BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 33-2

1 DECEMBER 1996

Communications and Information

INFORMATION PROTECTION

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/SCTW (Mr Neil C. Knowles)

Certified by: HQ USAF/SC
(Lt Gen John S. Fairfield)

Supersedes AFPD 33-2, 13 August 1993.

Pages: 16
Distribution: F

SUMMARY OF REVISIONS

This revision updates the entire Policy Directive and changes the title of this directive from C4 Systems Security to Information Protection.

1. Policy. Information demands to support Air Force operations have intensified at an exponential rate. To satisfy this demand, the Air Force needs a transparent infosphere that must provide accurate, timely, and secure information in any required form, at any time and place. To assure the availability, integrity, and confidentiality of information and information dependent systems, and the information required to support operations, the following information protection (IP) policy is established:

1.1. Train Information systems users protect information and resources against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons.

1.2. Information systems users protect them at a level commensurate with the risk and the magnitude of harm that could result from disclosure, loss, misuse, alteration, or destruction of the information or systems.

1.3. Information systems users prevent unauthorized access to and introduction of malicious logic into information systems.

1.4. Certify and accredit Air Force information systems before operational use.

1.5. Acquisition managers must consider IP requirements throughout the acquisition process (Air Force Instruction [AFI] 63-102, *Communications—Computer Systems Security Research Development, Test, and Evaluation*). Operating commands must work in conjunction with implementing, participating, and supporting command IP personnel.

1.6. Single managers establish IP measures and guidance within their acquisition programs.

2. Responsibilities:

2.1. Secretary of the Air Force (SAF)/AQ. Is responsible for making sure IP is considered in information systems acquisition, research and development, and contracts.

2.2. Headquarters, United States Air Force (HQ USAF)/SC.

2.2.1. Directs the Air Force IP Program.

2.2.2. Implements required national and Department of Defense (DoD) IP doctrine and policy, and develops and promulgates Air Force IP policy and procedures.

2.2.3. Represents the Air Force on DoD and national IP committees and working groups.

2.2.4. Provides oversight and guidance to Electronic Systems Center (ESC), Information Warfare Product Group (Air Force Material Command [AFMC]); the Standard Systems Group (AFMC), the San Antonio Air Logistics Center, Cryptologic Programs Product Group (AFMC); the Air Intelligence Agency (AIA), the Air Force Information Warfare Center (AFIWC), and the Headquarters, Air Force Communications Agency (HQ AFCA)--all designated agents for specific IP responsibilities.

2.2.5. Reviews information systems plans, directives, requirements' documents, and other related documents to make sure IP requirements are considered in program development.

2.2.6. Prepares and defends IP requirements funded through the Air Force budget process.

2.3. HQ USAF/XO. Responsible for IP with respect to single integrated operational plan (i.e., extremely sensitive information material, and command, control, communications and computer countermeasures).

2.4. HQ USAF/CE. Provides IP facility design and construction criteria. Construction criteria for facilities where sensitive compartmented information (SCI) is used and/or stored are provided in DCID 1/21, *Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF).*

2.5. HQ USAF/IN. Responsible for protection of SCI and for the accreditation of information systems processing SCI information (Air Force 14 series (Intelligence) publications contains guidance).

2.6. HQ USAF/SP. Develops and implements Air Force policy for the protection of information classified under Executive Order 12958, *Classified National Security Information.*

2.7. HQ AFOSI. Provides hostile and criminal threat assessment, technical surveillance countermeasures, and information on the exploitation of information systems. Serves as Air Force focal point for computer crime investigations.

2.8. HQ AFCA.

2.8.1. Supports HQ USAF/SC on IP matters.

2.8.2. Provides guidance and support to major commands (MAJCOM), field operating agencies (FOA), direct reporting units (DRU), and wing IP offices.

2.8.3. Reviews, evaluates, and interprets national and DoD IP policy and doctrine and makes recommendations on implementation to HQ USAF/SCTW.

2.8.4. Develops, coordinates and maintains Air Force IP instructions, manuals, and pamphlets.

2.8.5. Develops, coordinates, publishes, and maintains HQ USAF approved specialized IP publications.

2.8.6. Produces an "Annual Assessment of the State of Air Force Information Protection," and provides metric, assessment, and trend analysis information to HQ USAF/SCTW according to **Attachment 2**, and AFI 33-212, *Reporting COMSEC Incidents*.

2.8.7. Supports the ESC Information Warfare Product Group.

2.8.8. Develops information systems IP architectures.

2.8.9. Serves as the lead command for the Air Force Electronic Key Management System.

2.9. HQ AFMC.

2.9.1. Serves as the single manager for the acquisition, research, development, prototyping, assessment, production, and sustainment of IP systems and products**.**

2.9.2. Serves as the Air Force focal point for communication security (COMSEC) key and COMSEC equipment requirements, and the central office of record for all Air Force COMSEC material.

2.9.3. Serves as the Air Force focal point for IP technology insertion.

2.9.4. Identifies, develops, and prototypes operational countermeasures for vulnerabilities.

2.9.5. Provides Air Force-wide network visibility, and network and IP software technical support/ solutions.

2.10. HQ AIA

2.10.1. Manages the Computer Security Assistance Program to support MAJCOM IP Assessment and Assistance Program, and IP operations..

2.10.2. Provides technical support to the Air Force Office of Special Investigations (AFOSI) for computer crime investigations.

2.10.3. Obtains and distributes information systems threat and vulnerability information.

2.10.4. Supports the ESC Information Warfare Product Group.

2.10.5. Supports HQ AFCA in the development of information systems IP architectures.

2.10.6. Manages the Emission Security testing laboratory.

2.10.7. Manages the Air Force Telecommunications Monitoring and Assessment Program according to AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP).*

2.11. MAJCOMs and Wings. Manage centralized and integrated IP offices and programs. Specific responsibilities are in the IP instructions addressed in paragraph **4.** ***Note: The host wing is responsible when there is more than one wing assigned to a base. These responsibilities apply to FOAs and DRUs that elect to manage their own IP programs. Otherwise, FOAs and DRUs fall under the purview of the wing IP office.***

2.12. Users of Information Systems. Make sure information systems meet the security requirements outlined in the Air Force IP instructions addressed below.

3. Reporting Information. Metric reporting is assigned Report Control Symbol (RCS) HAF-SC(A) 9604, **Annual Assessment of Air Force Information Protection**.

3.1. Metrics reporting is designated emergency status code C2. Continue reporting during emergency conditions, normal precedence. Submit data requirements as prescribed, or as soon as possible after submission of priority reports.

3.2. Continue reporting during MINIMIZE.

4. This policy interfaces with Air Force Systems Security Instructions (AFSSI) 4100, *Communications Security Program (will convert to AFI 33-201)*; 5100, *The Air Force Computer Security (COMPUSEC) Program*, 5101, *Computer Security in the Air Force Acquisition Systems*, and 5102, *Computer Security (COMPUSEC) for Operational Systems*, (will convert to AFI 33-202); 7000, *The Air Force TEMPEST Program*, (will convert to AFI 33-203), and AFI 33-204, *The C4 Systems Security Awareness, Training, and Education (SATE) Program*. These publications provide direction, specific procedures and guidance relating to the Air Force IP program. (See **Attachment 1** for the Glossary of References, Abbreviations, Acronyms, and Terms.)

JOHN S. FAIRFIELD, Lt Gen, USAF
DCS Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

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

AFI 33-212, *Reporting COMSEC Incidents*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFI 63-102, *Communications—Computer Systems Security Research Development, Test, and Evaluation*

AFSSI 4100, *Communications Security Program (will convert to AFI 33-201)*

AFSSI 5100, *The Air Force Computer Security (COMPUSEC) Program* (will convert to AFI 33-202)

AFSSI 5101, *Computer Security in the Air Force Acquisition Systems* (will convert to AFI 33-202)

AFSSI 5102, *Computer Security (COMPUSEC) for Operational Systems*, (will convert to AFI 33-202)

AFSSI 7000, *The Air Force TEMPEST Program*, (will convert to AFI 33-203)

DCID 1/21, *Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)*

Executive Order 12958, *Classified National Security Information*

Abbreviations and Acronyms

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMC—Air Force Materiel Command

AFOSI—Air Force Office of Special Investigations

AFSSI—Air Force Systems Security Instruction

AIA—Air Intelligence Agency

COMSEC—Communications Security

COMPUSEC—Computer Security

DoD—Department of Defense

DRU—Direct Reporting Unit

ESC—Electronic Systems Center

FOA—Field Operating Agency

HQ USAF—Headquarters, United States Air Force

IP—Information Protection

MAJCOM—Major Command

SAF—Secretary of the Air Force

SATE—Security Awareness, Training, and Education

SCI—Sensitive Compartmented Information

SCIF—Sensitive Compartmented Information Facilities

TMAP—Telecommunications Monitoring and Assessment Program

Terms

Accreditation—The formal declaration by a designated approving authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards.

Certification—Comprehensive evaluation of the technical and non-technical security features and countermeasures of an information system and other safeguards, made in support of the accreditation process, to establish the extent a particular design and implementation meets a set of specified security requirements.

Communications Security (COMSEC)—Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications.

Computer Intrusion—An event of unauthorized entry, or attempted entry, to a computer system.

Computer Security (COMPUSEC)—Measures and controls that ensure confidentiality, integrity, or availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

COMSEC Incident—Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information.

Designated Approving Authority—Official with the authority to formally assume responsibility for operating an information system or network at an acceptable level of risk.

Emission Security—Protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment, information systems, and telecommunications systems.

Information Protection (IP)—Measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems. **NOTE:** IP includes communications security, computer security, and emission security. IP is an element of information warfare.

Information Systems—Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception, of voice and/or data, and includes software, firmware, and hardware. **NOTE:** This includes automated information systems.

Malicious Logic—Hardware, software, or firmware intentionally included in an information system for an unauthorized purpose. **NOTE:** Trojan horse is a form of malicious logic.

Network Security—Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects.

Trojan Horse—Computer program containing an apparent or actual useful function that contains

additional (hidden) functions that allows unauthorized collection, falsification or destruction of data.

Single Manager—A system program director, product group manager, or material group manager that is responsible for the acquisition and life cycle support of AFMC-supported products.

Attachment 2

ASSESSING THE AIR FORCE INFORMATION PROTECTION PROGRAM

A2.1. Assessing the IP Program. Assess the IP program by reporting measurements in seven areas: (1) information systems accreditation, (2) information systems intrusions (controlled), (3) information systems intrusions (uncontrolled), (4) malicious logic incidents, (5) COMSEC incidents, (6) COMSEC Audit/Functional Review results, and (7) SATE training. Additionally, summarize the results in an "Annual Assessment of the State of Air Force Information Protection."

A2.2. Information Systems Accreditation. Assess the policy to accredit all information systems for operational use by comparing the number of systems accredited (**Figure A2.1.**):

A2.2.1. At the classified level to the total number of systems operating at the classified level.

A2.2.2. At the unclassified (including sensitive but unclassified) level to the total number of systems operating at the unclassified level.

A2.3. Information Systems Intrusions (Controlled). Controlled intrusions are penetrations by computer security personnel to evaluate systems security. Assess the policy to detect, report, and prevent unauthorized access to information systems and the information they contain, transmit, or process by counting (**Figure A2.2.**):

A2.3.1. The number of attempted controlled intrusions.

A2.3.2. The number of successful controlled intrusions.

A2.3.3. The number of reported successful controlled intrusions.

A2.4. Information Systems Intrusions (Uncontrolled). Uncontrolled intrusions are penetrations by noncomputer security personnel--hackers. Assess the policy to detect, report, and prevent unauthorized access to information systems and the information they contain, transmit, or process by counting (**Figure A2.3.**):

A2.4.1. The number of reported actual intrusions.

A2.4.2. The number of successful actual intrusions.

A2.5. Malicious Logic Incidents. Assess the policy to detect, report, and prevent the introduction of malicious logic into information systems by counting (**Figure A2.4.**):

A2.5.1. Malicious logic incident reports.

A2.5.2. Systems affected.

A2.6. COMSEC Incidents. Assess the policy to prevent unauthorized access to COMSEC material by counting the number of incidents (**Figure A2.5.**):

A2.6.1. Actual compromises.

A2.6.2. Possible compromises.

A2.6.3. Incidents that did not result in compromises.

A2.7. COMSEC Audit/Functional Review Results. Assess adherence to IP policy throughout the Air Force by counting (**Figure A2.6.**):

A2.7.1. Satisfactory functional reviews.

A2.7.2. Unsatisfactory functional reviews.

A2.8. SATE Training. Assess the policy to train users of information systems by comparing the number of users (**Figure A2.7.**):

A2.8.1. Receiving initial information systems security training to the total number of users requiring initial IP awareness training.

A2.8.2. Receiving annual refresher training to the total number of users requiring annual refresher training.

Figure A2.1. Sample Metric of Information Systems Accreditation.

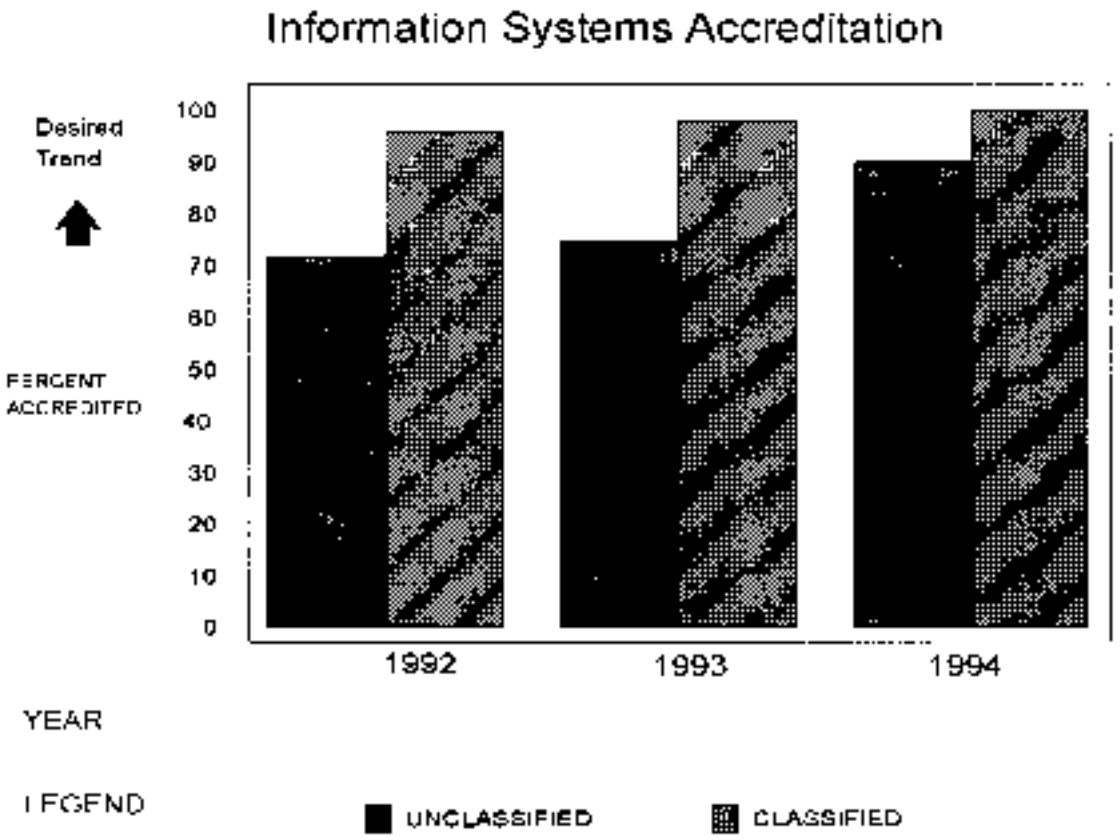
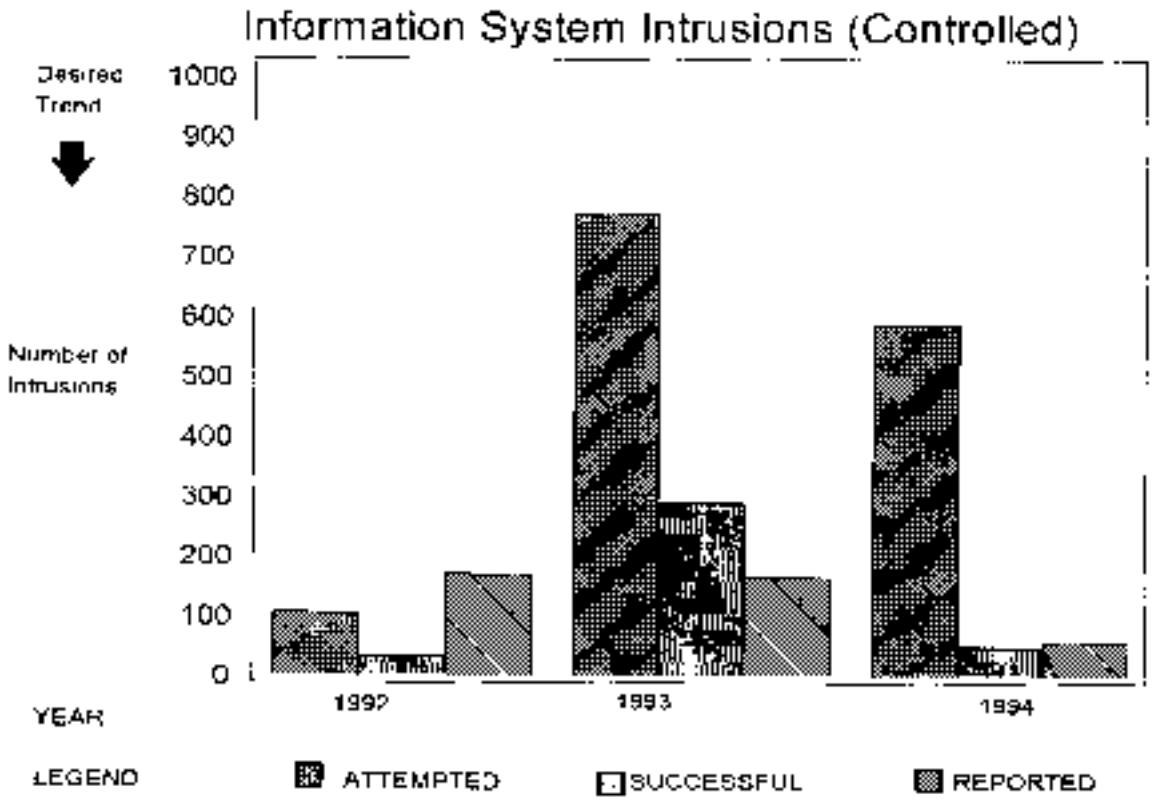
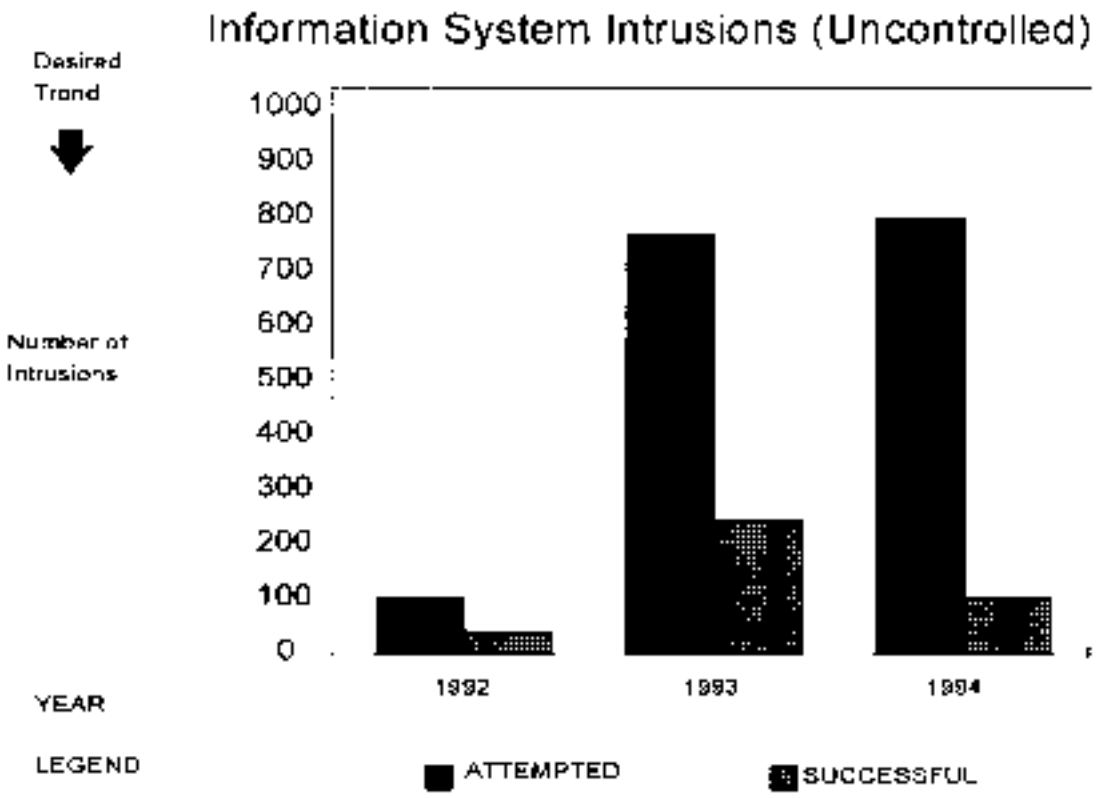


Figure A2.2. Sample Metric of Information System Intrusions (Controlled).



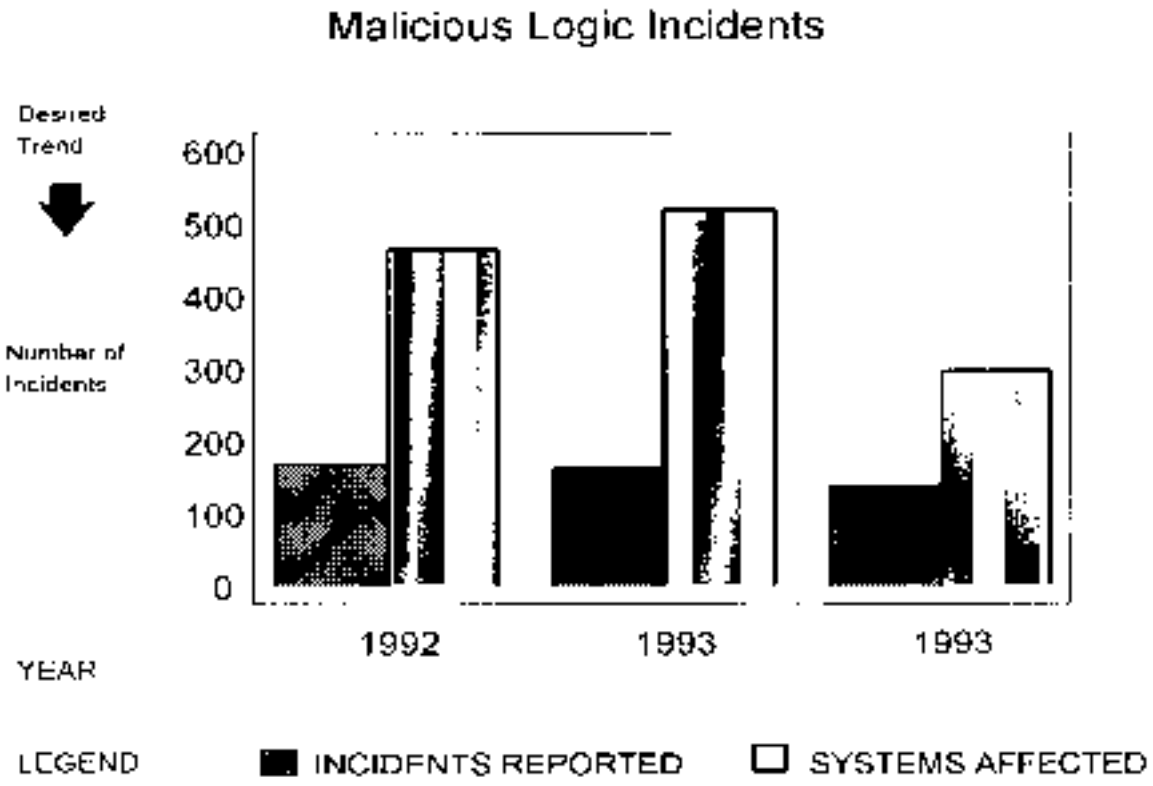
- Reported controlled intrusions should equal attempted controlled intrusions.
- Successful controlled intrusions should decline.

Figure A2.3. Sample Metric of Information System Intrusions (Uncontrolled).



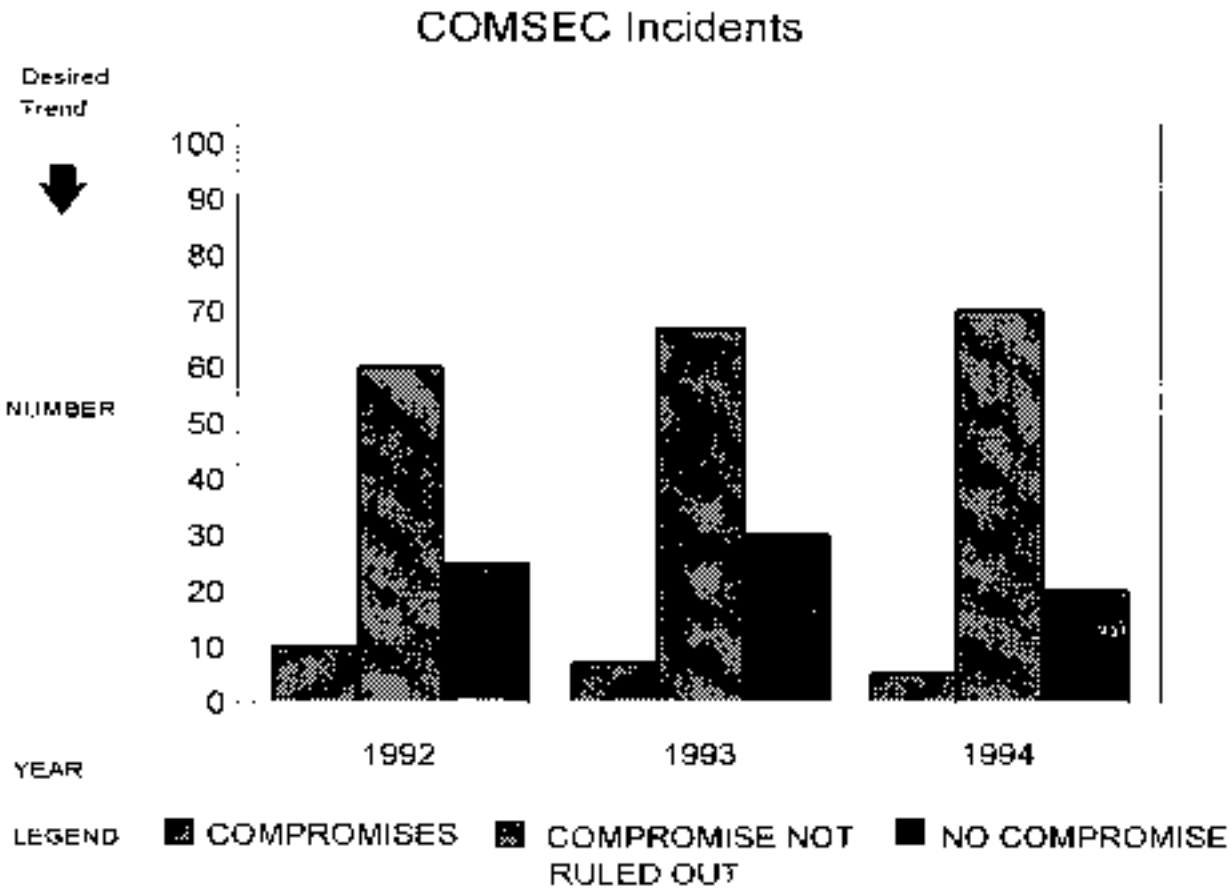
- Successful uncontrolled intrusions should decline.

Figure A2.4. Sample Metric of Malicious Logic Incidents.



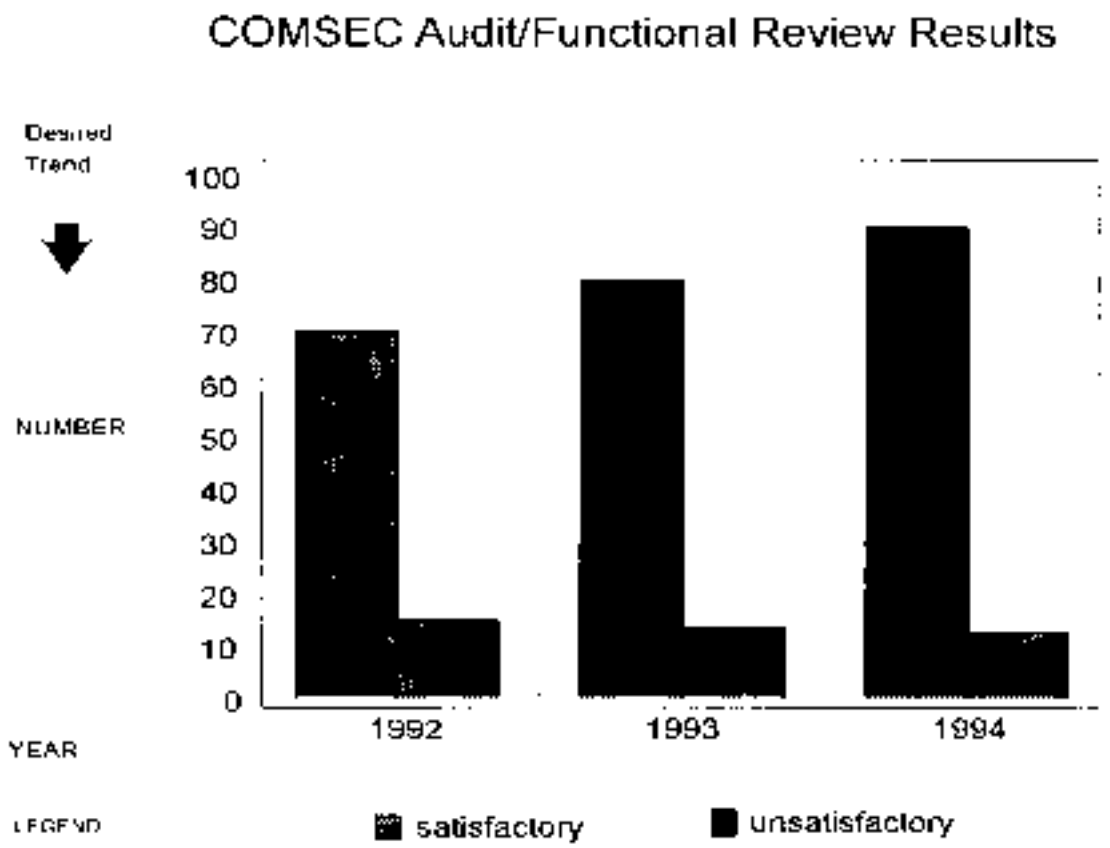
- Number of attacks and the number of systems affected should decline.

Figure A2.5. Sample Metric of COMSEC Incidents.



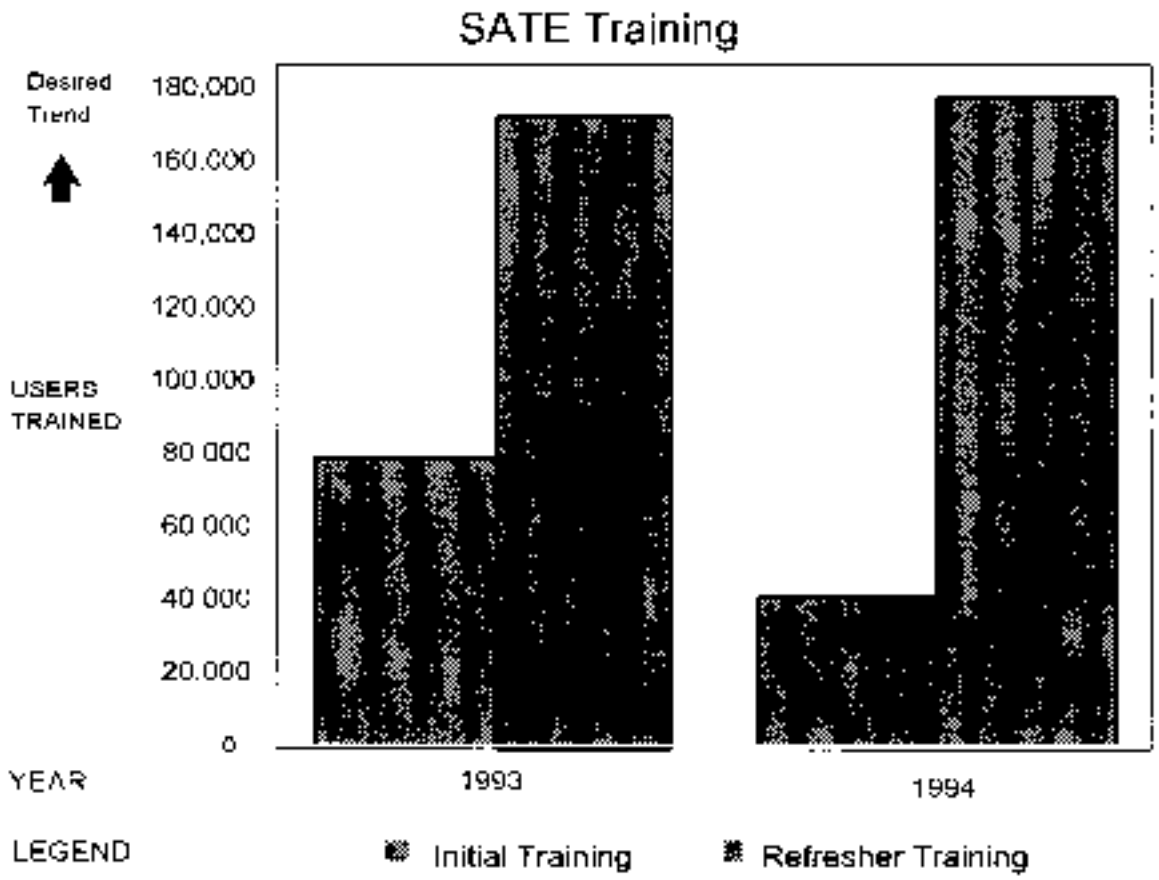
- Number of compromises should decline.
- Number of possible compromises should decline.
- Number of no compromises should stabilize.

Figure A2.6. Sample Metric of COMSEC Audit/Functional Review Results.



- Number of satisfactory reviews should increase.
- Number of unsatisfactory reviews should decrease.

Figure A2.7. Sample Metric of SATE Training.



- Number of people trained to increase.
- Across the board the other metrics should achieve their desired results.