Army Regulation 380–53

Security

Information Systems Security Monitoring

Headquarters
Department of the Army
Washington, DC
29 April 1998

UNCLASSIFIED

SUMMARY of CHANGE

AR 380–53
Information Systems Security Monitoring

This revision--

- Eliminates all reference to hearability surveys.

- Broadens the focus of the regulation to include all types of telecommunications (para 1-1).

- Allows all MACOMs to conduct Information Systems Security Monitoring operations (para 1-4i).

- Changes the certification of notification procedures requirement from annually to biennially (para 2-4).

- Expands forms of Information Systems Security Monitoring notification (para 2-5).

- Changes the reporting requirements for information obtained incidental to Information Systems Security Monitoring (para 2-8).

- Clarifies restrictions applied to the monitoring of contractor telecommunications (para 2-10e).

- Applies restrictions to Information Systems Security Monitoring of privileged communications (para 2-10i).

- Specifies who can conduct Information Systems Security Monitoring (para 2-10j).

- Stipulates minimal training required to participate in Information Systems Security Monitoring operations (para 3-3).

- Authorizes use of a hacker methodology, when penetrating computers and computer networks, to demonstrate the simplicity in which systems can be accessed (para 3-4h).

Headquarters
Department of the Army
Washington, DC
29 April 1998

*Army Regulation 380–53

Effective 29 May 1998

Security

Information Systems Security Monitoring

Robert M. Walker
Acting Secretary of the Army

History. This publication revises the previously published regulation, bringing it in line with current laws and national and Department of Defense (DOD) Information Systems Security Monitoring policy. Because the regulation has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation prescribes U.S. Army policy for the conduct of Information Systems Security Monitoring. This regulation implements National Telecommunications and Information Systems Security Directive No. 600 and Department of Defense Directive 4640.6.

Applicability. This regulation applies to the Active Army, the Army National Guard of the U.S., and the U.S. Army Reserve. During mobilization or national emergency, chapters and policies contained in this regulation may be modified by the proponent.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Intelligence. The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The proponent may delegate this approval authority, in writing, to a division chief in the proponent agency in the grade of colonel or the civilian equivalent.

Army management control process. This regulation contains management control provisions but does not identify key management controls that must be evaluated.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior written approval from the Deputy Chief of Staff for Intelligence (DAMI–CHI), 1000 Army Pentagon, Washington, DC 20310–1000.

Suggested Improvements. Users of this regulation are invited to send comments and suggestions for improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Deputy Chief of Staff for Intelligence (DAMI–CHI), 1000 Army Pentagon, Washington, DC 20310–1000.

Distribution. Distribution of this publication is made in accordance with the requirements of Initial Distribution Number (IDN) 092178 intended for command levels B, C, D, and E for the Active Army, the Army National Guard of the U.S., and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1
Introduction, *page 1*
Purpose • 1–1, *page 1*
References • 1–2, *page 1*
Explanation of abbreviations and terms • 1–3, *page 1*
Responsibilities • 1–4, *page 1*

Chapter 2
Objectives and Requirements of Information Systems Security Monitoring, *page 2*
Introduction • 2–1, *page 2*
Objectives • 2–2, *page 2*
Prerequisites to Information Systems Security Monitoring • 2–3, *page 2*
Certification of notification procedures • 2–4, *page 3*
Forms of notification • 2–5, *page 3*
Conduct of Information Systems Security Monitoring • 2–6, *page 4*
Acquisition of signals during maintenance and testing • 2–7, *page 4*
Use of Information Systems Security Monitoring products • 2–8, *page 4*
Foreign language communications • 2–9, *page 5*
Prohibitions on Information Systems Security Monitoring • 2–10, *page 5*

Chapter 3
Training, Standards, and Operations Applicable to Information Systems Security Monitoring, *page 6*
Introduction • 3–1, *page 6*
Request and authorization to conduct Information Systems Security Monitoring • 3–2, *page 6*
Training and standards for Information Systems Security Monitoring • 3–3, *page 6*
Information Systems Security Monitoring operations • 3–4, *page 6*
Information Systems Security Monitoring working materials • 3–5, *page 7*
Information Systems Security Monitoring reports • 3–6, *page 8*
Safeguarding Information Systems Security Monitoring equipment • 3–7, *page 8*

Chapter 4
Oversight and Reporting, *page 8*
Oversight • 4–1, *page 8*
Reporting violations • 4–2, *page 8*

Appendixes

A. References, *page 10*

*This regulation supersedes AR 380–53, 15 November 1984.

Contents—Continued

B. Computer Defense Assistance Program (CDAP), *page 10*

Glossary

Index

Chapter 1
Introduction

1–1. Purpose

a. This regulation sets forth responsibilities, policy, and procedures for conducting Information Systems Security Monitoring within the U.S. Army. It also provides guidance for U.S. Army elements conducting Information Systems Security Monitoring in support of joint and combined operations and activities.

b. The principles of this regulation apply to all forms of Information Systems Security Monitoring conducted by U.S. Army elements. This regulation does not pertain to—

(1) The interception of wire and oral communications for law enforcement purposes as described in AR 190–53.

(2) Operations center communications monitoring as described in AR 190–30.

(3) Electronic surveillance as described in AR 381–10.

(4) Technical surveillance countermeasures and TEMPEST as described in AR 381–14.

(5) Signals intelligence collection activities as described in AR 381–3.

(6) Monitoring of radio communications by Net Control Stations (NCS), to enforce net discipline.

(7) System and Network Administrators performing C2 Protect functions (outlined in app G, AR 380–19), in order to keep their own automated information systems infrastructure operational and secure. This exemption is limited to performing vulnerability analysis of the operating systems of the Automated Information Systems (AISs) directly under the control of the system and/or network administrators.

(8) The use of Intrusion Detection Systems (IDS) on AIS when the IDS is only used to monitor communications protocols, systems control information, and specific command, control, or words associated with commonly accepted or known penetration techniques. This exemption does not authorize users of such tools to conduct penetration testing or access the content of any communication.

(9) Research, Development, Acquisition, and Evaluation (RDAT&E) testing of U.S. Army telecommunications when such activities are performed in a lab environment, using test-generated users or data.

1–2. References

Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms

The following terms are defined here because they form the basis for understanding the provisions of this regulation. Abbreviations and other special terms used in this regulation are explained in the Glossary.

a. Telecommunications. The preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electro-mechanical, or electro-optical means.

b. Telecommunications security. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) or using classified or sensitive Government or Government-derived information, the loss of which could adversely affect the national security interest. It also includes the application of physical security measures to Communications Security (COMSEC) information or materials.

c. Information Systems Security Monitoring. The act of listening to, reading, copying, or recording one's own official telecommunications to provide material for analysis, so that the degree of security being provided to those telecommunications or automated information systems may be determined.

d. Telecommunications systems. The interconnected devices used to transmit, receive, or process telecommunications. Telecommunications systems include but are not limited to telephones (conventional wire line, field, and cellular), radiotelephones, facsimile machines (internal and external), computers (both stand-alone and networked), automated information systems using telecommunications circuits for a transmission medium, video teleconference systems, paging devices, and tactical radio systems (voice, radioteletype, data, and so forth).

e. Content. When used with respect to any wire, oral, or electronic communication, includes any information concerning the identity of the parties to such communication or the substance, purport, or meaning of that communication.

f. Penetration testing. Security testing in which evaluators attempt to circumvent the security features of an AIS based on their understanding of the system design and implementation. The purpose of penetration testing is to confirm and demonstrate, through exploitation, the degree of vulnerability of an AIS.

g. Penetration verification. Provides positive verification that a system- or machine-level compromise has been obtained through penetration testing (for example, usually in the form of a message or new user account).

h. Vulnerability analysis. Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

1–4. Responsibilities

a. The Office of the General Counsel. The Office of the General Counsel (OGC)—

(1) Reviews U.S. Army Information Systems Security Monitoring policy for compliance with public laws and national and Department of Defense (DOD) policies and regulations.

(2) Reviews and certifies in writing, biennially, that the Information Systems Security Monitoring notification procedures in effect throughout the U.S. Army are adequate.

(3) In the event that Information Systems Security Monitoring results must be used in a criminal prosecution, reviews the results and approves their use in court.

(4) Reviews all requests for proposed Information Systems Security Monitoring exercises that are not based upon a major Army command (MACOM) request for approval granted by the Deputy Chief of Staff for Intelligence (DCSINT) of the Army.

b. The Judge Advocate General. The Judge Advocate General (TJAG)—

(1) Provides direct legal support to the Army and coordinates issues with the Office of the General Counsel to ensure compliance with public laws and national and DOD policies and regulations.

(2) Reviews all requests to conduct Information Systems Security Monitoring exercises that are based upon a MACOM request prior to DCSINT of the Army approval.

c. The Inspector General. The Inspector General (TIG) is responsible for oversight of the U.S. Army Information Systems Security Monitoring Program to ensure regulatory compliance.

d. The Deputy Chief of Staff for Intelligence. As the Secretary of the Army's single designee for Information Systems Security Monitoring, the DCSINT—

(1) Prepares, publishes, and maintains U.S. Army Information Systems Security Monitoring policy.

(2) Grants waivers and exceptions to U.S. Army Information Systems Security Monitoring policy after obtaining legal review from the OGC and TJAG.

(3) Reviews and approves the techniques and procedures for conducting Information Systems Security Monitoring.

(4) Reviews and approves MACOM requests to perform Information Systems Security Monitoring.

(5) Certifies the adequacy of U.S. Army Information Systems Security Monitoring notification procedures to other DOD agencies when U.S. Army monitoring elements operate jointly with such

agencies in support of DOD, joint, combined, or multi-national operations.

(6) Represents and defends U.S. Army interests pertaining to Information Systems Security Monitoring policy at National, DOD, and Service meetings and working groups.

(7) Notifies MACOM commanders before authorizing Information Systems Security Monitoring that is not based upon a MACOM request.

e. Commanding General, U.S. Army Intelligence and Security Command. Commanding General, U.S. Army Intelligence and Security Command (CG, INSCOM)—

(1) Provides the U.S. Army's portion of support to the Joint COMSEC Monitoring Activity (JCMA) according to the most current JCMA Memorandum of Agreement.

(2) Develops and disseminates U.S. Army techniques for conducting Information Systems Security Monitoring.

(3) In coordination with the Information Operation TRIAD, and through Director of the Land Information Warfare Activity (LIWA), develops and disseminates for the U.S. Army, techniques and procedures for conducting AIS security penetration and verification testing as it pertains to applicable phases of the Computer Defense Assistance Program (CDAP). See appendix B.

f. Commanding General, U.S. Army Training and Doctrine Command. Commanding General, U.S. Army Training and Doctrine Command (CG, TRADOC)—

(1) Develops, produces, and maintains an exportable standardized Information Systems Security Monitoring training package to address requirements identified in paragraph 3–3*a* of this regulation.

(2) Coordinates with CG, INSCOM, to incorporate results of paragraphs 1–4*e*(2) and (3) into the standardized training package.

g. The Director of Information Systems for Command, Control, Communications, and Computers. The Director of Information Systems for Command, Control, Communications, and Computers (DISC4), as the Chief Information Officer (CIO) of the Army,—

(1) Promulgates rules and procedures in AR 380–19, outlining system and network administrators' responsibilities (vulnerability analysis) to keep U.S. Army AIS operational and secure.

(2) Implements procedural and material protective measures, develops plans and policies, and validates requirements to protect U.S. Army command, control, communications, and computers (C4).

(3) Acts as the U.S. Army focal point for C2 Protect.

(4) Maintains overall responsibility and oversight for policy and management of the U.S. Army Computer Emergency Response Team (ACERT) Program.

h. Deputy Chief of Staff for Operations. Deputy Chief of Staff for Operations (DCSOPS)—

(1) Acts as the Army Staff (ARSTAF) operational focal point for information operations (IO).

(2) Exercises operational tasking authority over the LIWA, to include prioritization and validation of requests for LIWA support.

i. Commanders of MACOMs. Commanders of MACOMs will—

(1) Ensure the notification procedures for Information Systems Security Monitoring (see para 2–5) are implemented and adhered to.

(2) Request authority to conduct Information Systems Security Monitoring according to paragraph 2–4.

(3) Ensure personnel authorized to conduct Information Systems Security Monitoring comply with the provisions of this regulation.

(4) Ensure the products of Information Systems Security Monitoring are used for their intended purpose (see para 2–2).

j. Commanders at all levels. Commanders at all levels will—

(1) Plan for and obtain Information Systems Security Monitoring to support command security programs and objectives.

(2) Ensure Information Systems Security Monitoring results are used only for security purposes (see para 2–2).

(3) Ensure a comprehensive and continuing Information Systems Security Monitoring notification program is in effect (see paras 2–4 and 2–5).

(4) Ensure essential elements of friendly information (EEFI) and essential program information, technology, and systems (EPITS) are made available to Information Systems Security Monitoring teams.

(5) Provide the necessary facilities and support, including security of Information Systems Security Monitoring equipment and working materials, required by the monitoring element for the conduct of the mission.

(6) Ensure no adverse action is taken against any employee (military, civilian, or contractor) for reporting activities described in paragraphs 2–8 and 4–2.

Chapter 2
Objectives and Requirements of Information Systems

2–1. Introduction

a. Department of Defense telecommunications systems are provided for official Government communications. When these systems are used by Department of the Army components, they are subject to Information Systems Security Monitoring in accordance with this regulation.

b. Information Systems Security Monitoring will be done in a manner that satisfies the legitimate needs of the U.S. Army. It will be conducted so as to minimize the monitoring of telecommunications not related to security objectives. It will be performed in a manner that also protects, to the greatest degree possible, the privacy and civil liberties of individuals whose telecommunications are subject to monitoring.

c. Information Systems Security Monitoring is a security assessment technique that provides information not available through other sources that is essential for evaluating security within the U.S. Army.

2–2. Objectives

Information Systems Security Monitoring is undertaken to—

a. Collect operational signals needed to measure the degree of security being achieved by U.S. codes, cryptographic equipment and devices, COMSEC techniques, and related materials.

b. Provide a basis from which to assess the types and value of information subject to loss through intercept and exploitation of Government telecommunications.

c. Provide an empirical basis for improving the security of U.S. Army telecommunications against Signals Intelligence (SIGINT) exploitation.

d. Assist in determining the effectiveness of electronic attack and electronic protect, cover, and deception actions and operations security (OPSEC) measures.

e. Identify U.S. Army telecommunications signals that exhibit unique external signal parameters, signal structures, modulation schemes, radio fingerprints, and so forth that could provide SIGINT elements of foreign powers the capability to identify specific targets for subsequent geopositioning and exploitation purposes.

f. Provide empirical data to train users of U.S. Army telecommunications systems in proper (COMSEC) techniques and measures.

g. Evaluate the effectiveness of U.S. Army COMSEC education and training programs.

h. Support Defensive Information Operations by identifying, verifying, and evaluating the susceptibilities of U.S. Army telecommunications and AIS from attempts to exploit, degrade, or neutralize such systems.

2–3. Prerequisites to Information Systems Security Monitoring

The following must occur before any Information Systems Security Monitoring can take place:

a. Notification. Users of official DOD telecommunications will be given notice that—

(1) Passing classified information over nonsecure DOD telecommunications systems, other than protected distribution systems or

automated information systems accredited for classified processing, is prohibited.

(2) Official DOD telecommunications systems are subject to Information Systems Security Monitoring at all times.

(3) Use of official DOD telecommunications systems constitutes consent by the user to Information Systems Security Monitoring at any time.

b. Certification. The Office of the General Counsel has certified the adequacy of the notification procedures in effect, and the OGC and TJAG have given favorable legal review of any proposed Information Systems Security Monitoring that is not based on a MACOM request.

c. Authorization. The Deputy Chief of Staff for Intelligence has authorized Information Systems Security Monitoring to be conducted within the MACOM involved.

2–4. Certification of notification procedures

The MACOM commanders will implement procedures to ensure all personnel, including contractors, are aware of the provisions of this regulation. Commanders must verify that their notification procedures are adequate. At Headquarters, Department of the Army (HQDA), the Director of Security Services will act as the MACOM head to ensure Secretariat/ARSTAF and ARSTAF field operating agency (FOA) compliance.

a. The MACOM commanders will submit requests for certification to the Deputy Chief of Staff for Intelligence (DAMI–CHI), 1000 Army Pentagon, Washington, DC 20310–1000. Requests will arrive not later than 15 July of each odd-numbered year. Approval periods will run from 1 October (of each odd-numbered year) through 30 September (of the next odd-numbered year) to correspond with the fiscal year. Requests will include a detailed description of the notification procedures within the MACOM including—

(1) The exact wording of the warning notice on telephone directories.

(2) The exact wording of the banner notice on AIS.

(3) The exact wording of the notice published quarterly in command bulletins, on command E-mail (unclassified and classified), and similar publications and systems.

(4) A statement that the Department of Defense (DD) Form 2056 (Telephone Monitoring Notification Decal) has been applied to all telephones and facsimile machines.

(5) A statement that command in-processing includes a briefing that informs personnel that use of official telecommunications systems constitutes consent to Information Systems Security Monitoring.

(6) The identification of any other notification procedures used (see para 2–5).

b. The Division of Counterintelligence and Human Intelligence, HQDA (DAMI–CHI), will review all requests to verify that the required information is present. The requests will be consolidated and forwarded to the OGC for legal certification.

c. Upon certification by the OGC, the DCSINT of the Army, as the Secretary of the Army’s single designee for Information Systems Security Monitoring, will approve MACOM submissions. This certification will be valid for a period of 24 months, unless otherwise indicated.

2–5. Forms of notification

Information Systems Security Monitoring notifications must ensure that all users of official DOD telecommunications systems understand that their use of DOD telecommunications systems constitutes consent to Information Systems Security Monitoring.

a. Mandatory forms of notification.

(1) *Telephone or communications directory notice.* Official U.S. Army telephone or communications directories will display the following notice on the front cover or prominently within the general information section:

ATTENTION!

DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON NONSECURE TELECOMMUNICATIONS SYSTEMS. OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS—INCLUDING TELEPHONES, FACSIMILE MACHINES, COMPUTER NETWORKS, AND MODEMS—ARE SUBJECT TO MONITORING FOR TELECOMMUNICATIONS SECURITY PURPOSES AT ALL TIMES. USE OF OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS CONSTITUTES CONSENT TO INFORMATION SYSTEMS SECURITY MONITORING.

(2) *DD Form 2056.*

(a) The DD Form 2056 will be applied to the front of all telephones (except tactical telephones) within the U.S. Army.

(b) The DD Form 2056 will also be applied to the front of all Secure Telephone Units (STUs); however the banner at the top of the form containing the words DO NOT DISCUSS CLASSIFIED INFORMATION will be removed or obliterated.

(c) The DD Form 2056 will be applied to the front of all data facsimile devices except those that are an internal part of another device (for example, a facsimile card in a personal computer). The DD Form 2056 will also be applied to the front of all secure data facsimile devices, but the words DO NOT DISCUSS CLASSIFIED INFORMATION will be removed.

(3) *Computer log-on banner notice.* All computers attached or accessible through Government-owned or -leased telecommunications networks must display the banner below. The banner will be placed on the computer in such a way that the user must press a key to get beyond it, thereby demonstrating his or her acceptance of its provisions.

(a) The warning banner is not required on computers that are an integral portion of a tactical weapons system, electronic personnel access control system, or intrusion detection system and stand-alone computers not connected to a telecommunications network.

(b) Security warning banners for publicly accessible, nonrestricted U.S. Army World Wide Web sites will be in accordance with the current provisions of HQDA, DISC4, Web-site management policy.

ATTENTION!

THIS IS A DOD COMPUTER SYSTEM. BEFORE PROCESSING CLASSIFIED INFORMATION, CHECK THE SECURITY ACCREDITATION LEVEL OF THIS SYSTEM. DO NOT PROCESS, STORE, OR TRANSMIT INFORMATION CLASSIFIED ABOVE THE ACCREDITATION LEVEL OF THIS SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (INCLUDES INTERNET ACCESS) ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES, BUT IS NOT LIMITED TO, ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING. UNAUTHORIZED USE OF THIS DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR ALL LAWFUL PURPOSES.

(4) *Periodic notices.* Periodic notices will be published at least quarterly in command bulletins (use words of the banner in paragraph (1) above), over command unclassified and classified E-mail (use words of the banner in para (3) above), and in similar publications and systems.

(5) *Initial briefing.* Initial briefings to all new personnel will include informing personnel that their use of telecommunications systems constitutes consent to Information Systems Security Monitoring.

b. Optional forms of notification. Optional forms of notification include the following:

(1) Periodic briefings and training classes for all assigned personnel.

(2) Special memorandums from the commander or responsible senior staff officer to all personnel.

(3) Local notification and consent procedures.

(4) Statements in standing operating procedures (SOPs), signal operation instructions (SOIs), and similar publications or documents.

(5) The following statement may be placed on facsimile cover sheets:

ATTENTION!

DO NOT PROCESS, STORE, OR TRANSMIT CLASSIFIED INFORMATION ON UNSECURED TELECOMMUNICATIONS SYSTEMS. OFFICIAL DOD TELECOMMUNICATIONS SYSTEMS, INCLUDING FACSIMILE MACHINES, ARE SUBJECT TO MONITORING FOR INFORMATION SYSTEMS SECURITY MONITORING AT ALL TIMES. USE OF THIS SYSTEM CONSTITUTES CONSENT TO INFORMATION SYSTEMS SECURITY MONITORING.

c. Waiver of mandatory forms of notification. Requests for waivers to the mandatory forms of notification will be forwarded to HQDA (DAMI–CHI) for action.

2–6. Conduct of Information Systems Security Monitoring

a. Information Systems Security Monitoring may be conducted only on certified MACOMs that have notification procedures in place approved by the OGC, and when authorized by the Deputy Chief of Staff for Intelligence (in accordance with para 2–4*c*).

b. Information Systems Security Monitoring will be conducted only in support of security objectives (see para 2–2). Information Systems Security Monitoring will not be performed to support law enforcement or criminal or counterintelligence investigations.

c. Information Systems Security Monitoring will be conducted in—

(1) The least obtrusive manner possible.

(2) A way that minimizes the monitoring of communications not relevant to security objectives (para 2–2).

(3) A manner that ensures maximum privacy consistent with monitoring objectives.

d. Information Systems Security Monitoring conducted by U.S. Army monitoring elements in support of joint or combined operations and activities will be conducted in accordance with joint or combined Information Systems Security Monitoring procedures, as long as those procedures have been reviewed and approved by the appropriate legal counsel.

2–7. Acquisition of signals during maintenance and testing

Maintenance and calibration of Information Systems Security Monitoring equipment may require the acquisition of signals by maintenance personnel.

a. The following signals may be used without restriction:

(1) Laboratory-generated signals.

(2) Communications signals with the consent of all parties involved.

(3) Commercial and public service broadcasts.

(4) Noncommunications signals such as beacons, telemetry, and radar.

b. Requests to use signals other than those in paragraph *a* above will be forwarded to HQDA (DAMI–CHI) for action.

2–8. Use of Information Systems Security Monitoring products

Information Systems Security Monitoring products will be used only in pursuit of security objectives, except that—

a. Information obtained through Information Systems Security Monitoring may be used in connection with disciplinary or administrative action against Department of the Army personnel for knowing, willful, or negligent actions that result in the unauthorized disclosure of classified information (see AR 380–5, paras 14–101 and 14–102). In this case, the Information Systems Security Monitoring element is authorized to release names, or recorded media, of the telecommunications involved to the supported commander or designated representative for use as evidence. Procedures will be strictly adhered to as follows:

(1) The supported commander, after having consulted with the servicing judge advocate (JA), will provide the Information Systems Security Monitoring element with a written request, specifically identifying the telecommunications messages or communications required. The request will identify the servicing JA consulted.

(2) The Information Systems Security Monitoring element will obtain a signed receipt from the supported commander or designated representative for the requested materials. The receipt will include a statement that the commander or representative is familiar with and will comply with the security requirements and privacy restrictions applicable to the material.

(3) The Information Systems Security Monitoring element will immediately notify its chain of command that the material has been requested and provided.

(4) The Information Systems Security Monitoring unit commander will notify HQDA (DAMI–CHI), in writing, within 5 working days of providing the material to the supported command.

b. Information may be obtained incidental to an authorized Information Systems Security Monitoring mission that relates directly to a serious crime such as sabotage or threats or plans to commit offenses that threaten a life or could cause significant damage to or loss of Government property (this includes data on Government AIS). This information will be reported immediately by the senior member of the Information Systems Security Monitoring team present when the information is discovered, as follows:

(1) Crimes or incidents identified in AR 381–12, at chapter 3, or AR 381–20, paragraph 4–2, will be reported under the provisions of AR 381–12.

(2) Questionable activity and information relating to violations of Federal law as addressed in procedure 15 of AR 381–10 will be reported under the provisions of AR 381–10.

(3) When evaluating or assessing the security of U.S. Army AIS, Information Systems Security Monitors may detect computer anomalies that could potentially be unauthorized intrusions into Army AIS. When Information Systems Security Monitors detect such anomalies, they must contact the system administrator and ACERT immediately. The system administrator will then follow the procedures of AR 380–19 by taking measures to ascertain that the anomaly is in fact an unauthorized intrusion, notifying counterintelligence (CI) and criminal investigation division (CID) so that the offices may conduct an investigation of the incident. Information Systems Security Monitors should not support this process and must discontinue monitoring the suspected intrusion as soon as the system administrator or ACERT has interceded, and in no case may the Information System Security Monitors continue monitoring the anomaly for more than 24 hours. Data pertaining to the anomaly or suspected intrusion recorded during the 24-hour period will not be accessed until the appropriate legal authorization is obtained to further investigate the activity. Information Systems Security Monitoring of the AIS may resume once the conditions of paragraphs *c*(1)(*a*) and (*b*) below are met.

(4) Crimes not covered above will be reported to the commander of the unit requesting the monitoring support under the provisions of this chapter.

c. Whenever any information is officially reported to the commander under paragraphs *a* and *b* above, procedures will be adhered to as follows:

(1) Stop all Information Systems Security Monitoring of the circuit, frequency, or network (except as authorized by para *b*(3) above) over which the information was obtained. Monitoring of the circuit, frequency, or network will not resume until—

(a) All actions by the commander or law enforcement agency related to the incident have been completed, or

(b) The party involved in the incident no longer has access to the circuit, frequency, or network.

(2) Once the incident is discovered and reported, under no circumstance will the Information Systems Security Monitoring element attempt to investigate the occurrence.

(3) The Information Systems Security Monitoring element team leader will immediately identify, mark as working papers, classify a minimum of "Confidential," segregate, hold in suspense, and protect all recording media pertaining to the incident. If these materials are required for evidence, the following procedures will be used:

(a) The investigating commander or law enforcement agency will request the recorded media in writing, after having consulted with the local servicing JA.

(b) The Information Systems Security Monitoring element leader will obtain a signed receipt from the supported commander or designated representative for the requested materials. The receipt will include a statement that the commander or representative is familiar with and will comply with the security requirements and privacy restrictions applicable to the materials, and the provisions of paragraph (4) below will be complied with.

(c) The requesting agency will be informed that the recorded media will be returned to the monitoring element for final disposition when the materials are no longer required as evidence.

(d) The Information Systems Security Monitoring element team leader will immediately notify his or her chain of command that materials have been requested and provided.

(4) The commander of the Information Systems Security Monitoring element releasing the recorded media containing suspected criminal activity will notify HQDA (DAMI–CHI), in writing, of the circumstances within 24 hours of release of the material. Headquarters, Department of the Army (DAMI–CHI), will subsequently notify the OGC. Notification will include—

(a) Nature of the suspected offense.

(b) Identification of the material released.

(c) Date, time, and location where information was obtained.

(d) Anticipated action resulting from disclosure of the information.

(e) Location, name, and telephone number of the responsible individual where the materials are being held.

(f) Names or other data sufficient to identify any individuals who participated in the monitored communication will not be included in the report.

(5) The results of Information Systems Security Monitoring may not be used in a criminal prosecution without prior consultation with the OGC and TJAG.

2–9. Foreign language communications

a. Translation of foreign language conversations, messages, or data files that are recorded on Government-owned or -leased telecommunications systems under the authority of this regulation is authorized.

b. Such communications may be translated by—

(1) A U.S. person with an appropriate U. S. security clearance.

(2) A foreign national employee of the U.S. Armed Forces with a Limited Access Authorization (LAA) for this purpose.

(3) A foreign national with an appropriate host nation security clearance who is assigned to U.S. Armed Forces or who is a member of a combined command where U.S. Armed Forces are participants.

c. Translation must be done under the direct supervision of Information Systems Security Monitoring personnel. Recordings and other working materials, including translations, will not be released outside the monitoring element, except as provided in paragraph 2–8 of this regulation. Transcripts will be treated as Information Systems Security Monitoring working materials.

2–10. Prohibitions on Information Systems Security Monitoring

a. Information Systems Security Monitoring will not be conducted in support of law enforcement or criminal or counterintelligence investigative purposes.

b. Information Systems Security Monitoring within the National Capital Region is prohibited without approval from the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) or a designee. Requests for such monitoring will be forwarded through command channels to HQDA (DAMI–CHI) for action. Requests must arrive at HQDA a minimum of 45 days prior to the date the monitoring is to commence.

c. Information Systems Security Monitoring, or the products of such monitoring, will not be used to enforce DOD policy limiting the use of official DOD telecommunications systems to the conduct of official business.

d. Information Systems Security Monitoring of official Government telecommunications systems outside DOD is prohibited without written approval from the ASD(C3I). Requests for such monitoring will be forwarded through command channels to HQDA (DAMI–CHI) for action. Requests must arrive at HQDA a minimum of 45 days prior to the date the monitoring is to commence.

e. U.S. Government contractors monitoring prohibitions follow.

(1) Monitoring telecommunications systems of U.S. Government contractors at their own facilities is prohibited without the express written approval of the chief executive officer (CEO) of the company or his or her designee. Requests for such monitoring will include a statement from the CEO outlining the procedures that have been implemented within the contractor's organization to afford notice to the contractor's employees. Such requests will be forwarded through command channels to HQDA (DAMI–CHI) for action. Headquarters, Department of the Army (DAMI–CHI), will obtain a written opinion from the Office of the General Counsel prior to taking any action. Requests must arrive at HQDA a minimum of 45 days prior to the date the monitoring is desired.

(2) Monitoring DOD-owned or -leased telecommunications that are provided by DOD for the exclusive use by U.S. Government contractors is prohibited without the express written approval of the CEO of the company or his or her designee. Requests for such monitoring will include a statement from the CEO outlining the procedures that have been implemented within the contractor's organization to afford notice to the contractor's employees. Requests involving DOD-owned or -leased telecommunications used by U.S. Government contractors will be reviewed by the local servicing JA.

f. The results of Information Systems Security Monitoring shall not be used to produce foreign intelligence or counterintelligence, as defined in Executive Order 12333.

g. Information Systems Security Monitoring shall not be conducted by U.S. Army personnel (military, civilian, or contractor) on the telecommunications of another DOD component without the express written approval of the head (or his or her written designee) of that department or agency. Any U.S. Army requests to conduct Information Systems Security Monitoring of another DOD component will be forwarded to HQDA (DAMI–CHI) for action. Within the U.S. Army, one MACOM will not monitor the telecommunications or conduct AIS penetration testing, of another MACOM without the consent of that Army MACOM. The exception to this restriction is when the activity is directed by the DCSINT of the Army.

h. Credentialed counterintelligence and law enforcement personnel are prohibited from performing or participating in Information Systems Security Monitoring collection/analysis operations. Counterintelligence personnel filling Technical Surveillance Countermeasures (TSCM) billets are exempted from this provision.

i. Special attention will be provided to ensure Information Systems Security Monitoring operations avoid telecommunications containing privileged doctor-patient, lawyer-client, and chaplain-petitioner communications.

j. All U.S. Army Information Systems Security Monitoring operations may be conducted only by the following personnel (military, civilian, or contractor):

(1) U.S. Army Military Intelligence personnel:

(a) Enlisted with MOS of 96B, 98C, 98G, 98H, 98J, and 98K.

(b) Warrant officers with a MOS code of 350 or 352.

(c) Commissioned officers with a 35-series MOS.

(2) Civilian intelligence specialists (GS–0132) and security specialists (GS–0080) assigned to Command Security Offices.

(3) Personnel assigned to LIWA's ACERT and the subordinate computer emergency response team (CERT) infrastructure (does not include system or network administrators).

k. All personnel conducting U.S. Army Information Systems Security Monitoring operations will acquire and maintain a clearance based on a Single Scope Background Investigation (SSBI).

l. Exceptions to the provisions of this paragraph may be granted on a case-by-case basis by HQDA (DAMI–CHI).

Chapter 3
Training, Standards, and Operations Applicable to

3–1. Introduction

The procedures in this chapter apply to all Information Systems Security Monitoring of official DOD telecommunications systems within the U.S. Army. Information Systems Security Monitoring will be conducted only when all of the following conditions exist:

a. The monitoring supports program objectives defined in paragraph 2–2 of this regulation.

b. Notification and consent procedures exist (paras 2–3 through 2–5).

c. The monitoring will be an efficient use of resources.

3–2. Request and authorization to conduct Information Systems Security Monitoring

Commanders are authorized to conduct Information Systems Security Monitoring operations under the provisions of this regulation. Monitoring may be performed at the commander's discretion throughout the 2-year approval cycle, provided that the OGC has certified adequacy of the command's notification procedures and that the DCSINT of the Army grants the command the authority to conduct the monitoring.

3–3. Training and standards for Information Systems Security Monitoring

Information Systems Security Monitoring and related activities will be conducted in strict compliance with this regulation.

a. Knowledge of regulations, laws, and other guidance. Each individual involved in the conduct (collection and analysis) of Information Systems Security Monitoring will receive formal training before participating in monitoring or penetration operations. As a minimum, personnel will be trained on—

(1) The provisions of this regulation, with particular emphasis on chapters 2 and 3.

(2) The provisions of AR 381–10, procedures 1 through 5, 14, and 15.

(3) The provisions of AR 381–12, paragraph 3–1.

(4) The provisions of AR 190–53.

(5) The provisions of applicable Federal-level guidance and laws (for example, title 18 of the U.S. Code (USC), sections 2510, 2511, 2512, and so forth).

b. Knowledge of conducting monitoring operations. Formal training requirements to conduct monitoring operations may be fulfilled through—

(1) Completion of a DOD COMSEC monitoring course.

(2) Completion of an internal command training program using approved TRADOC course materials (see paras 1–4*e*(2) and 1–4*f*(1)). The execution of command training programs will be approved by HQDA (DAMI–CHI).

(3) Completion of formal U.S. Army Intelligence Center training leading to award of primary MOS O5G or 97G.

c. Certification and training by ACERT. In addition to the training requirements identified in paragraphs *a*(1) through (5) above of this regulation, each individual involved in performing penetration or verification testing of U.S. Army AIS will be certified in accordance with the ACERT certification and training program.

d. Training certifications.

(1) For monitoring operations, the first lieutenant colonel (05) or civilian equivalent (GS–14) in the individual's chain of command will certify in writing the individual has been trained in accordance with the provisions of paragraph 3–3*a*. A copy of this certification will be maintained on file at the monitoring unit, available for inspection by any inspector general (IG), oversight officer, or command inspector. Copies of these certifications will be provided to DAMI–CHI upon request.

(2) For AIS penetration/verification testing, the Chief, ACERT, will certify in writing the individual has been trained in accordance with the provisions of paragraphs *a* and *c* above. A copy of this certification will be maintained on file at the ACERT Coordination Center (ACERT/CC), available for inspection by any IG, oversight officer, or command inspector. Copies of these certifications will be provided to HQDA (DAMI–CHI) upon request.

e. Nontrained personnel. When required, trained Information Systems Security Monitoring mission supervisors may augment the Information Systems Security Monitoring team's efforts with nontrained technical resources, provided—

(1) The mission supervisor briefs all nontrained personnel on the restrictions applied to Information Systems Security Monitoring operations.

(2) All nontrained personnel work directly under a trained Information Systems Security Monitoring supervisor.

(3) The use of the nontrained personnel is approved on a case-by-case basis by the MACOM commander.

f. Refresher training. Personnel participating in Information Systems Security Monitoring (includes operators, analysts, and supervisors) will annually receive unit level refresher training.

g. Violation reporting. Any individual discovering a violation of this regulation will promptly report the violation (see para 4–2).

h. Access for oversight. All personnel will cooperate fully with the U.S. Army and DOD General Counsels, intelligence oversight officers, and IGs and will allow them access to all information necessary to perform their oversight responsibilities.

i. Use of signals in training. Training in using Information Systems Security Monitoring equipment will use signals that are subject to Information Systems Security Monitoring whenever possible. When those signals are not available, training in the use of Information Systems Security Monitoring equipment may be conducted using those signals identified in paragraph 2–7*a*. When those signals identified in paragraph 2–7*a* are used to conduct Information Systems Security Monitoring training, the following restrictions apply:

(1) The signal acquisition will be limited in extent and duration necessary to train personnel in the use of the equipment.

(2) No particular U.S. person's communications will be targeted without the specific, written consent of that person.

(3) The content of the telecommunications will be—

(a) Retained only when actually needed for training purposes.

(b) Disseminated only to persons conducting or participating in the training, except as provided for in paragraph 2–8.

(c) Destroyed immediately upon completion of the training.

j. Waivers. Waivers to the provisions of this paragraph will be granted on an individual basis by HQDA (DAMI–CHI).

3–4. Information Systems Security Monitoring operations

Information Systems Security Monitoring operations include monitoring and recording telecommunications and penetration testing of Army AIS, as well as the analysis of the material obtained during the conduct of such activities.

a. Information Systems Security Monitoring will be limited to official DOD telecommunications systems (see para 1–3*d*) that are owned or leased by the Government for use by DOD personnel or the military departments.

b. Information Systems Security Monitoring will be conducted in a manner that minimizes, to the greatest extent possible, the monitoring and recording of telecommunications not relevant to the purpose of the monitoring.

c. Communications conducted over DOD telecommunications systems are assumed to be official communications subject to monitoring. However, recorded telecommunications will not be retained or disseminated if they have no relation to Information Systems Security Monitoring objectives (para 2–2), unless they relate to a crime (as specified in para 2–8*b*).

d. Information Systems Security Monitoring of wire line telephone systems will be conducted by bridging telephone lines before the point of connection between the DOD lines and the outside lines, as done at the main distribution frame. DOD telecommunications may not be monitored when combined, multiplexed, or otherwise mixed with non-DOD telecommunications in such a way that monitoring of the non-DOD telecommunications is likely.

e. Information Systems Security Monitoring of radio transmissions (other than those associated with cellular telephone systems), such as single channel voice radio, microwave, or similar means, will be limited to circuits dedicated only to DOD use and to transmissions that are sent and received by transmitting and receiving facilities dedicated to DOD use. No incidentally acquired non-DOD communication shall be further monitored when it is determined that it is a non-DOD communication. A record of the inadvertently acquired information may be kept for signal identification and avoidance purposes; the record may describe the signal parameters (frequency, modulation, type, and timing) but shall not identify the parties of the communication.

f. Information Systems Security Monitoring of cellular telephone systems will employ signal collection equipment that incorporates special design features (software) that allow for the targeting of specific command cellular telephone numbers. The equipment will be programmed by the user to activate only on calls made to and from command owned or leased cellular telephones.

g. Information Systems Security Monitoring of AIS (for example, E-mail and data transfer) will employ collection technologies (for example, Automated Security Incident Measurement devices with Network Security Monitoring software) designed to intercept network subscribers incoming and outgoing messages or data. Information Systems Security Monitoring will only be conducted on a network that originates or terminates on a DOD-owned or -leased telecommunication. Information Systems Security Monitoring of networks will not be performed with the intent to identify, track, or locate unauthorized users.

h. When penetrating computers and computer networks, the simulation of so-called "hacker methodology" may be used to demonstrate the simplicity with which unauthorized persons can obtain information, such as modem telephone numbers, accessible ports, and so forth, and the ease with which unprotected or underprotected computer systems and networks can be accessed. Procedures for conducting AIS penetration testing will be developed and disseminated by the LIWA, in accordance with paragraph 1–4*e*(3) of this regulation. This may include but is not limited to—

(1) Use of a wardialer or similar device to obtain computer dial-in telephone numbers within the specific area code and prefixes used by the command being monitored. Information Systems Security Monitoring will be performed only on those telephone numbers positively identified as belonging to the command being monitored. No other telephone numbers will be retained for any purpose.

(2) Placing a network security monitor on the command's network to perform searches of data traversing the system. Key word searches may be used as an analysis and time management tool. Selected key words may include standard terms associated with the identification of classified information (for example, confidential, secret, top secret, special intelligence, and so forth) and those words directly relating to the supported command's EEFI or EPITS.

(3) Evaluating the system's security by attempting to bypass system log-on procedures to gain access to the computer. If access is gained, a program may be placed on the system to verify the presence of the penetration effort. Penetration teams will obtain the unit commander's written guidance outlining authorized actions that may be taken by the penetration team.

(4) The use of a "key stroke capture program" to monitor networked computers.

i. Only official communications pertinent to the Information Systems Security Monitoring mission will be analyzed. These telecommunications will form the basis of the monitoring reports.

j. Telecommunications selected for analysis will not be routinely transcribed, except as provided for in paragraph 2–9. When transcripts are made, they will not be included in interim or final Information Systems Security Monitoring reports. Transcripts of communications (except those discussed in para 2–9) will be prepared and distributed as follows:

(1) If the supported commander's review of interim or final reports indicates that a knowing, willful, or negligent disclosure of classified information may have occurred, the commander, or designee, may request and be provided with transcripts of the telecommunications. Initial transcripts will not include the names of participants in the conversations or other information that would identify the participants, except in an official capacity (for example, "the radio operator on watch").

(2) If review of these transcripts indicates that a knowing, willful, or negligent violation of security directives may have occurred that warrants disciplinary or administrative action, the commander, or designee, may request in writing and receive from the Information Systems Security Monitoring element, the names of individuals involved. The commander or designee will consult with the servicing judge advocate to ensure that disciplinary or administrative action against the individuals involved is appropriate before requesting their names.

(3) The data (for example, recordings, disks, or printouts) may be provided as specified in paragraph 2–8.

(4) If the action taken includes a request by the commander for a counterintelligence investigation or supports criminal or law enforcement objectives, any subsequent monitoring of the communication will constitute electronic surveillance and must be conducted according to applicable polices and procedures. Information Systems Security Monitoring of the circuit(s) will cease immediately. No further attempt will be made by the Information Systems Security Monitoring activity to obtain or provide additional information.

k. Telecommunication data not related to the monitoring mission that are present on recordings will not be transcribed or otherwise annotated unless needed to support actions described in paragraph 2–8.

3–5. Information Systems Security Monitoring working materials

a. Routine access to Information Systems Security Monitoring working materials such as operator logs, operator or analyst notes, and recordings will be limited to those personnel specifically approved under paragraph 3–3. Working materials will not be released except as provided in paragraph 2–8. Working materials will be stored and maintained in a manner to ensure that the access restrictions are maintained.

b. Access to Information Systems Security Monitoring working materials may be granted to commanders and other personnel exercising direct management authority over the Information Systems Security Monitoring element if—

(1) Such access is for the purpose of supervising, directing, and checking the efficiency, regulatory compliance, and mission effectiveness of Information Systems Security Monitoring personnel.

(2) Such access takes place at the Information Systems Security Monitoring element.

(3) All personnel concerned are advised of the limitations on the release of information derived from Information Systems Security Monitoring (see para 2–8).

c. When Information Systems Security Monitoring is conducted as part of a broader vulnerability assessment, OPSEC survey, and so forth, results obtained from the monitoring may be shared with other elements of the team to ensure that a fully integrated, comprehensive assessment or survey is made. All personnel will be familiar with the provisions of paragraphs 3–3*a*(1) through (4).

d. All written Information Systems Security Monitoring working materials produced in the course of monitoring and analysis operations will be reviewed within 60 working days of the date they were produced to ensure that any information not pertinent to the monitoring mission is deleted. These written materials will be annotated with the name of the person conducting the review and the date the review was conducted.

e. Information Systems Security Monitoring working materials will be controlled as working papers under the provisions of AR 380–5, paragraph 7–304.

(1) If Information Systems Security Monitoring personnel are unable to determine the classification of the intercepted data, a minimum tentative classification of CONFIDENTIAL will be assigned. The material in question will then be coordinated with the supported command and the appropriate classification determined.

(2) Recording media (for example, computer disks) will be marked with the highest classification of material recorded and will retain this classification until degaussed, reused, or destroyed.

f. Information Systems Security Monitoring working materials will be destroyed or degaussed 30 calendar days after the final report is issued. Recording over previously recorded tapes or reformatting computer disks will satisfy this requirement, but the tapes and disks will remain classified until they are erased or degaussed by an NSA-approved degausser. To maintain the working materials, an extension of up to 30 days may be granted in writing by the MACOM commander having operational control over the Information Systems Security Monitoring element. Any extension beyond that must be submitted to HQDA (DAMI–CHI) for their submission for approval by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)).

g. Requests for access to Information Systems Security Monitoring working materials will be processed under provisions of AR 25–55 and AR 340–21 when the requester is the subject of the working materials.

h. When conducting support in accordance with paragraph 3–4*h* of this regulation, records of all penetration testing (type, time, and duration) against U.S. Army AIS will be maintained as required for statistical purposes.

i. Working materials will be reviewed to ensure they are devoid of data extraneous to Information Systems Security Monitoring objectives before the materials are released outside of the Information Systems Security Monitoring element.

3–6. Information Systems Security Monitoring reports

The composition, format, and frequency of submission of Information Systems Security Monitoring reports will be determined by the needs of the supported command. The final report should be submitted within 30 days of the completion of the monitoring mission, unless directed otherwise by the supported command.

a. Information Systems Security Monitoring reports will contain information only on the monitoring mission and the adequacy of security procedures within the command monitored.

(1) Paragraph one of all written reports will prominently state INFORMATION SYSTEMS SECURITY MONITORING INFORMATION. TO BE USED FOR OFFICIAL PURPOSES ONLY (AR 380–53/DODD 4640.6/NTISSD 600).

(2) Descriptions or gists of information disclosed that are necessary to understand the nature of any weakness may be included in the Information Systems Security Monitoring report.

(3) Reports submitted under paragraph 4–2 are not considered Information Systems Security Monitoring reports in the context of this paragraph.

(4) When Information Systems Security Monitoring is conducted as part of a vulnerability assessment effort, operations security survey, or other security support, a separate report of the results of the monitoring need not be prepared. Any report containing products of Information Systems Security Monitoring must be marked and prepared according to this regulation.

b. Reports and information acquired through Information Systems Security Monitoring will not be disseminated outside the U.S. Army, except—

(1) In support of mutual OPSEC objectives and the goals of the other military services, joint commands, and DOD agencies. This includes the exchange of information and reports (including working materials) within Information Systems Security Monitoring technical channels.

(2) When required by a court order and approved by the DOD General Counsel.

(3) For counterintelligence, law enforcement, or criminal purposes (see para 2–8).

c. Distribution of final reports will be determined through coordination with the supported command.

d. Reports will be reviewed to ensure they are devoid of data extraneous to Information Systems Security Monitoring objectives, before the materials are released outside of the Information Systems Security Monitoring element.

3–7. Safeguarding Information Systems Security Monitoring equipment

Equipment designed specifically for Information Systems Security Monitoring will be safeguarded to prevent unauthorized use. Required safeguards follow:

a. Equipment installed in facilities or installations for Information Systems Security Monitoring operations may be safeguarded by any of the following methods:

(1) Lock and key.

(2) Internal log-on/log-out security software.

(3) Removal of a component that renders the equipment inoperative.

b. Records will be maintained by each monitoring element that possesses equipment designed specifically for Information Systems Security Monitoring. These records will include—

(1) An inventory of the equipment on hand.

(2) Location of each item in use.

(3) Names of persons in charge of each item of equipment in use.

c. Only personnel assigned to Information Systems Security Monitoring duties will have access to Information Systems Security Monitoring equipment in use.

Chapter 4
Oversight and Reporting

4–1. Oversight

All Information Systems Security Monitoring activities, materials, records, and equipment are subject to IG, intelligence, and security oversight inspections at any time.

4–2. Reporting violations

Individuals discovering a violation of the activities described in paragraphs 2–8, 2–10, 3–3, and 3–4 of this regulation will promptly report the violation to the unit commander or any IG or intelligence oversight officer.

a. The commander, IG, or intelligence oversight officer will ensure that a competent inquiry or investigation into the reported violation is conducted. These persons will ensure that the circumstances of the violation are reported within 3 working days, through command channels to HQDA (DAMI–CHI), with information copies to HQDA (Office of the General Counsel and the Office of The Inspector General). Reports will contain the following:

(1) Nature of the violation (for example, unauthorized monitoring).

(2) Dates and times of the incident.

(3) Location (name of installation or activity) where the incident occurred.

(4) Individuals (last name, first name, middle initial) involved in the incident.

(5) Brief summary of the incident.

(6) Corrective actions taken.

(7) Current status of the inquiry.

b. HQDA (DAMI–CHI), the General Counsel, The Judge Advocate General, and The Inspector General will work together to ensure that appropriate action is taken to correct the violation and to prevent future occurrences of the same violation.

c. Within 5 working days of discovery of the incident, the General Counsel in coordination with the Inspector General will send a copy of the initial report and the proposed corrective actions to ASD(C3I).

Appendix A
References

Section I
Required Publications

AR 25–55
The Department of the Army Freedom of Information Act Program (Cited in para 3–5*g*.)

AR 340–21
The Army Privacy Program (Cited in para 3–5*g*.)

AR 380–5
Department of the Army Information Security Program (Cited in para 3–5*e*.)

AR 380–19
Information Systems Security (Cited in paras 1–1*b*(7) and 1–4*g*(1).)

AR 381–10
U.S. Army Intelligence Activities (Cited in paras 2–8*b*(2) and 3–3*a*(2).)

AR 381–12
Subversion and Espionage Directed Against the U.S. Army (SAEDA) (Cited in paras 2–8*b*(1) and 3–3*a*(3).)

AR 381–20
The U.S. Army Counterintelligence Program (Cited in para 2–8*b*(1).)

AR 381–143
Logistic Policies and Procedures (U) (Cited in para 3–7*b*.)

Section II
Related Publications

A related publication is a source of additional information. The user does not have to acquire or read a related publication to understand this regulation.

AR 25–1
The Army Information Resources Management Program

AR 190–53
Interception of Wire and Oral Communications for Law Enforcement Purposes

AR 381–14
(S) Technical Surveillance Countermeasures (TSCM) (U)

DODD 4640.6
Communications Security Telephone Monitoring and Recording

NTISSD 600
Communications Security (COMSEC) Monitoring

Section III
Prescribed Forms

DD Form 2056
Telephone Monitoring Notification Decal

Section IV
Referenced Forms

This section contains no entries.

Appendix B
Computer Defense Assistance Program (CDAP)

1.0. Introduction

1.1. Background. The Department of the Army (DA) Command and Control Protect (C2 Protect) Program Management Plan (PMP) identified as a deficiency the absence of an organic Army capability to monitor, detect, prevent, and respond to Army automated information systems (AIS) incidents. This deficiency may adversely affect ongoing Army operations and readiness. More specifically, Information Operations (IO) may be degraded. The threats to IO have three primary objectives: the compromise of information, the corruption of data, and the disruption of operations. To protect against the threat, the Army has established the Army Computer Emergency Response Team (ACERT). The ACERT provides the Army with the capability to prevent, monitor, detect, and respond to AIS security incidents. The ACERT leverages and integrates intelligence support and network/system management capabilities to a unified C2 Protect effort. As part of its mission, the ACERT has initiated the Computer Defense Assistance Program (CDAP) to provide requesting individual units and activities with identification, verification, and assessment of AIS vulnerabilities. In addition, the program offers technical support to mitigate these vulnerabilities.

2.0. CDAP goal/objective

The goal of CDAP is to prevent unauthorized access to Army computer systems by identifying points of unauthorized access, assessing depth and degree of potential compromise, and recommending methods, techniques, and configuration modifications needed to secure the system.

3.0. Scope

The CDAP will be executed to protect and defend all unclassified and classified AIS used to plan, direct, coordinate, control, and support Army forces across the full spectrum of conflict for Active, Reserve, and National Guard components.

4.0. Authorization

CDAP is authorized within the ACERT mission as identified in the C2 Protect Implementation Plan (Task 11, C2 Protect Central React Capability) and Joint Warfighter Capability Assessment (JWCA) process. The DA DCSOPS, DA DCSINT, and DISC4 established the ACERT at the Land Information Warfare Activity (LIWA) on 10 October 1995. CDAP identification and verification of AIS vulnerabilities are conducted in accordance with AR 380–19 and AR 380–53 and are authorized by the service provider, consent and communications security (COMSEC) exceptions to ECPA (Title 18 USC 2511 (2)(a)(i), 2511 (2)(c) and section 107 (b)(1) of Public Law 99–508, as well as the Computer Security Act of 1987 (Public Law 100–235) as amended by the Clinger-Cohen Information Management Act of 1996 (Public Law 104–106).

5.0. Program organization/structure

The CDAP is organized and structured in phases (fig B–1). Each phase provides a layer of evaluation and builds on the preceding phase/phases. This phased approach allows the requesting unit commander or activity to customize the program to meet needs and expectations. Phases 1 and 2 provide authorization and information about the target AIS network or subnet and establish the “operating/mission parameters.” Phases 3 and 4 provide identification of suspected AIS vulnerabilities. Phases 5 and 6 provide verification of suspected vulnerabilities and analysis of network protection capabilities. Phase 7 provides technical support to assist in the mitigation of these vulnerabilities. Phase 8 provides a final report to the requesting unit/activity. This report is considered "sensitive" and dissemination of information will be controlled by the requesting unit/activity.

5.1. Phase 1 - Request/authorization. The unit commander or activity responsible for the security of the target AIS must make a formal written request to participate in the program and provide the ACERT with specific authorization to analyze and/or penetrate the target network and, if required, conduct concurrent telecommunications security monitoring of the target network.

5.1.1. Objectives. The primary objectives of phase 1 are—

5.1.1.1. Establish written request/authorization to conduct network security analysis of the target AIS network or subnet, and/or telecommunications security monitoring of the target AIS network or subnet. The request will confirm the proper posting of the "notice and consent to monitoring" as specified in AR 380–53, paragraphs 2–4 and 2–5, on all target networks and subnets. Systems without appropriate banners will not be allowed to participate in the CDAP.

5.1.1.2. Establish priority for the effort and enter the request into the CDAP data base for control, management, and scheduling.

5.1.1.3. Establish "operating/mission parameters" for the target network or subnet.

5.1.2. Procedures. The following procedures for phase 1 will be executed:

5.1.2.1. Unit commander requests CDAP assessment and support from ACERT and confirms the proper posting of the "notice and consent to monitoring" banner on the target networks and subnets.

5.1.2.2. CDAP representatives provide pre-brief to unit commander and support staff. Details of each phase, expected outcomes, schedule, limitations, and so forth are discussed.

5.1.2.3. Working relationships are established with the unit points of contact; "operating/mission parameters" are established; and a Memorandum of Understanding is issued between the requesting unit/activity and the ACERT.

5.2. Phase 2 - Fact Finding. The purpose of this phase is to obtain information about the design and implementation of the target network or subnet and information about individual machines on the network.

5.2.1. Objectives. The primary objective of this phase is to obtain copies of network diagrams, obtain survey information from a sampling of users, obtain information about each and every machine on the network by name and address, operating system (OS), location, and dial-in capabilities.

5.2.2. Procedures. The requesting unit/activity shall provide network diagrams and other necessary documentation to the ACERT CDAP team 4 weeks prior to the start of the network survey phase.

5.3. Phase 3 - Network Survey. The purpose of this phase is to compare the target network layout as designed/implemented by the unit to a layout mapped from the outside. This helps to identify potential back doors into the network and assists with security improvement recommendations.

5.3.1. Objectives.

5.3.1.1. Identify all machines on the network at the subnet level.

5.3.1.2. Identify all dial-in connections into the network at the machine level.

5.3.1.3. Compare results with the documentation provided by the unit/activity.

5.3.1.4. Identify all paths of entry into each network subnet and flag risk areas.

5.3.2. Procedures.

5.3.2.1. An automated mapping tool will be used by the CDAP team to target each subnet address. The results will be referred to improve readability and identify connectivity. Results will be interpreted and compared to the layout as designed/implemented by the unit. Any vulnerabilities identified at this stage will be recorded and explored during the scanning and penetration phases.

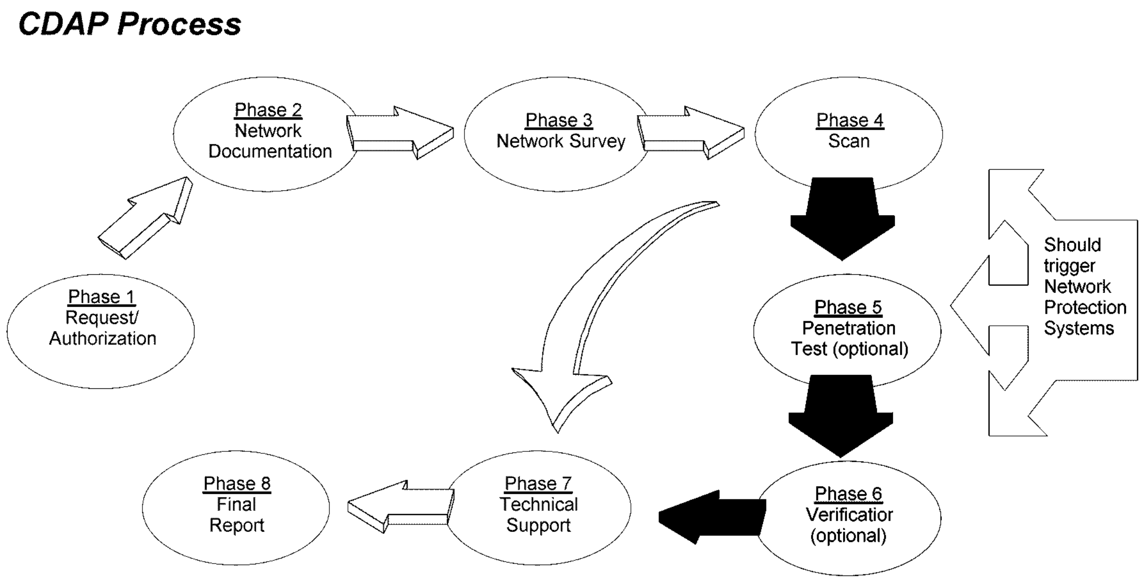

Figure B-1. Computer Defense Assistance Program process

Legend for Figure B-1;

Black arrow: Authorized under AR 380–53 only.

5.3.2.2. An automated dial-in tool will be used by the CDAP team to identify dial-in access points. The results will be compared to the layout as designed/implemented by the unit. Any vulnerabilities identified at this stage will be recorded and explored during the scanning and penetration phase.

5.4. Phase 4 - Network Scan. The purpose of this phase is to assess intrusion susceptibility of the network at the machine level.

5.4.1. Objectives. Identify all machines on the network which can be targeted for potential compromise/intrusion.

5.4.2. Procedures.

5.4.2.1. Using automated computer-based tools, scan the target network to examine and identify network topology, network services running, and types of hardware and software being used on the network.

5.4.2.2. Using automated computer-based tools, gather as much information about remote hosts and networks as possible. Examine network services such as finger, NFS, NIS, ftp and tftp, rexd, and others. The information gathered shall include the presence of various network information services as well as examining the network/subnet for potential security flaws. Security flaws include improperly set up or configured network services, well-known bugs in system or network utilities, and improperly implemented security policies.

5.4.2.3. An analysis matrix shall be completed on each network/subnet examined. Individual machines shall be identified by IP (Internet Protocol) address. Vulnerabilities shall be clearly annotated for further analysis.

5.4.2.4. Analysis of vulnerabilities will be conducted in one of two ways. Penetration testing is the most preferred method of vulnerability analysis, since it involves the actual exploitation of the vulnerability. The second method is AIS security engineering analysis which involves extrapolations of results from known security assessment data bases.

5.5. Phase 5 - Network Penetration. The purpose of network penetration is to examine the degree and depth of information compromise which could be obtained by potential intruders and to assess the ability of the target network/subnet to detect the presence of an intruder. Due to the intrusive nature of this phase, this phase is optional but highly recommended.

5.5.1. Objectives.

5.5.1.1. Exploit only vulnerabilities identified during the scanning phase.

5.5.1.2. Exploit vulnerabilities to the point of obtaining "superuser" access to the target machine or network.

5.5.1.3. Have no adverse effect on the performance of the target network, subnet, or machine.

5.5.1.4. If requested, conduct telecommunications security monitoring of the data traversing the target network, subnet, or machine.

5.5.2. Procedures. All AIS penetration tests and telecommunications security monitoring activities shall be conducted IAW AR 380–53 and Automated Information Systems Penetration Testing: Techniques and Procedures Guide (annex A).

5.6. Phase 6 - Penetration Verification. The purpose of penetration verification is to provide positive verification to the requesting unit or activity that system-level compromise had been obtained and to assess network intrusion detection. Due to the intrusive nature of this phase, this phase is optional.

5.6.1. Objectives. The objective of this phase is to provide positive verification of system or machine compromise in the form of a message or new user account.

5.6.2. Procedures. Following the compromise of the target network, subnet, or machine, the CDAP team shall leave evidence of compromise by inserting a "calling card" into the target. The calling card may be in the form of a new user account or a message for the system administrator. Penetration verification shall be conducted IAW AR 380–53 and Automated Information Systems Penetration Testing: Techniques and Procedures Guide (annex A).

5.7. Phase 7 - Technical Support. The purpose of the technical support phase is to provide support to the requesting unit or activity to fix the vulnerabilities identified during the vulnerability analysis and penetration phases.

5.7.1. Objectives. Assist the requesting unit or activity with security or configuration fixes needed to correct the vulnerabilities found during the vulnerability analysis and penetration phases.

5.7.2. Procedures.

5.7.2.1. Notify the requesting unit or activity as soon as a mission critical vulnerability is detected and provide timely support to fix the problems and secure the network.

5.7.2.2. Prepare correspondence logs of all support efforts provided to the unit or activity.

5.7.2.3. Provide the requesting unit or activity with the results of telecommunications security monitoring operations.

5.8. Phase 8 - Final Report. An executive summary report will be provided to the requesting unit or activity, outlining impacts and recommendations for securing the target network or subnets. The full report will provide detailed information on impacts, risk assessments, and recommended fixes to secure the target network or subnet. This report will be considered "security sensitive" and will be released to the requesting unit or activity only.

6.0. Operating/mission parameters

The operating/mission parameters will be established during phase 1 of the program and documented as part of the MOU. The following are the minimum operating/mission parameters to be exercised by the CDAP effort:

6.1. Verification of compliance with AR 380–53, paragraphs 2–4 and 2–5.

6.2. ACERT Coordination Center (ACERT/CC) will maintain all records pertaining to the CDAP efforts and results. These results will be used for statistical purposes or for follow-on assessments.

6.3. Only the requesting unit or activity and ACERT/CC will have access to the results of the program unless specifically authorized by the requesting authority.

6.4. The requesting unit or activity will determine the extent of the vulnerability analysis, penetration testing, and telecommunications security monitoring.

6.5. All AIS contact with the target network or subnet will be from outside the network but within the .mil environment. Other methods of information operations (IO), such as human engineering, will not be used.

6.6. During penetration testing, the requesting unit or activity explicitly gives consent to the application of techniques and procedures specified in the Automated Information Systems Penetration Testing: Techniques and Procedures Guide (annex A).

6.7. The CDAP team will cease activity if ACERT/CC determines an unauthorized intrusion is occurring during any phase of the program. The CDAP team will follow ACERT/CC established procedures for notifying the unit and protecting the affected network. CDAP efforts on the affected network will not continue until authorization is received by ACERT/CC.

6.8. The CDAP team does not have authority to investigate criminal or foreign intelligence service involvement. If requested, the CDAP team or other ACERT team will provide technical assistance to the proper investigating activity.

6.9. Only personnel with current Top Secret (TS/SBI) security clearances will conduct vulnerability analysis, penetration testing, telecommunications security monitoring, reporting, and technical assessments in accordance with this appendix.

6.10. All CDAP team members will be trained in accordance with the requirements of AR 380–19, AR 380–53, and the Automated Information System Penetration Testing: Techniques and Procedures Guide.

7.0. Responsibilities

7.1. LIWA/ACERT.

7.1.1. The CDAP team will organized and managed by the CDAP Program Manager under the authorization of the Chief, ACERT/CC.

7.1.2. The CDAP Program Manager will coordinate with the requesting units or activities and work directly with the requester's designated POC.

7.1.3. The CDAP Program Manager will ensure certifications and qualifications of all team members conducting CDAP efforts.

7.1.4. The CDAP Program Manager shall ensure understanding of the "operating/mission parameters" by all team members for assigned efforts.

7.1.5. The CDAP Program Manager shall coordinate CDAP efforts with the ACERT/CC to assess the target system's ability to detect and report intrusion or other hostile acts.

7.1.6. The LIWA will establish a training program for CDAP team personnel and provide certification in accordance with AR 380–19, AR 380–53, and the AIS Penetration Techniques and Procedures Guide.

7.1.7. The ACERT/CC shall be responsible for updates and revisions to this appendix in support of AIS security regulations and policies.

7.2. Requesting unit or activity.

7.2.1. The requesting unit or activity is considered to be the customer and the owner of all information systems within its authority.

7.2.2. The requesting unit or activity has the final decision authority for the CDAP level of effort.

7.2.3. CDAP support will not be provided unless based upon a request from the commander or chief of staff responsible for the target network. When the request originates from an organization other than the commander or chief of staff responsible for the target network, the commander of the targeted network must be notified, and the DCSINT of the Army must approve the support based upon a favorable OGC and TJAG legal review.

7.2.4. The requesting unit or activity will appoint a technical point of contact (POC) who will act as the customer's representative during interactions with the CDAP team.

7.2.5. The requesting unit or activity POC will provide confirmation of paragraphs 2–4 and 2–5, AR 380–53, compliance.

ANNEX A. Automated Information Systems Penetration Testing: Techniques and Procedures Guide

1. Authorization

Qualified U.S. Army personnel (military, civilian, and contractors) are authorized to conduct Automated Information Systems (AIS) Penetration Testing (as defined below) IAW AR 380–53.

2. Purpose/definition

As defined by NTISSI No. 4009, AIS Penetration Testing is security testing in which evaluators attempt to circumvent the security features of an AIS based on their understanding of the system design and implementation. Its purpose is to confirm and demonstrate through exploitation the degree of AIS vulnerabilities.

3. Objectives

Using automated computer security assessment tools, qualified personnel are authorized to execute intrusion into target networks, subnets, and AIS machines to—

3.1. Confirm and demonstrate the ease of intrusion and compromise that could be accomplished by unauthorized users (hackers, organized criminals, nation states, terrorist groups, and so forth) located outside the target network.

3.2. Confirm and demonstrate the depth and degree of intrusion.

3.3. Assess the network's ability to detect/respond to intrusion.

3.4. Evaluate/exploit system-level files, user identification, and log-in/log-off scripts only. Other user files and data (including electronic mail) will not be examined, read, modified, recorded, or deleted as part of the penetration testing effort.

3.5. Terminate intrusion activities when root access has been achieved on 10 percent of the total network or it is determined that the identified vulnerabilities cannot be exploited.

4. Procedures

4.1. Penetration testing in support of the U.S. Army will be conducted IAW the provisions of NTISSD 600, DOD Directive 4640.6, and AR 380–53.

4.2. Penetration testing will normally be conducted as an integral part of the ACERT/CC's Computer Defense Assistance Program (CDAP). Appendix B of AR 380–53 provides instructions and procedures for requesting vulnerability assessments and penetration testing. All requests must be provided in writing by the unit commander or the AIS Authority for the target network or subnet, unless the DCSINT of the Army approves a request from another organization to conduct penetration testing. In cases in which the request does not originate from the unit commander, the unit commander will be notified in advance of the exercise, and DCSINT of the Army approval will be based upon OGC and TJAG favorable legal review.

4.3. IAW appendix B of AR 380–53, penetration testing (CDAP phases 5 and 6) will only be accomplished as a follow-on effort to the vulnerability identification phases (phases 1 – 4). Only those vulnerabilities identified during the vulnerability identification phases will be exploited during the penetration process. Additional vulnerabilities may be exposed during the penetration tests. These vulnerabilities may also be exploited. When identical vulnerabilities are found on several machines on the same subnet, the vulnerability will be exploited to the extent necessary to confirm and determine the depth and degree of the vulnerability.

4.4. Penetration testing will only be conducted on U.S. Army automated information systems (machines and networks) that have: (1) the mandatory warning banner prescribed by paragraph 2–5*a*(3) of AR 380–53 in place; (2) MACOM notification procedures certified by the OGC; and (3) the DCSINT of the Army approval to perform Information Systems Security Monitoring operations.

5. Techniques

The penetration process will emulate a "hacker's attack" as much as possible, using software tools or programs generally available to the public. The following are examples of techniques which may be used by penetration testers:

5.1. Obtain user password.

5.1.1. Getting the password file. If password files are not shadowed, testers can copy or paste the file into their own machines and run a password cracking program such as "crack" to process and decrypt users' passwords. If password files are shadowed, testers can view limited user account information, some of which may be sufficient to simply guess the user's password.

5.1.2. Finding passwords in clear text. File Transfer Protocol (FTP) Configuration files and other configuration files contain and pass user identification (userid) and passwords from machine to machine. Some of this information is transferred in clear text if the files are not properly configured. Bad log-in attempts are recorded in clear text; testers can use this information to guess userids and passwords.

5.1.3. Use standard default passwords. Default passwords associated with software utilities and applications can be exploited if the system has not been properly installed and configured. Examples of default passwords and accounts include Guest account with *Guest* as password, Admin account with no password, and so forth.

5.2. Using other users to run a Trojan horse. A Trojan horse is a program that looks like a useful program but has an alternate agenda. Trojan horses installed by the assessment team during penetration testing will be limited to the creation of new user accounts or gaining rights/access.

5.2.1. Program spoofing. Spoofs are a type of Trojan; they duplicate the actions of existing commands and are run unknowingly by the user. Spoofs may be invoked by way of an inappropriate path variable. A spoof that simulates the log-in sequence can be planted onto a terminal. When a valid user enters his/her userid and password, the spoofing program will record the information, tell the user the log-in was incorrect, and exit leaving the real log-in to reprompt. A review of the program records will provide the tester with the userids and passwords. Spoofs installed by the assessment team will only be used to gain access to the system—user information will not be modified, read, or duplicated.

5.2.2. Cron jobs. Cron allows for time-based scheduling of jobs. Permission problems with the cron jobs directory or with any of the processes started from cron allow the tester to substitute his or her own process and gain the privileges of that job.

5.2.3. Modify user startup scripts. Programs can be inserted into a user's startup script; when the user logs in, the programs will be executed.

5.3. Exploitation of configuration errors.

5.3.1. Users' log-in/log-out scripts. Every time a user logs into the system, a set of startup scripts are executed. These scripts are often written by the user and have permissions that are lax or that call programs without the use of fully qualified path names, making them vulnerable to Trojan horse attacks.

5.3.2. File and directory permissions. File and directory permissions are the primary source of security problems on most machines. The security of a file or directory is based on both its permissions and the permissions of its parent directory. Testers can exploit permissions to move from one directory or file to another.

5.3.3. System patch level. Use of older versions of software or failure to install all current security patches leaves systems vulnerable to well-known attacks.

5.4. Exploitation of new software vulnerabilities. This area is most easily exploited. Reports of new bugs or variations of old bugs in system software are released almost daily.

5.5. Exploitation of hardware vulnerabilities. Hardware vulnerabilities are generally caused by the exploitation of features that have been put into the hardware to differentiate it from the competition or to support maintenance of the hardware. Some features that can be exploited include terminals with memory that can be reread by the computer. This memory could contain configuration and password information.

6. Training/qualifications

Penetration testers will be skilled in network security for Novell Netware, Microsoft NT, and/or Unix operating systems and be certified to conduct penetration testing. All personnel conducting penetration testing will receive additional training in the area of COMSEC monitoring rules and procedures IAW paragraph 3–3*a* of AR 380–53.

7. Corrective actions

Penetration testing results will be recorded and published IAW the CDAP reporting standards. Each exploited machine will be identified by IP address and complete details of the exploit and associated risk assessments, and recommended security fixes will be provided. The CDAP team will provide additional assistance as requested. As specified in appendix B of AR 380–53, machine and network specific security vulnerabilities will be disclosed only to the requesting authority. All others will receive non-specific data.

Glossary

Section I
Abbreviations

AGC
Army General Counsel

AIS
Automated Information System(s)

ARSTAF
Army Staff

ASD(C3I)
Assistant Secretary of Defense for Command, Control, Communications, and Intelligence

C4
command, control, communications, and computers

CEO
chief executive officer

CG
commanding general

CI
counterintelligence

CID
criminal investigation division

CIO
chief information officer

COMSEC
Communications Security

DCSINT
Deputy Chief of Staff for Intelligence

DCSOPS
Deputy Chief of Staff for Intelligence

DD
Department of Defense

DISC4
Director of Information Systems for Command, Control, Communications, and Computers

DOD
Department of Defense

EEFI
essential elements of friendly information

FOA
field operating agency

FOIA
Freedom of Information Act

HQDA
Headquarters, Department of the Army

IG
inspector general

INSCOM
United States Army Intelligence and Security Command

JA
judge advocate

LAA
Limited Access Authorization

MACOM
major Army command

MOS
military occupational specialty

NCR
National Capitol Region

NCS
Net Control Stations

OGC
Office of the General Counsel

OPSEC
operations security

RDAT&E
Research, Development, Acquisition, Test and Evaluation

SIGINT
Signal Intelligence

SOP
standing operating procedures

STU
secure telephone unit

TIG
The Inspector General

TJAG
The Judge Advocate General

TRADOC
U.S. Army Training and Doctrine Command

USC
United States Code

Section II
Terms

Communications security
Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Note: Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.

Consent
An agreement by a person to permit DOD communications security components to monitor official communications. Consent may be oral, written, or implied. Consent is implied when adequate notice is given that the use of official Government communications carries with it the presumption of consent.

Electronic surveillance
The acquisition of the contents of nonpublic communication by electronic means without the consent of a person who is a party to the communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter.

Government telecommunications
Telecommunications of an employee, officer, contractor, or other entity of the United States Government which concern an official purpose of Government and which are transmitted over a telecommunications system owned or leased by the U.S. Government or a Government contractor.

Keystroke monitoring
A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the host computer returns to the user.

National Capitol Region
The region that includes the District of Columbia, Montgomery and Prince Georges Counties in Maryland; Arlington, Fairfax, Loudoun, and Prince William Counties in Virginia; and the cities of Manassas, Alexandria, and Falls Church in Virginia.

Nonpublic communications
A communication in which the parties thereto have a reasonable expectation of privacy.

Protected Distribution System
A wire line or fiberoptic communication system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Section III
Special Abbreviations and Terms

ACERT
Army Computer Emergency Response Team

CDAP
Computer Defense Assistance Program

CERT
computer emergency response team

EPITS
essential program information, technology, and systems

FIS
Foreign Intelligence Service

IDN
initial distribution number

IDS
Intrusion Detection Systems

IO
information operations

JCMA
Joint COMSEC Monitoring Activity

LIWA
Land Information Warfare Activity

SOI
signal operation instruction

SSBI
Single Scope Background Investigation

TSCM
Technical Surveillance Countermeasures

Index

This index is organized by topic and subtopic within a topic. Topics and subtopics are identified by paragraph number.

administrative action, 2–8*a*
analyst, 3–5*a*
automated information systems, 1–3*d*

beacons, 2–7*a*

calibration, 2–7
cellular telephones, 1–3*d*, 3–4*e*, 3–4f
classification, 3–5*e*
commercial signals, 2–7*a*
computer banner, 2–5*a*
contractors, 2–10*e*
counterintelligence, 2–6*b*, 2–10*a*, 2–10*h*
criminal activity, 2–8*b*
  Federal offenses, 2–8*b*
  reporting serious crime, 2–8*b*, 4–2
  response procedures, 2–8*c*
  sabotage, 2–8*b*

DD Form 2056, 2–5*a*

disciplinary action, 2–8*a*

electronic surveillance, 3–4*j*

facsimiles, 1–3*d*

Freedom of Information Act (FOIA), 3–5*g*

Joint COMSEC Monitoring Activity (JCMA), 1–4*e*

laboratory signals, 2–7*a*
loss of Government property, 2–8*b*

maintenance, 2–7
monitoring equipment, 3–3*i*, 3–7
  operators, 3–5*a*
  oversight, 4–1

Net Control Station (NCS), 1–1*b*

noncommunications signals, 2–7*a*

pagers, 1–3*d*
public service broadcasts, 2–7*a*

radar, 2–7*a*
recorded media, 2–8*a*
reports, 3–4*i*, 3–6*a*, 4–2

sabotage, 2–8*b*

Secure Telephone Unit (STU), 2–5*a*

signal acquisition, 2–7, 3–3*i*
significant damage, 2–8*b*
supervisors, 3–3*e*, 3–3*f*

tactical radio, 1–1*b*, 3–4*e*

Telecommunications, 1–3*a*
  security, 1–3b, 2–2
  systems, 1–3*d*

telemetry, 2–7*a*
testing, 2–7
threats, 2–8*b*
transcripts, 2–9*c*, 3–4*j*

video teleconference systems, 1–3*d*
violations of Federal law, 2–8*b*

Vulnerability Assessment, 3–6*a*

working materials, 3–5*a*, 3–5*b*, 3–5*d*, 3–5*e*, 3–5*f*

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.52

PIN:	004092–000
DATE:	05-18-98
TIME:	14:38:21
PAGES SET:	21
DATA FILE:	a380x53.fil
DOCUMENT:	AR 380–53
DOC STATUS:	REVISION