BY ORDER OF THE SECRETARY OF THE
AIR FORCE

AIR FORCE INSTRUCTION 63-102

22 MARCH 1994

Acquisition

COMMUNICATIONS--COMPUTER SYSTEMS
SECURITY RESEARCH,DEVELOPMENT,
TEST, AND EVALUATION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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).

This instruction implements AFPD 33-2, C^4 *Systems Security*. It establishes procedures and assigns responsibility for managing Communications-Computer System Security research, development, test, and evaluation (RDT&E). It applies to Air Force activities responsible for identifying Communications-Computer Systems Security needs and conducting Communications-Computer Systems Security RDT&E. This instruction applies to all forms of Air Force Communication-Computer Systems processing information at all levels of classification. This instruction directs Air Force Command, Control, Communications, and Computer (C^4) systems security RDT&E efforts to ensure that they support National and Department of Defense (DoD) policies. It does not apply to the Air National Guard or United States Air Force Reserve.

SUMMARY OF REVISIONS

This is the first publication of AFI 63-102. It aligns with AFPD 33-2.

1. Responsibilities:

1.1. Air Force activities shall identify C^4 systems security RDT&E requirements in appropriate research and development (R&D) technical requirements documents and process them through the Air Force focal point.

1.2. The Air Force, as directed by HQ USAF/SC, shall participate in the National Security Agency (NSA) and other DoD component C^4 systems security RDT&E programs.

1.3. Air Force C^4 systems security requirements will include program protection planning and systems security engineering.

1.4. SAF/AQ, office of the Secretariat of the Air Force for Acquisitions will:

- Provide direction to Air Force C^4 systems security RDT&E efforts through issuance of a Program Management Directive (PMD).

- Provide representation on the C^4 systems security RDT&E Requirements Review Panel (RRP).

1.5. HQ USAF/SCX, Directorate of Plans, Policy and Resources, will:

- Establish the Air Force C^4 Systems Security Program.

- Assess and coordinate national C^4 systems security RDT&E goals, plans, and programs.

1.6. Offices of collateral responsibility:

1.6.1. HQ USAF/SCM will:

- Provide oversight and guidance to the Air Intelligence Agency (AIA) on RDT&E matters.

- Establish and chair the C^4 systems security RRP. The RRP shall prioritize and allocate funds for validated RDT&E projects.

1.6.2. HQ AIA. Is responsible to HQ USAF/SCM for RDT&E management oversight. On behalf of the AIA, the Air Force Information Warfare Center (AFIWC):

- Pursues an Air Force C^4 systems security RDT&E program to reduce the risk of technological exploitation of Air Force C^4 systems by hostile intelligence services or other hostile entities.

- Is the Air Force focal point for all C^4 systems security RDT&E programs managed by NSA and other DoD components.

- Reviews and evaluates all Air Force C^4 systems security RDT&E requirements.

- Programs and advocates funds for the C^4 systems security RDT&E program.

- Provides representation to the C^4 systems security RDT&E RRP.

- Assists major commands (MAJCOM) in the evaluation, identification, and documentation of MAJCOM C^4 Systems security needs/required capabilities which may require security RDT&E efforts.

1.6.3. HQ AFMC will:

- Conduct C^4 systems security RDT&E.

- Execute C^4 systems security RDT&E funds.

- Provide representation to the C^4 systems security RDT&E RRP.

- With AIA (AFIWC) and the Air Force C^4 Agency (AFC^{4}A), assess the NSA and other DoD components C^4 systems security RDT&E programs.

- Advise Air Force C^4 systems security users of availability of security technologies applicable to their operational needs.

1.6.4. HQ AFC^{4}A will:

- Provide representation to the C^4 systems security RDT&E RRP.

1.6.5. MAJCOMs will submit all C^4 systems security RDT&E requirements through AFIWC for review and evaluation.

2. Commonly Used C^4 Systems Security Terms:

2.1. Command, Control, Communications, and Computer (C^4) Systems. Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of C^2, through all phases of the operational continuum.

2.2. Communications Security (COMSEC). The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.

2.3. Computer Security (COMPUSEC). Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

2.4. Emanation Security (TEMPEST). Short name referring to investigation, study, and the control of compromising emanations from telecommunications and automated information systems equipment.

3. Measures of Compliance. The degree of compliance with this instruction shall be measured by comparing the number of C^4 security R&D requirements identified to AFIWC through MAJCOM submissions against those identified through other sources.

RICHARD E. HAWLEY, Lt General, USAF
Principal Deputy, Assistant Secretary of the
Air Force for Acquisition