policy.

RICHARD A. COLEMAN, Brig General, USAF
Director of Security Forces

Attachment 1

MEASURING AND DISPLAYING POLICY SUCCESS

A1.1. The Air Force will measure success of information security policy by evaluating the number of violations and infractions that occur within the Air Force. These are defined by Executive Order 12958, Section 5.1.(b)(1) - (2) and 5.1.(c).

A1.1.1. Major commands (MAJCOM), direct reporting units (DRU), and field operating agencies (FOA) will submit a report semiannually to HQ USAF/SFI by 31 January and 31 July of each calendar year. All will report on the

A1.1.1.1. Number and type of violations.

A1.1.1.2. Number and type of infractions.

A1.1.2. Reporting activities will categorize each type of violation and infraction under one of the following categories:

A1.1.2.1. Unauthorized Access (This type will always be considered a violation).

A1.1.2.2. Mismarking.

A1.1.2.3. Unauthorized Transmission.

A1.1.2.4. Improper Storage.

A1.1.2.5. Unauthorized Reproduction.

A1.1.2.6. Improper Classification.

A1.1.2.7. Improper Destruction.

A1.1.2.8. Other.

NOTE:

Count violations and infractions that could fall under several category types, under the most serious category. In a footnote, identify the other categories. For example, the incident is a security violation that started as a result of mismarking a classified document. The incident resulted in unauthorized access. Count the incident under unauthorized access and identify in a footnote that 1 under the unauthorized access category also falls under mismarking.

A1.2. The Air Force will measure the results of automatic declassification reviews on all information that is more than 25 years old and of permanent historical value.

A1.2.1. For the next five years the Air Force is committed to declassifying and releasing each year at least 20% of the amount of classified information it holds that is 25 years old and permanently historical in value. The Annual Declassification Review Summary Metric will monitor the Air Force's effort in reaching its annual 20% goal.

A1.2.2. All Air Force activities--MAJCOMs, DRUs, and FOAs, that classify and/or maintain classified holdings will submit the results of their declassification reviews to HQ USAF/SFI. Reports for calendar year 1996 are to be submitted by the 15th day of the first month following the end of each

calendar quarter. For calendar years 1997-2000, reports will be submitted semiannually by 31 January and 31 July of each year. All will report on:

A1.2.2.1. The total number of reviewed pages that will be exempt from automatic declassification. The exemption category(ies) must be identified in the report.

A1.2.2.2. The total number of reviewed pages that will be declassified.

A1.2.2.3. The total number of pages that will be downgraded.

A1.3. Reporting will be continued during emergency conditions using emergency status code C-1 priority. Do not report during MINIMIZE. Measurement data will be provided by reporting activities described in paragraphs A1.1. and A1.2. to HQ USAF/SFI via RCS: HAF-SPI(SA)9222, *The Information Security Measurement Report.*

A1.4. Reporting activities are encouraged to provide their ideas on how to improve the measurement method.

Figure A1.1. Sample Metric of Violations and Infractions by Type.

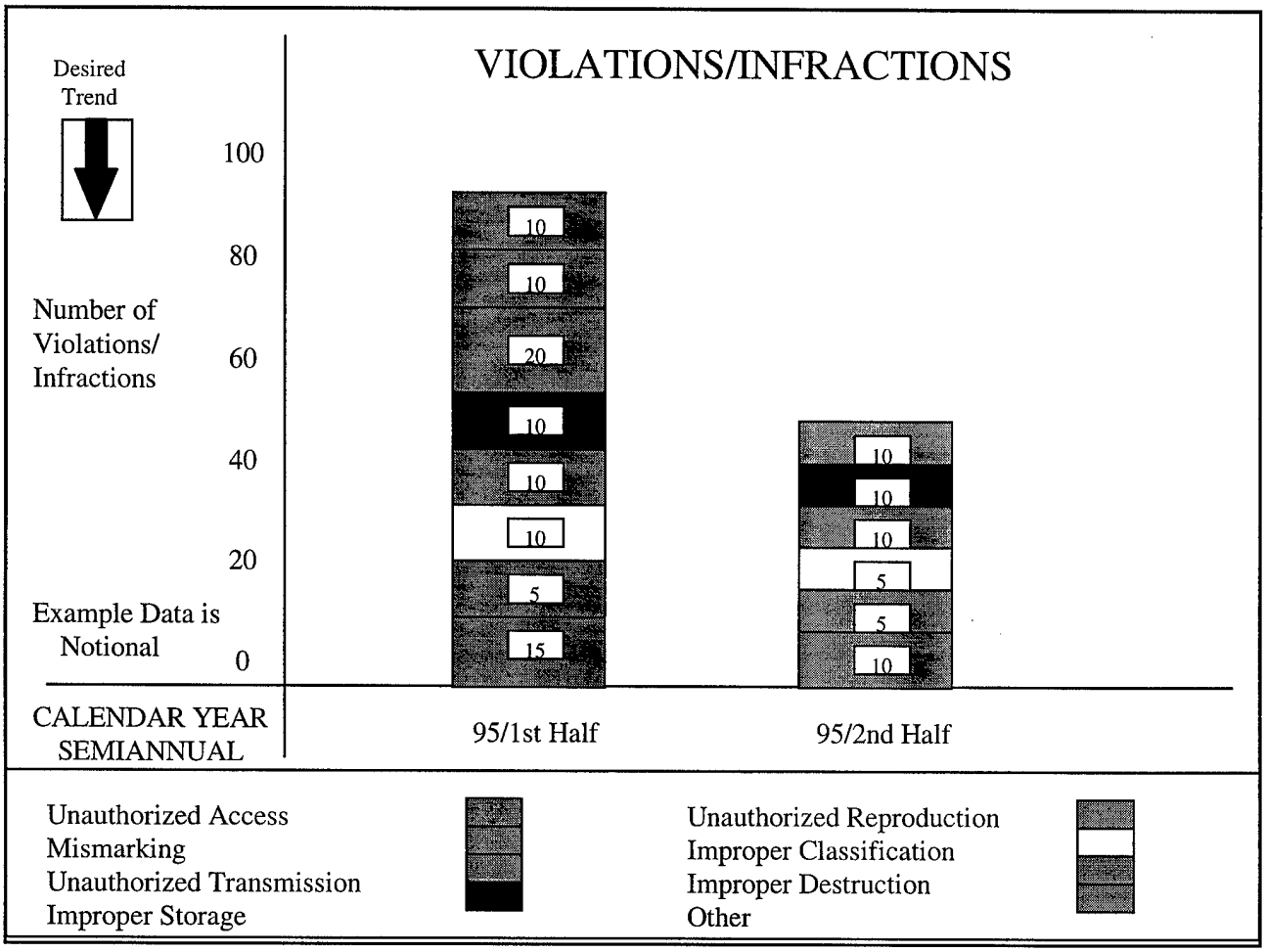
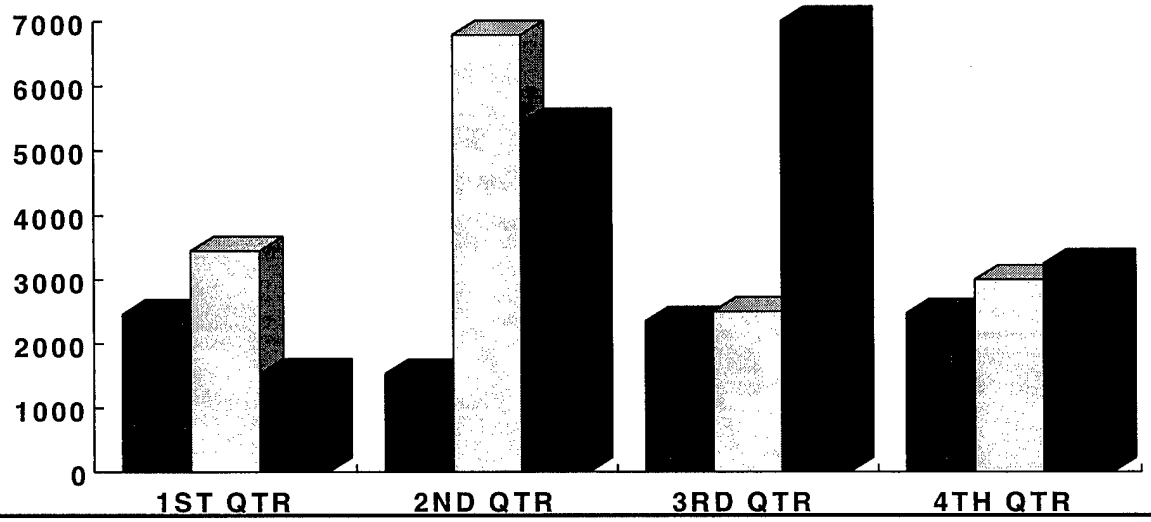


Figure A1.2. Sample Metric of Air Force Annual Declassification Review Summary.

[NOTIONAL DATA]

AIR FORCE ANNUAL DECLASSIFICATION REVIEW SUMMARY



TOTAL NUMBER OF PAGES REVIEWED QUARTERLY FOR FY 96 *(NOTIONAL DATA)*

EXEMPT	2453	1530	2345	2457
DECLASS	3456	6785	2500	3000
DOWNGRADE	1534	5432	7000	3250
TOTAL	7443	13747	11845	8707