

**1 SEPTEMBER 1998**



**Security**

**INFORMATION SECURITY**

---

**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/SFI (Mrs Deborah Ross)

Certified by: HQ USAF/SFI  
(Mr Eugene J. White Jr)

Supersedes AFPD 31-4, 1 August 1997

Pages: 7  
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 revision clarifies the reporting requirements for metric data on the Automatic Declassification Program (**Attachment 1**). A | denotes a revision from the previous edition.

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 Administrative Assistant to 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 Forces, senior security forces 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 2** for ways to measure compliance with this policy.

F. WHITTEN PETERS  
Acting Secretary of the Air Force

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Executive Order 12958, *Classified National Security Information*, 20 April 1995

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

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*

AFI 31-401, *Information Security Program Management*

DCID 1/19, *Security Policy for Sensitive Compartmented Information*, 19 February 1987

USAFINTEL 201-1, *The Security, Use, and Documentation of Sensitive Compartmented Information (SCI)*, 1 May 1990

***Abbreviations and Acronyms***

**AFI**—Air Force Instruction

**AFPD**—Air Force Policy Directive

**CFR**—Code of Federal Regulations

**DoD**—Department of Defense

**DRU**—Direct Reporting Unit

**FOA**—Field Operating Agency

**ISPM**—Information Security Program Manager

**MAJCOM**—Major Command

**SCI**—Sensitive Compartmented Information

**USAFINTEL**—United States Air Force Intelligence

**Attachment 2****MEASURING AND DISPLAYING POLICY SUCCESS**

**A2.1.** 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).

A2.1.1. 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

A2.1.1.1. Number and type of violations.

A2.1.1.2. Number and type of infractions.

A2.1.2. Reporting activities will categorize each type of violation and infraction under one of the following categories:

A2.1.2.1. Unauthorized Access (This type will always be considered a violation).

A2.1.2.2. Mismarking.

A2.1.2.3. Unauthorized Transmission.

A2.1.2.4. Improper Storage.

A2.1.2.5. Unauthorized Reproduction.

A2.1.2.6. Improper Classification.

A2.1.2.7. Improper Destruction.

A2.1.2.8. 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.

**A2.2.** 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. The chart at **Figure A2.2.** will monitor the Air Force's progress.

A2.2.1. 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 fiscal years 1997-2000, will be submitted semiannually as follows:

A2.2.1.1. Report data for 16 Oct 97 - 16 Apr 98 by the end of May 98.

A2.2.1.2. Report data for 17 Apr 98 - 15 Oct 98 by the end of Nov 98.

A2.2.1.3. Report data for 16 Oct 98 - 16 Apr 99 by the end of May 99.

A2.2.1.4. Report data for 17 Apr 99 - 15 Oct 99 by the end of Nov 99.

A2.2.1.5. Report data for 16 Oct 99 - 16 Apr 00 by the end of May 00.

A2.2.2. All reporting activities will include the following items in these reports:

A2.2.2.1. The total number of pages reviewed during the reporting period.

A2.2.2.2. The total number of reviewed pages that do not fall under the Automatic Declassification provision and should not have been included in the latest baseline count.

A2.2.2.3. The total number of reviewed pages that will be referred to another agency or activity for declassification review.

A2.2.2.4. The total number of reviewed pages that will be exempted from automatic declassification. Also show the exemption categories.

A2.2.2.5. The total number of reviewed pages that will be declassified.

**NOTE:**

Downgraded pages should be included in the exemption category since that is the only way they can remain classified.

**A2.3.** 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 **Figure A2.1.** and **Figure A2.2.** to HQ USAF/SFI via RCS: HAF-SFI(SA)9222, *The Information Security Measurement Report*.

**A2.4.** Reporting activities are encouraged to provide their ideas on how to improve the measurement method.

Figure A2.1. Sample Metric of Violations and Infractions by Type.

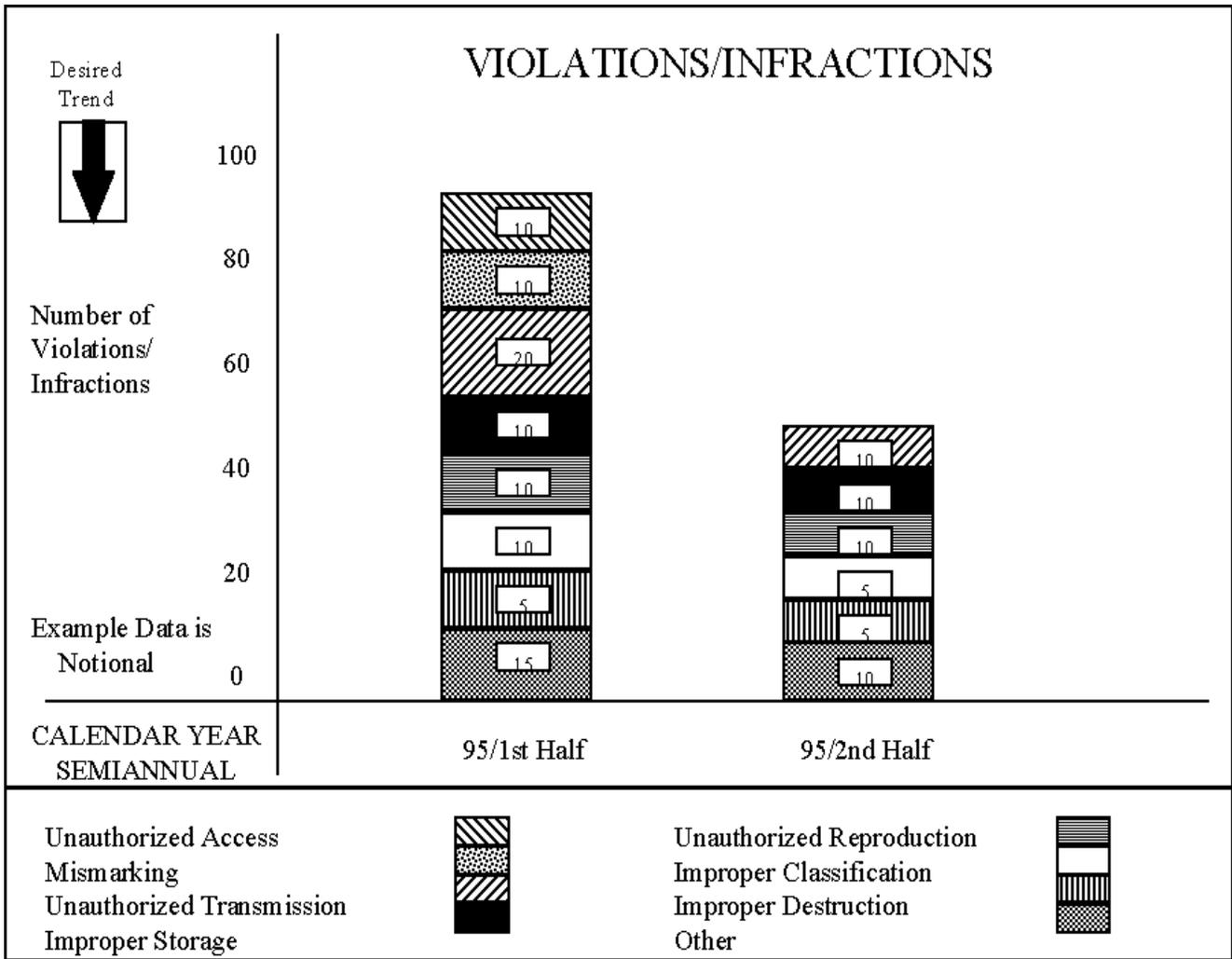


Figure A2.2. Sample Metric of Air Force Declassification Program Progress.

