BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-205

1 AUGUST 1997

Communications and Information

INFORMATION PROTECTION METRICS AND MEASUREMENTS PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: HQ AFCA/SYSC CMSgt James Hogan

Certified by: HQ USAF/SCXX
Lt Col Francis X. McGovern
Pages: 9
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*, and establishes the Air Force Information Protection Metrics and Measurements Program. It prescribes reporting procedures and formats for use within this program, and explains how this program relates to information protection. This instruction applies to all activities that use, operate, or manage information systems. You may use extracts from this Air Force instruction (AFI). Refer questions and comments on the technical contents of this instruction, and recommended changes and conflicts between this AFI and other Air Force publications on AF Form 847, **Recommendation for Change of Publication**, through appropriate command channels to Headquarters Air Force Communications Agency (HQ AFCA/SYS), 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234. Send an information copy to Headquarters Air Force Communications and Information Center (HQ AFCIC/SYNI), 1250 Air Force Pentagon, Washington DC 20330-1250. See **Attachment 1** for a glossary of references, abbreviations, acronyms, and terms. **Attachment 2** contains information on preparing accreditation and training reports.

SUMMARY OF REVISIONS

This is the initial publication of AFI 33-205.

1. General Information.

1.1. Introduction. AFPD 33-2 establishes Air Force information protection (IP) policy. The Air Force Information Protection Metrics and Measurements Program measures compliance with and the effectiveness of IP policy. The accurate collection of security metric and measurement information is critical to the success of information protection metrics and measurements. Equally as important is the trend analysis feedback and changes in security policy that come about as a result.

1.2. Applicability and Scope. This instruction applies to all Air Force organizations that use, operate, or manage information systems. Major command (MAJCOM) responsibilities outlined in this instruction also apply to field operating agencies (FOA) and direct reporting units (DRU) that elect to manage their own IP programs. Otherwise, FOAs and DRUs fall under the purview of the wing IP office.

1.3. Terms Explained. See **Attachment 1** and Air Force Manual (AFMAN) 33-270, *Command, Control, Communications, and Computer (C4) Systems Security Glossary*.

1.4. Relationship to Other Directives. This instruction delineates the process of collecting and reporting information protection measurement data to facilitate reporting required by AFPD 33-2. AFI 33-212, *Reporting COMSEC Incidents*, contains the communications security (COMSEC) incident reporting procedures. COMSEC audit and, or functional review reporting requirements are outlined in AFI 33-213, *Communications Security (COMSEC) Functional Review Program*. Air Force Systems Security Instruction (AFSSI) 5102, *Computer Security (COMPUSEC) Program for Operational Systems*, contains accreditation and reporting requirements for Air Force automated information systems (AIS). AFSSI 5021, *Vulnerability and Incident Reporting* (to be replaced by AFMAN 33-225 when published), provides details on how to report vulnerabilities and incidents. AFI 33-204, *The C4 Systems Security Awareness, Training, and Education (SATE) Program*, details the awareness training reporting requirements. Other IP publications are listed in Air Force Index (AFIND) 2, *Numerical Index of Standard and Recurring Air Force Publications*, and AFIND 5, *Numerical Index of Specialized Information Protection Publications*.

2. Roles and Responsibilities.

2.1. HQ AFCIC/SYNI:

2.1.1. Establishes and directs the Air Force IP Program.

2.1.2. Briefs appropriate Air Staff personnel concerning compliance with and effectiveness of IP policy.

2.1.3. Evaluates and directs IP policy changes based on metrics and measurement feedback.

2.2. HQ AFCA:

2.2.1. Manages the Air Force Information Protection Metrics and Measurements Program.

2.2.2. Consolidates information collected from MAJCOM IP offices and the Air Force Information Warfare Center (AFIWC).

2.2.3. Analyzes compliance with, and effectiveness of, IP policy based on measurement information.

2.2.4. Identifies trends based on this analysis.

2.2.5. Advises HQ AFCIC/SYNI annually, or on request, of conclusions reached based on this analysis.

2.2.6. Provides HQ AFCIC/SYNI with recommended IP policy and procedural changes.

2.2.7. Provides trend analysis data to HQ AFCIC/SYNI, MAJCOMs, FOAs, and DRUs.

2.3. HQ Air Intelligence Agency (AIA). HQ AIA is responsible for and has directed the AFIWC/EA to:

2.3.1. Collect, consolidate, and analyze AIS intrusion and malicious logic attack measurement data.

2.3.2. Provide measurement statistics and analysis results to HQ AFCA/SYS.

2.4. MAJCOM IP Office:

2.4.1. Implements and manages IP metrics and measurements as part of its command IP program.

2.4.2. Collects and consolidates IP measurement information (for example, awareness training and AIS accreditation) and reports to HQ AFCA/SYS.

2.4.3. Reports intrusions and malicious logic attacks to the Air Force Computer Emergency Response Team (AFCERT).

2.5. Wing IP Office:

2.5.1. Acts as the base focal point for the data collection.

2.5.2. Reports awareness training and AIS accreditation information to their MAJCOM.

2.5.3. Reports intrusion and malicious logic information according to AFSSI 5021.

2.5.4. Reports COMSEC incidents according to AFI 33-212.

2.6. Air Force Organizations:

2.6.1. Implement and manage organizational IP programs.

2.6.2. Collect and report training measurement data to the wing IP office.

2.6.3. Identify and accredit all Air Force AISs within the organization, making sure accreditation information is entered in the Information Processing Management System (IPMS), and report measurement data to the wing IP Office.

2.6.4. Detect and report AIS intrusions (attempted or actual) and malicious logic attacks according to AFSSI 5021.

2.6.5. Detect and report COMSEC incidents according to AFI 33-212.

3. Reporting Procedures.

3.1. IP Security Awareness, Training, and Education (SATE). Every Air Force organization must appoint a unit SATE program manager according to AFI 33-204. The manager will make sure all assigned personnel receive initial and refresher awareness training. The data will include the total number of personnel receiving initial training and the total number of personnel receiving refresher training. Each unit SATE program manager will collect and forward the data to the wing IP office who will consolidate training statistics for the wing and report them to their MAJCOM IP office. The MAJCOM will consolidate the MAJCOM training statistics. MAJCOMs report using Report Control Symbol (RCS): HAF-SC(A)9604, *Annual Assessment of Air Force Information Protection Report*. Unless otherwise directed, the report will cover the period 1 January to 31 December and will be submitted to HQ AFCA/SYS by 1 February of each year. (***Note: See AFI 33-204, Figure 1 for sample of report format.)***

3.2. AIS Accreditation. Every Air Force organization will appoint a unit COMPUSEC manager according to AFSSI 5102. The unit COMPUSEC manager will determine the total number of classi-

fied and unclassified AISs assigned to their unit. They will also determine the total number of systems that have valid designated approving authority (DAA) accreditations (interim or final) on file in the two categories (classified and unclassified). The unit COMPUSEC manager will report accreditation statistics to the wing IP office. The wing IP office will consolidate the accreditation statistics and report them to their MAJCOM IP office. The MAJCOM IP office will consolidate MAJCOM accreditation statistics and report them on RCS: HAF-SC(A)9604. Unless otherwise directed, the report will cover the period 1 January to 31 December and will be submitted to HQ AFCA/SYS by 1 February of each year.

3.3. AIS Intrusions. AIS users will report intrusions according to AFSSI 5021. AFIWC will examine and compile the data and report to HQ AFCA/SYS. Intrusion data is collected in two categories: controlled and uncontrolled. Controlled intrusion data will include the number of intrusion attempts; the number of attempts that were detected and, or reported; the number of attempts that were successful; the number of successful attempts that gained limited access to the AIS; and the number of successful attempts that gained total control (root-level privileges) of the AIS. Uncontrolled intrusion data will include the number of attempts reported, the number of attempts that were successful, the number of successful attempts that gained limited access to the AIS, the number of successful attempts that gained total control of the AIS, and the number of probing (that is, finger, who is, and so forth) events. Statistics should include only validated intrusions; false positives are not included. AFIWC/EA will submit these statistics on RCS: HAF-SC(A)9604 (see Attachment 3 for format). Unless otherwise directed, the report will cover the period of 1 January to 31 December. The reports are due to HQ AFCA/SYS by 1 February of each year.

3.4. Malicious Logic Incidents. AIS users will report these incidents according to AFSSI 5021. AFIWC/EA will examine and compile the data and report to HQ AFCA/SYS. Data will include the number of incidents reported and the total number of systems affected. AFIWC/EA will submit these statistics on RCS: HAF-SC(A)9604. Unless otherwise directed, the reporting period is 1 January to 31 December. The reports are due to HQ AFCA/SYS by 1 February of each year.

3.5. Audits and, or Functional Reviews. Audits and, or functional reviews are conducted according to AFI 33-213 and AFKAG-1, *Air Force Communications Security (COMSEC) Operations*. MAJCOMs conduct audits and, or functional reviews on each Air Force COMSEC account under their control. MAJCOMs provide audit and, or functional review reports and follow-ups to HQ AFCA/SYS, who compiles and analyzes the data.

3.6. COMSEC Incident Reporting. COMSEC users report incidents to the wing COMSEC manager. The wing COMSEC manager reports these incidents according to AFI 33-212. HQ AFCA/SYS evaluates incidents and compiles COMSEC incident statistics.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS AND TERMS

References

AFIND 2, *Numerical Index of Standard and Recurring Air Force Publications*

AFIND 5, *Numerical Index of Specialized Information Protection Publications*

AFKAG-1, *Air Force Communications Security (COMSEC) Operations*

AFI 33-204, *The C4 Systems Security Awareness, Training, and Education (SATE) Program*

AFI 33-212, *Reporting COMSEC Incidents*

AFI 33-213, *Communications Security (COMSEC) Functional Review Program*

AFMAN 33-270, *Command, Control, Communications, and Computer (C4) Systems Security Glossary*

AFPD 33-2, *Information Protection*

AFSSI 5021, *Vulnerability and Incident Reporting*

AFSSI 5102, *Computer Security (COMPUSEC) Program for Operational Systems*

Abbreviations and Acronyms

AFCERT—Air Force Computer Emergency Response Team

AFIWC—Air Force Information Warfare Center

AFI—Air Force Instruction

AFIND—Air Force Index

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

AFSSM—Air Force Systems Security Manual

AIS—Automated Information System

COMPUSEC—Computer Security

COMSEC—Communications Security

CSSO—Computer System Security Officer

DAA—Designated Approving Authority

DRU—Direct Reporting Unit

FOA—Field Operating Agency

HQ AFCA—Headquarters Air Force Communications Agency

HQ AFCIC—Headquarters Air Force Communications and Information Center

HQ AIA—Headquarters Air Intelligence Agency

IP—Information Protection

IPMS—Information Processing Management System

MAJCOM—Major Command

SATE—Security Awareness, Training, and Education

Terms

Malicious Logic— Hardware, software, or firmware that is intentionally included in an automated information system for an unauthorized purpose (for example, "Trojan horses," "viruses," and "worms").

Trojan Horse— Computer program containing an apparent or actual useful function that contains additional (hidden) functions that allow unauthorized collection, falsification or destruction of data.

Virus— Self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.

Worm— Independent program that replicates from machine to machine across network connections often clogging networks and computer systems as it spreads.

Attachment 2

ACCREDITATION AND TRAINING REPORT

A2.1. Submission Requirements. Report Control Symbol (RCS): HAF-SC(A)9604, *Annual Assessment of Air Force Information Protection Report*, is submitted by Air Force organizations, wing, and major command (MAJCOM) information protection (IP) offices to report IP security awareness training and automated information system (AIS) accreditation measurement data to the next higher level. The MAJCOM IP offices will send the final report to HQ AFCA/SYS by 1 February of each year. Paragraphs 3.1 and 3.2 of this instruction detail what information will be collected and reported.

A2.2. Emergency Status Code. This report is designated emergency status Code C-2. Continue reporting during emergency conditions, delayed precedence. Submit data requirements as prescribed, but they may be delayed to allow the submission of higher precedence reports.

A2.3. MINIMIZE. During MINIMIZE, forward reports via non-electrical means.

Attachment 3

SAMPLE FORMAT AUTOMATED INFORMATION SYSTEM (AIS) INTRUSION AND MALI-COIUS LOGIC REPORT (HAF-SC[A]9604)

(LETTERHEAD)

MEMORANDUM FOR:

FROM:

SUBJECT: Automated Information System (AIS) Intrusion and Malicious Logic Report (HAF-SC[A]9604)

1. Reporting Period: 1 January through 31 December.

2. Automated Information System Intrusions.

a. Controlled:

(1) Attempts:

(2) Attempts Reported:

(3) Successful (Limited Access):

(4) Successful (Total Control):

b. Uncontrolled:

(1) Attempts Reported:

(2) Successful (Limited Access):

(3) Successful (Total Control):

(4) Probing Events:

c. Trends, Conclusions, and General Comments:

3. Malicious Logic Attacks.

a. Total Number of Reported Incidents:

b. Total Number of Systems Affected:

c. Trends, Conclusions, and General Comments:

(Signature Block)