Army Regulation 380–19

Security

Information Systems Security

Headquarters
Department of the Army
Washington, DC
27 February 1998

UNCLASSIFIED

SUMMARY of CHANGE

AR 380–19
Information Systems Security

This regulation--

o Requires the use of cost-effective information systems security (ISS) measures to respond to the specific threats and vulnerabilities associated with each information system (para 1-5a).

o Emphasizes the requirement to address security in all stages of system development (para 1-5e).

o Provides information systems security requirements for system administrators (para 1-6d).

o Removed the position/title of terminal area security officer (TASO) to comply with national policies (para 1-6).

o Replaces the acronyms US1, US2, CS1, CS2, and CS3 with Unclassified Nonsensitive, Sensitive But Unclassified, Confidential, Secret, Top Secret, and Sensitive Compartmented Information Subsystem to comply with national policies (para 2-2).

o Removed paragraph 2-11, ’Location and construction of a Central Computer Complex,’ because the U.S. Army has very few central computer facilities under construction and should not be included in an ISS policy regulation.

o Removed paragraph 2-12, ’Mainframe computer equipment room standards,’ because the U.S. Army has very few mainframe computers remaining and should not be included in an ISS policy regulation.

o Addresses security requirements for laptop, notebook, and portable information systems (para 2-11).

o Provides minimum standards for generating and using passwords to control access to information systems (para 2-14).

o Introduces the Land Information Warfare Activity as the Army focal point for reporting system vulnerabilities (2-27).

o Updates reporting requirements for automated information system (AIS) security incidents and technical vulnerabilities (para 2-27).

o Introduces the concept of site-based accreditation for the Sensitive Compartmented Information (SCI) system and an alternative to accrediting collateral systems while taking into account their interconnectivity concerns and allows other related systems to be included in a site (para 3-11).

o Introduces a warning banner for the monitoring of the Army system (para 4-1m).

- Reconstructs chapter 5, Risk Management, to meet the ISS environment currently facing ISS managers.

- Introduces policy and guidance for use of Government-sponsored Internet accounts (app B).

- Incorporates the National Security Agency’s Manual 130-1, annex S, as requested by the Department of the Army Inspector General, to address clearing, purging, declassifying , and destroying magnetic media (app F).

- Provides an Army Management Control Process for administration of the Army Information System Security Program (app C).

Headquarters
Department of the Army
Washington, DC
27 February 1998

*Army Regulation 380–19

Effective 27 March 1998

Security

Information Systems Security

Robert M. Walker
Acting Secretary of the Army

History. This is a revision. Because the publication has been extensively revised, the changed parts have not been highlighted.

Summary. This publication introduces the concept of site-based accreditation, provides new security policies for the use of laptop and small deployable computers and for the use of the Internet and Homepages, and issues minimum requirements for degaussing, declassifying, and downgrading of information and media. This regulation is an update to meet changing information system security (ISS) policies and directives for all Army automated information systems (AIS); it implement the transition to site-based accreditation (SBA) concepts and requirements for those Army intelligence systems subject to Defense Intelligence Agency (DIA) or National Security Agency (NSA) directives derived from Director, Central Intelligence, Directive (DCID) 1/16. This regulation implements the ISS portion of the Command and Control Protect (C2 Protect) component of the Army's Information Operations Program as defined in Field Manual (FM) 100–6 and AR 525–20. This regulation implements national and Department of Defense (DOD) guidance contained in DOD directives governing security for information in an electronic form, including DOD Directives 5200.28, 5200.5, and 5200.19 (when used in conjunction with AR 381–14). It also provides the Army's implementation of sections 1 through 8, Act of 8 January 1988, Public Law (PL) 100–235, U.S. Statute (Stat) 101, pp. 1,724–1,730, cited as the Computer Security Act of 1987. This regulation designates ISS as the security discipline that encompasses communications security (COMSEC), computer security (COMPUSEC). It defines the Army Information Systems Security Program (AISSP) and prescribes a structure for implementing that program. This regulation provides specific policy on accreditation of AIS and networks. It also provides minimum security standards for transmitting classified and sensitive unclassified information.

Applicability. This regulation applies to the Active Army, the Army National Guard of the U.S. (ARNGUS), and the United States Army Reserve (USAR). It applies to contractors who operate Government-owned or contractor-owned, AIS that process or store Army information. Contractors who process Sensitive But Unclassified (SBU) information on contractor-owned AIS are governed by this regulation if specified in the contractual requirements or if they connect to an installation AIS/network system. All of the above must comply with sections 1 through 8, Act of 8 January 1988, PL 100–235, 101 Stat 1, 724–1,730. During mobilization, deployment, or national emergency, this regulation remains in effect without change.

Proponent and exception authority. Effective 1 January 1997, the proponency of this regulation has been transferred to the Director of Information Systems for Command, Control, Communications, and Computers. The proponent has the authority to approve exceptions to this regulation that have received a legal review to ensure that the exception is consistent with controlling law and regulation. The proponent may delegate the approval authority, in writing, to a division chief within the proponent agency in the grade of colonel or the civilian equivalent.

Army management control process. This regulation contains management control provisions and identifies key management controls that must be evaluated.

Supplementation. Major commands may supplement this regulation. Copies of all supplements must be forwarded to Director of Information Systems for Command, Control, Communications, and Computers (SAIS–PAC), 107 Army Pentagon, Washington, DC 20310–107, for concurrence and legal review prior to implementation.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Director of Information Systems for Command, Control, Communications and Computers (SAIS–PAC), 107 Army Pentagon, Washington, DC 20310–107.

Distribution. Distribution of this publication is made in accordance with initial distribution number (IDN) 095066, intended for command levels B, C, D, and E of the Active Army, Army National Guard of the U.S., and U.S. Army Reserve and Government contractors.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 380–19, 1 August 1990.

Chapter 1
Introduction

1–1. Purpose

This regulation establishes Department of the Army (DA) information systems security (ISS) policy. It specifically addresses the ISS subdisciplines of communications security (COMSEC) and computer security (COMPUSEC). (Army Regulation (AR) 381–14 addresses TEMPEST.) This regulation provides the following guidance:

a. Prescribes ISS policy for the protection of classified and sensitive but unclassified (SBU) information processed, stored, or transmitted over automated information systems (AIS).

b. Prescribes unique policies for the following ISS subdisciplines:

(1) COMPUSEC (see chaps 2 and 3).

(2) COMSEC (see chap 4).

c. Deals with all Army AIS. However, certain systems are also governed by the policies, procedures, or directives of the Joint Chiefs of Staff (JCS), Defense Intelligence Agency (DIA), National Security Agency (NSA), Defense Information System Agency (DISA), or other Department of Defense (DOD) directives. In the event of conflicting guidance, major Army commands (MACOMs) should submit a request for a policy review to the Office of the Director of Information Systems for Command, Control, Communications, and Computers (DISC4). This regulation is a minimum standard applicable in all areas not specifically covered in other higher level documents. Refer to the documents listed below for DOD policy and guidance for certain unique applications:

(1) Systems processing intelligence information will comply with national intelligence agency regulations and procedures (such as those of the NSA and DIA) that are, in turn, derived from Director, Central Intelligence, Directive (DCID) 1/16. Accreditation of AIS under the purview of the National Security Agency (NSA) is not governed by this regulation (chap 3) and must be accomplished in accordance with NSA guidance (Supplement 1 to NSA/Central Security Services (CSS) 130–1).

(2) Joint Chiefs of Staff Publication 6–03.7 and other applicable Global Command and Control System (GCCS) publications provide compliance requirements for the GCCS sites.

(3) Joint Chiefs of Staff Memorandum (MJCS) 75–87 provides compliance requirements for systems processing Single Integrated Operational Plan—Extra Sensitive Information (SIOP–ESI).

(4) Department of Defense Publication C–5030–58–M provides the security requirements for an Automated Message Handling System (AMHS) at sites that store or process Sensitive Compartmented Information (SCI) in a consolidated Defense Special Security Communications System (DSSCS)/General Service facility.

(5) Army Regulation (AR) 380–381 (C) provides the security requirements for systems processing Special Access Program (SAP) information.

d. Describes ISS policy as it applies to security in the following areas:

(1) Hardware.

(2) Software.

(3) Procedures.

(4) Telecommunications.

(5) Personnel.

(6) Physical environment.

(7) Networks.

(8) Firmware.

e. Provides guidance for satisfying Department of Defense (DOD) SBU requirements.

1–2. References

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

1–3. Explanation of abbreviations and terms

Abbreviations and terms used in this regulation are explained in the Glossary.

1–4. Responsibilities

a. Deputy Chief of Staff for Intelligence. The Deputy Chief of Staff for Intelligence (DCSINT), Headquarters, Department of the Army, is responsible for certain elements of information security. The DCSINT will—

(1) Review, develop, and coordinate Army input to DOD ISS policy documents.

(2) Establish and issue Army ISS policy and standards.

(3) Oversee the collection, analysis, and dissemination of information on the foreign threat to Army AIS.

(4) Act as the certifying and accrediting authority for security accreditation of certain AIS which process intelligence information (see chap 3).

(5) Develop policy for safeguarding and controlling COMSEC material to be published as AR 380–40.

(6) Establish and maintain standardized evaluation and test methodologies, certification procedures, and security requirements.

(7) Provide a point of contact with DIA and the Information Security Office at NSA to coordinate ISS policy issues affecting AIS processing or storing Army information or an AIS operated/located on Army installations.

(8) Provide guidance concerning the ISS portion of C2 Protect Program, to include the following actions:

(a) Ensure ISS concerns are integrated within intelligence management systems.

(b) Ensure ISS requirements are integrated into intelligence information systems.

(9) Act as approving authority for determining whether a system or site based concept will be used for accreditation.

b. Director of Information Systems for Command, Control, Communications, and Computers. The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) is responsible for certain information security actions. The DISC4 will—

(1) Establish procedures to manage a cohesive Army ISS program, including a contingency plan so that recovery procedures are available if data are modified or destroyed or if the integrity of the system is suspect. At a minimum, the contingency plan should include a Continuity of Operations Plan (COOP) and an emergency destruction plan. Deployable systems must have an emergency destruction plan. The contingency planning process may include Memorandum of Agreement (MOA) back-up for critical support services with another Army command or Federal agency.

(2) Serve as the Army focal point for managing and implementing the Army ISS program and coordinate certification procedures as part of the accreditation process.

(3) Serve as the Army member of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and the subcommittees for Telecommunications Security and Automated Information Systems Security. Distribute throughout the Army, the NSTISSC issuances that are not implemented by other Army promulgations.

(4) Develop and promulgate procedures for Army implementation of national, DOD, and Army ISS policy, directives and standards, including ISS guidelines for specific systems and products.

(5) Review and evaluate proposed policies, procedures, directives, doctrinal publications, plans, material requirements documents, life cycle management documents, basis of issue plans, and similar documents which have ISS implications for adherence to ISS policy.

(6) Participate with the DCSINT in analyses and studies concerning foreign intelligence threats and operational vulnerabilities against which ISS countermeasures are directed.

(7) Assess the effectiveness of new ISS concepts in achieving Army goals and objectives.

(8) Evaluate technological trends in ISS and establish a methodology to integrate advancements into the information mission area (IMA).

(9) Develop, present, and defend Army Information Systems Security Resources Program (ISSRP) requirements in the planning, programming, and budgetary process.

(10) Provide ISS guidance to Army elements to include advising and assisting program managers/project managers/product managers (PMs) in identifying and incorporating ISS requirements in project development.

(11) Provide program oversight of the Army Key Management Program (AKMP) for cryptographic keys.

(12) Act as the Army focal point for the ISS training and awareness program.

(13) Provide a point of contact to the National Computer Security Center (NCSC).

(14) Assist the Deputy Chief of Staff for Operations and Plans (DCSOPS) in evaluating ISS requirements and establishing priority for procurement and fielding of ISS equipment and systems.

(15) Participate in joint ISS programs to ensure compatible and supportable ISS measures are employed in joint systems.

(16) Act as the designated approving authority (DAA) for collateral systems in the following areas:

(a) DA Staff agency systems operating in the multilevel security mode.

(b) Systems developed by program executive officer (PEO)/PM that are generically accredited to operate in the multilevel security mode.

(17) Provide a point of contact with the Defense Information Systems Agency/Center for Information Systems Security (DISA/CISS) for advice and assistance and implementation of certification test programs for Army-operated AIS.

(18) Perform the following actions in regard to the ISS portion of the C2 Protect Program:

(a) Ensure C2 Protect concerns are an integral part of C4I management systems.

(b) Ensure C2 Protect requirements are integrated into C4I information systems.

(c) Implement security countermeasures to protect Army systems.

(d) Serve as the Army focal point for automated Information System Security Engineering and System Security Engineering models.

(e) Serve as the Army focal point for the management of the Army Information System Security Program and the Army C2 Protect Program.

(f) Serve as the Army focal point for validation of requirements for C2 Protect Army Information System Security funds.

(g) Provide C2 Protect direction, procedures and guidance to all Army support organizations.

(h) Ensure C2 Protect is addressed during system development, at the earliest possible time, prior to the initiation of the milestone II advanced technology development (ATD).

(i) Develop and publish C2 Protect system security standards.

c. Deputy Chief of Staff for Operations and Plans. The Deputy Chief of Staff for Operations and Plans (DCSOPS) is responsible for certain elements of information security. The DCSOPS will—

(1) Monitor training activities to ensure that proper emphasis is given to ISS during training conducted at all levels.

(2) Perform the following actions during combat development:

(a) Approve ISS studies and concepts.

(b) Approve operational and organizational plans and required operational capabilities for systems and cryptographic equipment. Establish priorities for the research, development, test, and evaluation (RDTE) effort.

(c) Include realistic and essential ISS requirements in material requirements documentation for AIS.

(d) Monitor the allocation of manpower to accomplish essential ISS functions.

(e) Monitor the individual training programs at Army Service Schools to ensure they include adequate ISS instruction.

(3) Perform the following actions, when establishing requirements:

(a) Integrate ISS into operations security (OPSEC) planning and practices.

(b) Set operational priorities, considering both operational and security requirements, for worldwide distribution of cryptographic equipment.

(4) Prescribe policy and procedures for physical security planning of facilities.

(5) Advise the DCSINT, DISC4, and U.S. Army Criminal Investigation Division (CID) Command on crime and fraud prevention as they relate to AIS.

(6) In coordination with the DISC4, validate Army ISS requirements and establish priorities for procurement and fielding of ISS equipment and systems.

(7) Perform the following actions in regards to the ISS portion of the C2 Protect Program:

(a) Oversee the integration of all developmental C2 Protect technologies and procedures into Army modernization strategies and unit training.

(b) Ensure C2 Protect training is vigorously integrated throughout the force. Provide DA Staff supervision of the planning and execution of C2 Protect in all field training and command post exercises.

(c) Coordinate with the Joint Requirement Oversight Committee (JROC) to minimize duplication and achieve standardization.

(d) Coordinate C2 Protect system performance, operational employment, Tactics, Techniques, and Procedures (TTP) with the other military services and allies, as appropriate.

(e) Coordinate with the Assistant Secretary of the Army for Research, Development, and Acquisition (ASA (RDA)) and DISC4 and DCSINT to ensure C2 Protect is integrated into the U.S. Army's research and development programs.

(f) Identify requirements to the DCSINT for studies and analysis of C2 systems to determine vulnerabilities.

(8) Act as the Army Staff (ARSTAF) operational focal point for Information Operations (IO).

(9) Exercise operational tasking authority over the Land Information Warfare Activity (LIWA), to include prioritization and validation of requests for support.

d. Deputy Chief of Staff for Logistics. The Deputy Chief of Staff for Logistics (DCSLOG) is responsible for certain elements of information security. The DCSLOG will—

(1) Develop logistics policies (including integrated logistics support policy), concepts, procedures, and guidance for distribution, supply, maintenance, and transportation of ISS equipment used in support of all Army information management equipment and systems.

(2) Prescribe execution of NSA or DOD logistics management directives that apply to classified COMSEC and Controlled Cryptologic Information (CCI) material.

(3) Act as proponent of the Army COMSEC Commodity Logistics Accounting Information Management Systems (ACCLAIMS) and AKMP.

(4) Prescribe and supervise the implementation of procedures for property control and the accounting of CCI material during distribution, storage, maintenance, use, and disposal. All guidance will conform with the security standards developed by the DCSINT for safeguarding COMSEC and CCI material.

(5) Supervise logistics support planning to ensure the availability of material and publications needed for repair, test measurement, and diagnosis of ISS equipment and systems.

(6) Ensure C2 Protect Program ISS requirements are integrated into logistics information systems.

(7) Provide continuous logistic support for fielded C2 Protect material and test equipment.

e. The Assistant Secretary of the Army for Research, Development, and Acquisition. The Assistant Secretary of the Army for Research, Development, and Acquisition (ASA(RDA)) is responsible for certain elements of information security. The ASA(RDA) will—

(1) Develop, coordinate, and allocate RDTE and procurement

resources in support of program requirements for ISS. Supervise the execution of RDTE and procurement.

(2) Justify and defend program and budget requirements for ISS RDTE and procurement.

(3) Forward to NSA, Headquarters, Department of the Army (HQDA) approved material requirements documents for cryptographic equipment along with requests for RDTE efforts to fulfill those needs. Designate an Army material developer to monitor development and to satisfy Army material life cycle management milestones.

(4) Monitor NSA or other Service COMSEC or ISS RDTE projects which are of interest to the Army. Designate an Army developing agency as defined in AR 70–1 for each project having potential application for Army use. Require the designated agency to maintain liaison with the developer and inform interested Army agencies of the progress of such projects.

(5) Establish, in coordination with NSA, concurrent life cycle management milestones for the development of cryptographic equipment and any companion information system.

(6) Provide the primary Army member for the NSA COMSEC research and engineering coordination group.

(7) Ensure that ISS program requirements are designed into all AIS under their purview. Develop necessary procedures and guidance so ISS programs are known throughout the ASA(RDA).

(8) Perform the following actions in regards to the ISS portion of the C2 Protect Program:

(a) Provide or coordinate funding for C2 Protect R&D activities.

(b) Provide relevant C2 Protect input to the DISC4 to support Army ISS policy. Plan and coordinate development or procurement of simulated hostile C2 systems for testing and training.

(c) Conduct research and acquire basic knowledge of the techniques and circuitry required to provide an effective defensive (vulnerability assessment) Information Warfare (IW) capability in appropriate types of Army equipment.

(d) Develop capabilities to perform information systems risk analysis, risk reduction, and risk management.

(e) Ensure that Army PEOs/PMs include Systems Security Engineering Modeling in all systems development activities.

f. Commanders of MACOMs, the Chief of the National Guard Bureau (Army System), and the Administrative Assistant to the Secretary of the Army (acting as the MACOM for all HQDA staff agencies). Commanders of MACOMs, the Chief of the National Guard Bureau (Army System)(CNG), and the Administrative Assistant to the Secretary of the Army (AASA) (acting as the MACOM for all HQDA staff agencies) are responsible for certain information security actions. The MACOM commanders, the CNG, and the AASA will—

(1) Administer all aspects of ISS for AIS developed or operated by MACOM personnel, contractors, or field operating agencies under their jurisdiction.

(2) Appoint a knowledgeable individual as the ISS program manager (ISSPM) to implement the ISS program within their respective commands. Provide the ISSPM with sufficient staff and resources to effectively manage the COMPUSEC and COMSEC subdisciplines of ISS.

(3) Establish an ISS personnel structure to ensure that ISS responsibilities are delineated at all echelons of the MACOM as required by paragraph 1–6.

(4) Ensure proper accreditation of AIS that fall under their authority as specified in chapter 3.

(5) Ensure the DODIIS COMPUSEC program is properly implemented and develop guidance where necessary.

g. Commanding General, U.S. Army Intelligence and Security Command. Commanding General (CG), U.S. Army Intelligence and Security Command (INSCOM), in addition to the MACOM responsibilities above, will—

(1) Serve as the Army Service Cryptologic Element (SCE) and point of contact for AIS under the purview of NSA. Provide implementing guidance to NSA promulgations as required.

(2) Provide counterintelligence support to Army elements on ISS matters and advise accreditation authorities on the foreign intelligence threat.

(3) Provide technical advice and assistance to MACOMs, as requested, on implementation and/or operation of the DODIIS COMPUSEC program.

(4) Conduct the certification test program for all Army intelligence AIS.

(5) Coordinate with the Army Computer Emergency Response (ACERT)/Coordination Center for security incidents and violations as applicable for Army.

h. Commanding General, U.S. Army Training and Doctrine Command. Commanding General, U.S. Army Training and Doctrine Command (TRADOC), in addition to the MACOM responsibilities above, will—

(1) Integrate approved ISS doctrine, procedures, and techniques into applicable programs of instruction for TRADOC schools.

(2) Develop Army-wide training literature and training aids in support of the ISS training and awareness program.

(3) Integrate ISS procedures and techniques into the formal evaluations of both individual soldiers and units.

(4) Develop, test, and recommend operational and organizational concepts and doctrine to achieve ISS goals.

(5) Conduct or participate in operational tests of ISS implementations as part of system-wide operational tests, as directed.

i. Commanding General, U.S. Army Materiel Command. Commanding General, U.S. Army Materiel Command (AMC), in addition to MACOM responsibilities above, will—

(1) Ensure that the ISS requirements are integrated into the architecture, hardware, software, and systems engineering of those systems for which AMC is the material developer.

(2) Provide ISS Army wide material developer support for RDTE and production.

(3) Assist AIS functional proponents and PMs in identifying security requirements for proposed or existing tactical (deployable) battlefield systems.

(4) Perform integrated material management of unclassified and classified COMSEC and CCI commodities.

j. Program executive officers and program managers. Program executive officers (PEOs) and program managers (PMs) will—

(1) Ensure that the requirements of this regulation are applied throughout the project development of all AIS.

(2) Ensure information systems security engineering is embedded in all system research, development, testing, and evaluation (RDT&E) activities.

(3) Act as the accreditation authority for generic accreditation for systems as indicated in paragraph 3–8.

(4) Appoint an ISS manager (ISSM) to perform those duties listed in paragraph 1–6*d*(2). Additionally, the ISSM is responsible for implementing and managing all security aspects of systems development efforts unique to PEO/PM organizations which are not specifically addressed by this regulation.

(5) Ensure the ISSM has performed the pre-deployment duties listed in paragraph 1–6, as appropriate.

(6) Ensure that designated ISSMs and information systems security officers (ISSOs) effect continuous coordination with the MACOM ISSPM in which the systems being developed are to be demonstrated, tested and/or fielded.

(7) Ensure that draft generic accreditation documentation per paragraph 3–2 is completed and delivered to the MACOM ISSPMs prior to initial operational test and evaluation.

(8) Ensure that approved generic accreditation documentation is delivered to the receiving MACOM ISSPM prior to delivery of the system to the receiving unit.

(9) When PEO/PM retains responsibility for system changes subsequent to deployment, ensure that generic reaccreditation documentation reflecting system changes is provided to MACOM ISSPMs and using activities.

(10) Perform the following actions in regards to the ISS portion of the C2 Protect Program:

(a) Integrate system security engineering processes into system design and development.

(b) Integrate ISS practices into pre-milestone zero activities and events.

(c) Develop and submit to the system DAA a C2 Protect system security engineering implementation plan for all transport and information systems developments for which they have design and development responsibilities.

(d) Develop and perform security risk analysis on all systems developments before determining the omission of security features.

(e) Perform acquisition and life-cycle management of material in support of the IO strategy.

1–5. Security-related requirements

a. Automated information systems exhibit inherent security vulnerabilities and are known to be targeted by a number of sources other than the foreign intelligence services. Cost-effective ISS measures must be established and applied to manage identified risk against these powerful vulnerabilities and threats.

(1) Measures taken to attain ISS objectives will be commensurate with the importance of the operation to mission accomplishment, the sensitivity and criticality of the material being processed, and the relative risks (threats and vulnerabilities) to the system. Cost-effective ISS measures will be applied to counter identified risks.

(2) Statements of security-related requirements will be accomplished in the earliest phases of AIS development and followed through subsequent phases of the system development life cycles.

(3) AIS procurement packages will include security requirements that are based on stated needs and a cost-benefit analysis.

(4) Costly or elaborate security countermeasures will be applied only when the risk analysis indicates that administrative, personnel, physical, and other less costly measures do not achieve an acceptable level of risk.

b. Defense information labeled Classified, Unclassified Non-Sensitive, and Sensitive But Unclassified defense information in Army AIS must be safeguarded against unauthorized disclosure, modification, destruction, and denial of use. Information systems security measures must be designed to ensure confidentiality, integrity, and availability of information and AIS resources that impact on mission accomplishment. Information systems security countermeasures must also prevent unauthorized use of Army AISs. The specific mix of ISS measures chosen will depend on the relative importance of the AIS mission and the information. Information that is SBU will normally fall into one of the following categories.

(1) Systems that contain sensitive but unclassified information are exempt from the provisions of sections 1–8, Act of 8 January 1988, Public Law 100–235, and U.S. Statute at Large, volume 101, pp. 1724–1730, cited as the Computer Security Act of 1987. This information requires protection primarily from foreign intelligence services to ensure confidentiality. This information must be protected if it falls in any of the following categories:

(a) Involves intelligence activities.

(b) Involves cryptologic activities related to national security.

(c) Involves command and control of forces.

(d) Is contained in systems that are an integral part of a weapon or weapon system.

(e) Is contained in systems that are critical to the direct fulfillment of military or intelligence missions.

(f) Involves processing of research, development, and engineering data.

(2) Information labeled SBU must be protected to ensure confidentiality, availability, and integrity and may or may not require protection from foreign intelligence services or other unauthorized personnel. Examples may include information dealing with logistics, medical care, personnel management, Privacy Act data, contractual data, For Official Use Only (FOUO) information, and certain categories of financial data.

c. Information will be safeguarded by the application of protective measures addressed in chapter 2. Applicability of safeguards will be determined through the risk management review and may consist of the following:

(1) Hardware security.

(2) Software security.

(3) Procedural security.

(4) Telecommunications security.

(5) Personnel security.

(6) Physical security.

(7) Network security.

(8) Firmware.

(9) TEMPEST per AR 381–14.

d. Each AIS handling classified or SBU information will be subject to a risk management program per chapter 5 and will undergo a detailed review leading to formal accreditation according to chapter 3.

e. Compliance with ISS requirements is an integral part of the Information Management Area (IMA), the Army technical architecture, and life-cycle management of information systems defined in AR 25–1.

f. The application of ISS measures must include compatibility considerations.

g. Training in ISS principles and techniques will be integrated into unit operations at all levels of command.

1–6. U.S. Army Information Systems Security Program

a. The Army Information Systems Security Program (AISSP) is a unified approach to protecting classified, unclassified, and SBU information while in AIS and is established to consolidate and focus Army efforts in securing that information and its associated systems and resources. The AISSP encompasses security requirements of AIS during development, acquisition, training, deployment, operations, maintenance, and disposition. The AISSP has been created in recognition of the Army's widespread use of AIS and the unique problems associated with their security. The potential risk to an AIS increases as more interfacing systems are implemented, more sensitive information is handled, and more complex functions are performed.

b. The AISSP is designed to achieve the most effective and economical security possible for all AIS using the risk management approach for implementing security safeguards. To attain an acceptable level of risk, a combination of staff and field actions are necessary to develop policy and guidance, identify problems and requirements, and adequately plan for required resources.

c. Commanders and managers are responsible for implementing the AISSP in their command or activity and will ensure the following is accomplished:

(1) Systems within their command or activity are operated within the requirements of this regulation.

(2) Requests for new systems or changes to existing systems include security requirements appropriate to the system's concept of operation. Once validated, these security requirements must be incorporated into the system design and defined in procurement contracts.

(3) Use of commercial-off-the-shelf (COTS) products or specific production requirements is consistent with ISS requirements and does not render necessary security measures impractical or cause unacceptable degradation in security.

d. A clearly defined structure of ISS personnel will assist commanders and managers in implementing the AISSP. These personnel act as the focal point for ISS matters within their command or activity. They should have the authority to enforce security policies and safeguards for systems within their purview. This authority includes stopping system operation if warranted by the impact of a security deficiency. This hierarchical structure will be established as follows:

(1) *Information systems security program manager.* At each Army MACOM and within the Office of the Administrative Assistant to the Secretary of the Army (acting as the HQDA MACOM), an information systems security program manager (ISSPM) will be appointed to establish, manage, and assess the effectiveness of the ISS program within that command or activity. This individual will be assigned sufficient personnel assets to effectively manage the COMPUSEC and COMSEC subdisciplines of ISS. The ISSPMs

appointed by MACOM commanders and the Administrative Assistant to the Secretary of the Army will—

(a) Establish and manage the command ISS program, to include defining the ISS personnel structure and directing the appointment of an ISSM at appropriate subordinate commands, installations, DA staff agencies, and field operating activities.

(b) Promulgate ISS guidance within each command, to include developing command-unique guidance, as required.

(c) Establish a procedure within the command to document the status of all AIS accreditation, the AIS sensitivity level, and the security mode of operation.

(d) Establish and oversee an ISS training program that meets the requirements of this regulation and integrates ISS into operational training programs for managers, system administrators, users, and maintenance personnel.

(e) Develop guidance to ensure the DODIIS COMPUSEC program is properly implemented.

(f) Establish, conduct, and oversee a program of announced and unannounced ISS inspections to determine compliance with this regulation and other applicable security directives. Notify the commander of the results of such inspections.

(g) Develop the applicable portion of the ISS resource requirements for the MACOM.

(h) Maintain a strong liaison with supporting DISA, CID, and INSCOM elements.

(i) Develop and maintain an Internet security policy (see app B).

(j) Administer management evaluation controls (see app C).

(2) *Information systems security manager.* At all appropriate levels of command below Army MACOM and at DA staff and field operating agencies and at the PEO level, an information systems security manager (ISSM) will be appointed to establish and implement the ISS program for all AIS within that command or activity or for AIS under development. This includes posts, installations, and installation equivalents. These appointments will result in a chain of command for ISSM that parallels the command structure. The ISSM may not be capable of directly handling all aspects of ISS within their purview as AIS expand in geographic boundaries. The ISSMs can secure the growing complexity of personal computers (PCs), local area networks (LANs), metro area networks (MANs), and wide area networks (WANs) by assigning various tasks to ISSOs and system administrators. For systems within their purview, ISSMs will—

(a) Oversee the execution of the ISS training and awareness program within their command or activity.

(b) Ensure that an information systems security officer (ISSO) is appointed for each separate AIS, group of AIS, or network, as necessary.

(c) Establish an AISSP that will provide protection for all information systems and ensures all AIS and/or networks are accredited per this regulation.

(d) Periodically review the status of all AIS and networks to ascertain that changes have not occurred that affect security and negate the accreditation.

(e) Review threat and vulnerability assessments to enable the commander or manager to properly analyze the risks to the AIS information and determine appropriate measures to effectively manage those risks.

(f) Report security incidents and technical vulnerabilities per this regulation, AR 381–14 (S), AR 380–5, and AR 381–12. All attempts and actual penetrations of Army AIS will be immediately reported to ISSM. In turn, the ISSM will notify the Land Information Warfare Activity's (LIWA) Army Computer Emergency Response Team (ACERT) or its subordinate computer emergency response team (CERT) infrastructure, who will notify HQ, CID, and the Army Case Control Office (ACCO) at INSCOM of all successful penetration incidents. The local supporting CID and INSCOM office should also be notified.

(g) Implement the DODIIS COMPUSEC program and site-based accreditation, where feasible.

(h) Establish the scope of responsibilities for each ISSO using guidance from the ISSPM and applicable regulations.

(3) *Information system security officer.* For each AIS or group of AIS, there will be an information system security officer (ISSO) appointed by the commander or manager of the activity responsible for the AIS. The same ISSO may be appointed for multiple AIS, particularly in the environment where personal computers, workstations, file servers, local area networks, or small systems are oriented toward the functional user as the operator. The ISSOs will perform the following duties for each AIS under their purview:

(a) Ensure systems are operated and maintained according to this regulation.

(b) Ensure managers, system administrators, and users have the appropriate security clearances, authorizations, and need-to-know.

(c) Include all personnel associated with AIS in system-specific and general awareness security training.

(d) Conduct threat and vulnerability assessments to enable the commander or manager to properly analyze the risks to AIS information and determine appropriate measures to effectively manage those risks.

(e) Prepare, distribute, and maintain plans, instructions, guidance, and standing operating procedures (SOPs) concerning the security of system operations.

(f) Report immediately to the ISSM any attempt to gain unauthorized access to information or any system failure or suspected defect that could lead to an unauthorized disclosure, loss of integrity, or unavailability of system information.

(g) Review and evaluate the security impact of system changes, including interfaces with other AIS. Ensure that all interconnected systems comply with the security requirements levied within the infrastructure and do not have a negative security impact on any other systems with which they must interact and support.

(h) Report security incidents and technical vulnerabilities to the ISSM per this regulation, AR 381–14 (S), AR 380–5, and AR 381–12. Incidents involving criminal activity or foreign intelligence services will also be reported to the local CID or supporting counterintelligence (CI) field office. Refer to paragraph (*f*) above for additional information and guidance and required reporting procedures.

(i) Prepare or oversee the preparation of the certification and accreditation documentation.

(j) Maintain a current network or AIS certification or accreditation statement and initiate recertification and re-accreditation when changes affecting security have occurred.

(k) Establish and implement a system for issuing, protecting, and changing system passwords.

(l) Oversee the review of system audit trails and resolve discrepancies.

(m) Maintain access control records and ensure they are reviewed at least weekly. Ensure that only authorized personnel can gain access to the system.

(n) Ensure appointment of individuals, as needed, for securing each terminal, inal, workstation, computer, or associated group of computers that are not under the direct control of the ISSO.

(o) Maintain close liaison with supporting system administrators to promote security at all levels of AIS operations.

(4) *System administrators.* System administrators (SAs) must be trained in in all aspects of information system security. The SAs must be highly trained and experienced on the AIS that they are required to maintain. The SA must be able to maintain the AIS audit functions and have the ability to review audit information for detection of possible system abuse and to coordinate with the ISSO. SA responsibilities for maintaining, securing and monitoring systems are provided in appendix G, "Monitoring Capabilities and Restrictions." Systems administrators are encouraged to discuss the limitations of their authorities and the implications of appendix G with their supporting legal advisors. In coordination with the ISSO, the SA must ensure that all components of the AIS are protected so that the AIS can effectively and securely operate in the three operational modes: in-garrison, in-transit, and deployed.

e. In addition to this hierarchical structure, the following personnel have crucial roles in the AISSP.

(1) Certification authorities and accreditation authorities will be identified for all AIS as described in chapter 3.

(2) The COMSEC custodians and command COMSEC inspectors will be appointed as required in AR 380–40.

(3) Command intelligence officer (DCSINT/G2/S2). For each network, the command intelligence officer or activity equivalent will be identified to assume the responsibility for identifying and assessing foreign intelligence threats to command assets. The command intelligence officer will—

(a) Ensure the Command Statement of Intelligence Interest (SII) (AR 381–10 and AR 381–20) registers requirements for the receipt of validated intelligence impacting upon the integrity and reliability of AIS.

(b) Provide assistance in the identification of threat factors impacting upon the risk management approach for implementing security safeguards in accordance with paragraph *b* above.

(c) Coordinate with national intelligence production agencies on behalf of commanders and managers to request information to fill intelligence gaps developed during any phase of the AISSP process.

f. Implementing the AISSP in installation or installation-equivalent environments involving host and tenant units or activities requires thorough coordination between the host and tenant ISS personnel. Army tenant units or activities must comply with this regulation and the ISS requirements of their parent MACOM. Army tenant's and non-Army tenant's AIS operations must comply with the host installation ISS policy that does not conflict with their parent command/activity or agency ISS policy and that does not impede their operational mission objectives. Conflicts of ISS policy that cannot be resolved per this regulation should be addressed through local command channels to HQDA, DISC4. Non-Army tenants must comply with the host installation security requirements if they connect to the installation's information infrastructure. This includes the use of gateways or information management resources as pathways to connect their information systems. If the non-Army tenant uses any part of the host installation IMP infrastructure, the host installation ISSM will require the use of configuration management control consistent with the installation's information management and configuration management process.

(1) Host installation ISSM will—

(a) Ensure that adequate ISS support is provided to tenant activities and written into inter-service support agreements.

(b) Ensure that tenant activities are included in the installation physical security plan, ISS plan, and AIS plans and procedures, as appropriate.

(c) Ensure integration and coordination of installation-level activities that affect security requirements of tenant activities.

(d) Identify security risk that may occur as a consequence of a relationship between different systems that must be understood and accepted.

(2) Army tenant activities will—

(a) Identify AIS to the host installation ISSM.

(b) Provide accreditation status, including date of accreditation and sensitivity level to the host installation ISSM.

(c) Identify their security support requirements to the host installation ISSM and provide technical assistance as may be required.

(d) Identify a point of contact for ISS matters to the host installation ISSM.

Chapter 2
Computer Security

Section I
General Policy

2–1. Overview

a. This chapter provides guidance to implement ISS requirements defined in national level security directives and policies and establishes the Army security policies that apply uniquely to AIS.

b. Security policy for AIS will be defined at concept development. Security requirements based on this policy will be considered throughout the life cycle. There will be a security plan for AIS processing classified information and SBU information, showing the steps planned to comply fully with stated security requirements.

c. A DAA will be responsible for the overall security of each AIS.

d. The AIS developer must ensure the early and continuous involvement of the PEO, PM, the functional proponent, users, ISSM, ISSO data owners, certification authority, and DAAs in defining and implementing security requirements of the AIS.

e. Statements of security requirements will be included, as applicable, in the acquisition and procurement specifications for AIS. The statements will reflect an initial risk assessment and will specify the required level of trust per DOD 5200.28–STD. The PEOs/PMs or functional proponents will not field and commanders will not accept, the following systems:

(1) Systems that do not meet minimum standards stated in the acquisition and procurement specifications.

(2) Systems that do not provide complete documentation supporting certification and accreditation.

(3) Systems that have not been fully certified or generically accredited.

f. Classified or SBU data will not be introduced into an AIS until the data classification and sensitivity of the AIS has been determined. The appropriate AIS protection mechanisms will be in place and DAA approval to operate will be obtained. The data owner will approve entering the data, where applicable. Data will not exceed the security classification level for which the AIS is approved to process.

g. Commanders will ensure that AIS under their purview are operated in a manner consistent with the system accreditation and this regulation.

h. Organizations must strive to ensure that new AIS development and modifications to existing AIS are performed in a manner that makes security an integral part of the development, acquisition, fielding, and operational processes.

i. There will be a security plan for AIS processing classified and SBU information, showing the steps to comply fully with stated security requirements. The security plan evolves through system life cycle and security requirements into the Security Plan/Accreditation Document (see app D).

2–2. System sensitivity designation and mode of operation

a. The AIS will be categorized based on the sensitivity of information that the system is authorized to process or store.

(1) The AIS that process classified information will be designated by the highest classification, handling code, and category of information processed (for example, Confidential, Secret, TS/SCI, SIOP–ESI).

(2) The AIS that process unclassified information will be designated as SBU.

b. The security processing modes of operation are based on DOD 5200.28 and DCID 1/16 for systems processing intelligence information. Determination of the security processing mode of an AIS is based on the classification or sensitivity and the formal categories of data processed and the clearance, formal access approval, and need-to-know of users of the system. Formal categories of data are those for which a written approval must be issued before access; for example, SCI compartments, North Atlantic Treaty Organization (NATO) information, or SAPs. The available or proposed security features of the system are not relevant in determining the actual security mode. All AIS will be accredited to operate in one of the following security processing modes:

(1) *Dedicated security mode.* A mode of operation wherein all users who access the system directly or indirectly possess the required personnel security clearance or authorization, formal access

approval, and need-to-know for all information the system is accredited to process.

(2) *Systems high security mode.* A mode of operation wherein all users who access the system directly or indirectly possess the required personnel security clearance or authorization and formal access approval but not necessarily a need-to-know for all information the system is accredited to process.

(3) *Compartmented security mode.* A mode of operation wherein all users who access the system directly or indirectly possess the required personnel security clearance or authorization but not necessarily formal access approval or a need-to-know for all information the system is accredited to process.

(4) *Multilevel security mode.* A mode of operation wherein not all users who access the system directly or indirectly possess the required personnel security clearance or authorization, formal access approval, or a need-to-know for all information the system is accredited to process.

2–3. Minimum requirements

a. All AIS processing classified or SBU information will achieve the minimum requirements of this paragraph through automated or manual means. Commanders and accreditation authorities may impose more stringent requirements based on a risk analysis. All risk analyses will evaluate the possible vulnerabilities and the security impact on associated AIS and networks within the area of responsibility. Although manual procedures are acceptable when an automated safeguard is not feasible, security safeguards should be embedded into design of AIS to ensure a secure infrastructure.

(1) *Accountability.* Safeguards will be in place to ensure that each person having access to an AIS may be held accountable for his or her actions on the AIS. For all AIS except small computers (see the Glossary for workstations and laptops), a security audit trail will provide a documented history of AIS use. In a client server environment (CSE), audits will not be collected at the workstation level but will be maintained at the server level. The audit trail will be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise or damage should a security violation or malfunction occur. Audit trails should be reviewed for security implications daily but, as a minimum, will be reviewed once per week. The DAAs will determine how long to retain the audit information. The manual or automated audit trail will document the following:

(a) The identity of each person and devices accessing the AIS.

(b) The date and time of the access.

(c) User activity sufficient to ensure user actions are controlled and open to scrutiny.

(d) Activities that might modify, bypass, or negate safeguards controlled by the AIS.

(e) Security-relevant actions associated with periods of processing or the changing of security levels or categories of information.

(f) Other security-relevant events. The list of events will be provided as part of the accreditation request for approval of the DAA.

(2) *Access.* Each AIS will have an associated access control policy that will include features or procedures to enforce the access control measures required for the information within the AIS. The identity of each authorized user will be established positively before granting access.

(3) *Security training and awareness.* All persons accessing an AIS will be a part of the security training and awareness program. The program will ensure that all persons responsible for managing AIS resources or who access AIS are aware of proper operational and security-related procedures and risks. As a minimum, items detailed in paragraph 2–16 below will be covered.

(4) *Controls.* All AIS hardware, software, and documentation and all data handled by the AIS will be protected to prevent unauthorized (intentional or unintentional) disclosure, destruction, or modification and will provide control measures. The level of control and protection will be commensurate with the maximum sensitivity of the information present in the system and will provide the most restrictive control measures required by the data to be handled. This includes personnel, physical, administrative, and configuration controls. Unclassified hardware, software, or documentation of an AIS will be protected if access to such AIS resources reveals classified information or information that may be used to eliminate, circumvent, or otherwise render ineffective the security safeguards for classified information. Software development and related activities (for example, systems analysis) will incorporate appropriate security measures.

(5) *Marking.* Markings on classified or SBU output will reflect the sensitivity of the information as required by existing directives. Army Regulation (AR) 380–5 contains requirements for security classification and applicable markings for classified information, and AR 25–55 governs FOUO information. Appropriate markings will be applied manually or through an automated means (that is, the AIS has a feature that produces the markings). Automated markings on classified output must not be relied on for accuracy unless the security features and assurances of the AIS meet the requirements for a minimum trusted computing base class of B1 as specified in DOD 5200.28–STD. If the B1 requirement is not met, but automated controls are used, all classified output will be protected at the highest level of classification of the information handled by the AIS until an authorized person manually reviews it to ensure that it was marked accurately with the classification and special markings. All media will be marked and protected commensurate with the requirements for the highest security classification level and the most restrictive category of information ever stored on the media until the media is declassified or destroyed under this regulation or until the information is declassified or downgraded under AR 380–5.

(6) *Least privilege.* The AIS will function so that each user has access to only the information to which he or she is entitled (by virtue of clearance and formal access approval). In the case of need-to-know for classified information, access must be deemed essential to accomplish lawful and authorized Government purposes. Users will also be restricted from having access to system privileges that allow operations on data and other system resources not required to perform their job.

(7) *Data continuity.* An owner or proponent will be identified for each file or data grouping on the AIS throughout its life cycle. The file or data grouping accessibility, maintenance, movement, and disposition will be governed by security clearance, formal access approval, need-to-know, and protective marking as appropriate. All files or data groupings will be labeled to ensure that the security classification and or special markings are maintained during storage, processing, and communication transfer.

(8) *Data integrity.* Appropriate safeguards will be in place to detect and minimize unauthorized access and inadvertent, malicious or nonmalicious modification or destruction of data. There will be an appropriate safeguard to ensure that security classification labels remain with the data if it is transmitted via a network to some other AIS.

(9) *Accreditation.* Before operation, each AIS will be certified and accredited under a set of security requirements and safeguards approved by the DAA.

(10) *Risk management.* A risk management program will be put in place to determine what level of protection is required, what protection currently exists, and the most economical way of providing the needed protection (see chap 5).

(11) *Security planning.* An AIS security plan will be developed and maintained for the life of each AIS, including prototype, test, and developmental systems. The security plan evolves into the accreditation document and will be maintained to reflect system changes. (See app D for suggested format.)

(12) *Copyright laws.* Personnel who violate copyright laws will be subject to disciplinary actions per appropriate Army regulations, which may result in civil or criminal penalties by judicial action.

b. In addition to the requirements above, AIS operating in other than the dedicated security mode must provide security features that meet the trusted computing base (TCB) from DOD 5200.28-STD. as determined by the procedures in appendix D of this document. The following instructions for implementation of these provisions apply:

(1) All AIS that process or handle classified or SBU information and require at least Controlled Access Protection (that is, TCB class C2 security protection) will implement required security features based on the procedures described in appendix C of this document.

(2) If the procedures in appendix E require a Trusted Systems class above the trusted computing class of C2, a timetable for meeting this requirement will be determined individually for each system. This timetable will be part of the accreditation, and it must be approved by the DAA.

(3) These requirements will be met either by using trusted computer products listed in the NSA Information System Security and Service Catalogue, using a product not in the catalogue that has security features that meet the level of trust required for the AIS or developing a product that has security features that meet the level of trust required. In any case, the cognizant DAA will determine whether or not all security requirements in DOD 5200.28–STD have been satisfied.

(4) For an existing AIS, there are cases where introduction of additional computer-based security features, according to the schedule given in subparagraphs 2–3*b*(1) and (2), may be prohibitively expensive, time-consuming, or technically unsound or may adversely affect operational effectiveness to an unacceptable degree. In such cases, an exception to the requirement may be approved by the DAA with the written concurrence of the MACOM commander or the Administrative Assistant to the Secretary of the Army (acting as the MACOM commander for HQDA activities). Application for such exceptions will include a determination that one or more of the conditions in this paragraph exist. Exceptions should be reviewed during each reaccreditation.

Section II
Software Security

2–4. Software controls

a. Controls will be implemented to protect system software from compromise, subversion, or unauthorized manipulation.

b. All software used on Army AIS must be approved by the ISSM or ISSO prior to installation and operation.

c. Each Army AIS will include an identified list of executable software that is authorized to be run on that AIS. Such software will be protected from unauthorized modification to the maximum extent possible by the hardware and software mechanisms of the AIS. If the risk analysis reveals unacceptable risk from attacks by malicious software, additional measures (for example, commercial“anti-virus” programs, tamper-resistant holographic seals, and non-technical security methods) will be employed to reduce this risk to an acceptable level.

d. Documentation that addresses software design and capabilities will be maintained for the use of programming, operations, and user personnel. Only personnel performing official duties should be allowed access to this software documentation.

e. Upon acceptance for operational use, whether developmental, governmental off-the-shelf (GOTS), or commercial off-the-shelf (COTS), software must be kept under close and continuous configuration management controls so that unauthorized changes are not made. A master copy of the software must be safeguarded and never used for actual production operations. Production copies of software should be generated from the master copy as required. System and application program libraries will be protected and backup copies maintained. Strict configuration management controls will be enforced to lessen the risk of introducing untested or malicious software.

f. Operational software may be modified and maintained only under rigorously controlled conditions requiring verification.

g. Personnel who violate computer software copyright laws will be subject to disciplinary actions per appropriate Army regulations and (where applicable) the UCMJ. Such actions may result in civil penalties by the software manufactures and/or the Army.

2–5. Data base management systems

a. Protecting shared data bases is essential, as they represent a significant asset and frequently reveal considerably more information taken as a whole than can be obtained from their individual parts. Commercial data base management systems have different characteristics, such as those listed below, that affect their security stability and must be considered when acquiring a system for handling classified or unclassified information:

(1) Distributed data base access and synchronization,

(2) Data-base integrity,

(3) Data-base availability (fail-over, recovery, and restart functions),

(4) Data and program protection mechanisms that control read and write permission levels, and

(5) Audit mechanisms and utilities.

b. When data base management systems containing classified defense information are used, the classified identifiable element (for example, word, field, or record) within the data base must be protected according to the highest security classification of any database element. If the data base cannot provide field protection, then it should provide record protection to the highest security classification level of the fields within the record. Data-base systems that do not provide protection at the record or field level will be restricted to operation in the dedicated or system high security mode. In all cases the data base management systems (DBMS) must meet the minimum trust requirements identified in paragraph 2–3 above.

c. Data-base systems that bypass the production of operating system audit trail data must produce their own audit trail data similar to those prescribed for the operating system. These audit trails must also be used in determining the confidentiality, integrity, and availability of the automated system and the data contained therein.

d. Designers and developers of data base management systems, in coordination with security specialists and proponents for the data elements, must consider the effect that compilation of data will have on the final security classification of the data-base system. The degree to which a given user can be reliably denied access to portions of the data base will influence the final classification decision.

e. A data-base administrator (DBA) will be appointed for each data base and appropriate duties assigned by the ISSM.

2–6. Software security packages

a. Software security packages are available from various commercial vendors. Products other than those evaluated by the NSA and included in the NSA Information System Security Products and Services Catalogue may be used; however, such products must be approved by the DAA and based on a valid justification.

b. The evaluation of software security packages must be included in the risk assessment so that the accreditation authority can document advantages and disadvantages.

c. The decision to use software security packages will be based upon cost and the level of security protection required.

d. The DISC4 must approve purchase or annual lease costs of products not listed in the NSA Information System Security and Services Catalogue that exceed $50,000.

2–7. Software design and test

a. Software security requirements must be considered in the future design, development, and acquisition of Army systems.

b. Examination of the control over the procedures used to develop computer programs is an integral part of the software certification and AIS accreditation process. The key to eventual certification is to develop systems that are easily understood and verifiable.

c. Programs must be completely tested before becoming operational. Both valid and invalid data must be used for testing. Testing is not complete until all security mechanisms have been examined and expected results are attained and attempts to circumvent or defeat these mechanism fail.

d. Upon completion of maintenance or modification of software, independent testing and verification will be required before returning software to operation.

Section III
Hardware Security

2–8. Hardware-based security controls

a. Hardware-based security controls represent an important factor when evaluating the security environment of any Army system. The absence of hardware-embedded security features or the presence of known hardware vulnerabilities will require compensation in other elements of the security program.

b. Hardware security requirements must be considered in the future design, development, and acquisition of Army systems.

2–9. Maintenance personnel

a. Maintenance personnel must be cleared to the highest level of data the AIS is accredited to process.

b. Maintenance personnel who do not access classified data during their maintenance operation should, nevertheless, be cleared for the highest level of data processed on the system. However, if this is not feasible, maintenance personnel will be monitored at all times during their maintenance operation by individuals with the technical expertise to detect unauthorized modifications.

c. Non-U.S. citizens will not perform maintenance on TS/SCI- and SIOP–ESI-accredited AIS or on AIS that process SAP information. If non-U.S. citizens are employed to maintain other AIS, such use will be addressed as a system vulnerability in the risk assessment, and appropriate countermeasures will be employed.

d. Any parts removed from an AIS operating in a sensitive compartmented information facility (SCIF) will be retained in the facility until approved for release by the local special security officer (SSO) in coordination with the ISSM or ISSO per AR 380–5, AR 380–28, and DCID 1/21.

Section IV
Physical Security

2–10. Security objectives and safeguards

a. A balanced AIS security program must include a firm physical security foundation with the following objectives:

(1) Safeguard personnel.

(2) Prevent unauthorized access to equipment, facilities, material, media, and documents.

(3) Safeguard against espionage, sabotage, damage, and theft.

(4) Reduce the exposure to threats that could cause a denial of service or unauthorized alteration of data.

b. Commanders and managers will protect AIS assets under their control through cost-effective physical security measures.

c. Facilities that house systems, computer rooms, network components (for example, routers or file servers), and related sensitive areas may be designated as restricted areas or mission essential vulnerable areas under AR 190–13. Facilities and systems so designated will be included in the installation physical security plan required by the same regulation. Periodic physical security inspection requirements are also contained in AR 190–13 and AR 190–51.

d. Facilities that house systems processing SCI material will be subject to the provisions in DCID 1/21.

e. Particular attention must be paid to the physical security of AIS that are not operated or otherwise attended continuously. An AIS that processes classified defense information must be properly declassified prior to being left unattended, unless it is secured in areas or containers approved for storage of classified material under AR 380–5.

f. The number and diversity of Army AIS (fixed and deployable systems) and installations make it impractical to establish universal, rigid physical security standards. However, adequate physical security at each installation is essential to achieving a secure data processing environment. Physical security standards must be based on an analysis of both wartime and peacetime mission criticality, sensitivity levels of the information processed, overall value of the information to the mission of the organization, the local criminal and intelligence threat, and the value of the automated equipment.

g. Physical security will be provided through an in-depth application of barriers and procedures, which may include continuous monitoring (human or electronic) of the protected area. Barriers and procedures include structural standards, key control, lighting, lock application, and inventory and accountability.

h. Physical access controls commensurate with the level of processing will be established to deter unauthorized entry into the facility and other critical areas (such as input or output area, programming, data preparation, and storage) that support or affect the overall operation.

i. Facilities housing AIS equipment will be of sufficient structural integrity to provide effective physical security at a reasonable cost. Trained physical security specialists will be consulted in all phases of selection, design, and modification of such facilities to provide expertise in physical security requirements.

2–11. Physical security standards for smaller computers and other automated information systems

a. Many AIS, including some file servers, clearly do not warrant the physical protection detailed in paragraphs 2–8 and 2–10 above. These include personal computers, workstations, notebook computers, and laptop computers, as well as other AIS where the computing environment is fully integrated into the work environment. Application of the above standards will depend on AIS size, complexity, manufacturer specifications, number of terminals, sensitivity of data, and environmental requirements. If the mainframe physical security requirements do not apply, the provisions in this paragraph will be followed.

b. Physical security requirements must be considered and selected based on the sensitivity and classification of data being protected, as well as assessed risk to the information and the risk of equipment theft. The physical security requirements must be examined to ensure protection of equipment is cost effective, that the impact on objectives is negligible, and that the level of risk is acceptable to the local commander.

c. All AIS must be protected, and physical security requirements must be carefully selected.

(1) An AIS with nonremovable media that processes classified information must be stored in an area or a container approved for safeguarding classified media per AR 380–5.

(2) An AIS with SBU information on nonremovable media should be in a locked office or building during non-duty hours or be otherwise secured to prevent loss or damage.

(3) When users leave their workstations or personal computers, they will log-off or lock the keyboard and screen until reauthentication.

(4) Workstations and personal computers should include a local“idle lockout/screen saver” feature that automatically locks the screen and keyboard after a specified period of no activity (that is, 3–5 minutes), requiring reauthentication before unlocking the system (for example, a password protected screen saver).

Section V
Procedural Security

2–12. Reporting and accountability

a. Procedural security measures can be cost-effective, since they usually involve a minimum financial expenditure while producing a higher corresponding level of security.

b. The procedures and techniques described herein apply to AIS operations as well as to software development, maintenance activities, and other support operations. Control of software during the development process is as important as control over the AIS in operation.

c. The procedural measures listed below will be an integral part of each AIS security program.

(1) Key duties will be clearly delineated and separated to reduce the risk of one individual adversely affecting the entire system

operation. Checks and balances will be established to detect deviations from assigned duties.

(2) The ISSO must report directly to the responsible manager of the AIS on security-related matters. The ISSM should be positioned organizationally to avoid having a vested interest in keeping the system operational at the expense of security.

(3) Proposed changes to the AIS configuration (to include changes to the software, facility, environmental support, or equipment interfaces) will be reported to the ISSO for a determination about the security implications of the change. If required by AR 381–14 (S), a TEMPEST Countermeasures Review will be conducted by or validated by a certified TEMPEST technical authority (CTTA).

(4) All AIS hardware, software, firmware, and documentation will be protected to prevent intentional or unintentional disclosure, destruction, or modification. This includes having appropriate physical, personnel, administrative, and configuration controls.

2–13. SCI policy

a. All AIS equipment used for processing, handling, and storing of SCI will be operated and secured in compliance with Defense Intelligence Agency Manual (DIAM) 50–4, NSA Manual 130–1, DCID 1/16, this regulation, or successor documents.

b. Prior to use, automated information systems located in a SCIF must be accredited under the provisions of this regulation, Defense Intelligence Agency Manual (DIAM) 50–4, or National Security Agency Manual (NSAM) 130–1.

c. All AIS processing SCI and classified collateral information will comply with the following requirements:

(1) Any removable magnetic media placed in an AIS with fixed media must be protected at the same classification level as the system. Fixed media include systems having memory retention capabilities such as internal memory retention devices or non-removable hard disks.

(2) Any removable magnetic media placed in an AIS without fixed media (for example, a diskless workstation in a client server environment) must be protected at the highest classification level of any media used simultaneously in the AIS.

(3) If the classification of removable media is more restrictive than the level for which the AIS is accredited under this regulation, the special security officer (SSO) must be notified of a security violation, and the AIS must be protected at the more restrictive level. Additionally, the AIS accreditation must be resubmitted to accommodate the more restrictive level unless the system is completely sanitized and there is no intent to process at the more restrictive level in the future.

(4) All fixed media systems processing SCI data must be stored in a GSA-approved container, or the SCIF must have authority for open storage of SCI material. If such authority is not granted in the facility accreditation, permission will be requested through command channels to HQDA (DCSINT).

d. Contractors utilizing AIS within a contractor SCIF that is intended to process or store SCI in support of Army SCI contractual efforts will refer to DIAM 50–5, DIAM 50–4, AR 381–14, or successor documents, and separate guidance provided from the Contractor Support Element, 716th MI Battalion, Fort Meade, MD 20755.

(1) Supporting contractor support detachments (CSDs) of the 902d MI Group may approve the entry of processing equipment into contractor SCI facilities (SCIFs). This approval does not constitute processing approval.

(2) Department of Defense (DD) Form 254 (Contract Security Classification Specifications) and other contractual documents will require appropriate TEMPEST countermeasures to be applied in the contract (see AR 381–14 (S)).

e. All equipment used to transmit, handle, or process SCI electronically (including communications, word processing and automated information systems equipment) must satisfy the requirements of AR 381–14 (S). Army activities processing SCI electronically will use AR 381–14 (S) for TEMPEST guidance. After consulting with the ISSM, SSOs may approve the entry of any processing equipment listed on the current Preferred Products List (PPL) or endorsed TEMPEST product list (ETPL) into a SCIF. Entry approval does not constitute processing approval.

f. Appendix F of this document contains guidance in declassifying, releasing, and shipping of media containing sensitive compartmented information.

2–14. Password control

a. User identification and password systems support the minimum requirements of accountability, access control, least privilege, and data integrity contained in paragraph 2–3*a* above. While not always appropriate for stand-alone small systems or for other systems operating in the dedicated mode, these mechanisms are often the most cost-effective and efficient method of achieving the minimum security requirements. Other techniques (for example, biometrics access control devices or smart cards) provide practical alternatives for use in conjunction with, or in place of, password systems.

b. The ISSO or designated representative is responsible for managing generation, issuance, and control of all passwords.

c. After creation, passwords will be handled and stored at the level of the most sensitive data contained in the system. In the case of multilevel security mode operations, passwords will be safeguarded according to the level of system access to which the user is authorized. Knowledge of individual passwords will be limited to a minimum number of persons, and passwords will not be shared. Passwords will be issued if the user has a confirmed authorization to access the system.

d. Methods of password distribution will be appropriate to the level of the data that they protect.

e. At the time of password issuance, individual users will be briefed on the following:

(1) Password classification and exclusiveness;

(2) Measures to safeguard classified and unclassified passwords;

(3) Prohibitions against disclosure to unauthorized personnel, even though they may be assigned to the same project and hold identical clearances; and

(4) The requirement to inform an ISSO or designated representative immediately of password disclosure or misuse or other potentially dangerous practices.

f. A password will be issued only once and will be retired when the time limit has expired or the user has been transferred to other duties, reassigned, retired, discharged, or otherwise separated from the duties or the function for which the password was required. The holder of a password is the only authorized user of that password. Without proper authority, personnel may not use another person's password or allow another person who does not have proper authority to use his or her password.

g. Passwords on classified systems will be changed at least quarterly. Passwords on nonsensitive and SBU will be changed semiannually.

h. Passwords will be inhibited, overprinted, or otherwise protected from unauthorized observation on terminals and video displays.

i. Passwords for AIS processing SCI/SIOP–ESI must be randomly generated with, as a minimum, eight character strings using the 36 alphabetic-numeric characters. Passwords for systems processing other classified or SBU information must be at least a eight character string using the 36 alphabetic-numeric characters and do not need to be randomly generated. At least two of the characters should be numeric.

Section VI
Personnel Security

2–15. Training and awareness programs

All individuals who are appointed as ISSPM, ISSMs, ISSOs, and systems administrators must complete an AIS security course of instruction equal to the duties assigned to them. All other personnel who manage, design, develop, maintain, or operate AIS will undergo a training and awareness program consisting of the following topics:

a. An initial security training and awareness briefing for AIS managers and users. This briefing can consist of training material governing ISS in general but must be tailored to the system the employee will be managing or using. The briefing will include the following:

(1) Threats, vulnerabilities, and risks associated with the system. Under this portion, specific information regarding measures to reduce the threat from malicious software will be provided, including prohibitions on loading unauthorized software, the need for frequent backup, and the requirement to report abnormal program behavior immediately.

(2) Information security objectives (that is, what is it that needs to be protected?).

(3) Responsibilities and accountability associated with system security.

(4) Information accessibility, handling, and storage considerations.

(5) Physical and environmental considerations that are necessary to protect the system.

(6) System data and access controls.

(7) Emergency and disaster plans.

(8) Authorized system configuration and associated configuration management requirements.

b. Periodic security training and awareness, which may include various combinations of the following:

(1) Self-paced or formal instruction.

(2) Security education bulletins.

(3) Security posters.

(4) Training films and tapes.

(5) Computer-aided instruction.

2–16. Personnel security standards

a. Personnel who require access to AIS processing classified defense information to fulfill their duties will possess a security clearance based on the appropriate personnel security investigation as delineated in AR 380–67.

b. Civilian, military, consultant, and contractor personnel meeting the requirements of an automated data processing (ADP) I, II, or III position (see AR 380–67) will successfully complete a security investigation as listed below. The investigation must be completed before the individual is permitted access to an AIS and is placed in an ADP position.

(1) ADP–I. Single Scope Background Investigation (SSBI).

(2) ADP–II. National Agency Check or National Agency Check with Inquiries.

(3) ADP–III. National Agency Check, Entrance National Agency Check, or National Agency Check with Inquiries.

c. Before users are granted access to any system, the system owner must determine if access requires a background check and the type of background check required per the level of ADP sensitivity and the ADP position requirements defined in paragraph b above.

d. All positions will be designated as Critical-Sensitive for ADP–I, Non-Critical Sensitive for ADP II, and Non-Sensitive for ADP III per AR 380–67, paragraph 3–101.

e. Criteria for occupying an ADP I, II, or III position are contained in AR 380–67, paragraph 2–200. Commanders or supervisors who become aware of adverse information, either through the formal security investigation or through other official sources, will follow the procedures in chapter 8 of AR 380–67, which may include suspension from duties. Suspensions or other more adverse actions will be based on the normal security clearance determination process contained in AR 380–67. The investigation must be successfully completed prior to assigning an individual to any ADP I or II duties.

f. Additional responsibilities for personnel managing, supervising, and performing ADP I, II, and III duties are found in AR 380–67, chapter 9.

2–17. Foreign national employees

a. Use of foreign national employees in positions that allow access to AIS is discouraged. However, when circumstances necessitate this practice, the requirements in this paragraph apply.

b. Army Regulation 380–67, paragraph 3–608, requires pre-employment checks of prospective foreign nationals who will not require access to classified information to perform their duties. Before employment, each foreign national must have a favorable National Agency Check or host country equivalent. If the foreign national is hired prior to the completion of the security check, the employment contract will state that retention in the position is contingent upon completion of a favorable security screening.

c. Foreign nationals will not be employed in positions that meet the definition of ADP I or II, unless specifically approved by officials listed in AR 380–67, appendix F, paragraph F–2.

d. Foreign nationals will not be employed in AIS positions which will afford access to classified defense information except when the foreign national meets the provisions for a limited access authorization (LAA) due to other special expertise. An LAA may be granted only under the provisions of AR 380–67 and only if there are no qualified U.S. personnel available. Access must be limited to that described in the approved LAA, and the foreign national must be supervised at all times by appropriately cleared U.S. personnel. The LAA must be reviewed annually to verify that it is still required as approved and has not evolved into a need for greater access. The LAAs will always be kept to the minimum, consistent with mission requirements, and will be terminated when no longer required.

Section VII
Automated Information System Media

2–18. Protection requirements

a. The AIS media consist of any substance or material on which information is represented or stored, used for either input or output to an AIS, or the media are an integral part of the AIS.

b. Users of classified media must protect the media in accordance with the procedures of AR 380–5 unless media is properly declassified or destroyed pursuant to this regulation or NSA regulations.

c. All toner cartridge assemblies used in laser printers that are connected to a collateral classified AIS will be considered to be unclassified after three blank pages have been printed. Cartridge assemblies used in printers connected to an AIS that processes SAP or SCI must be controlled per NSA policies as defined in National Security Telecommunications and Information Systems Security Agency Manual (NSTISSAM) COMPUSEC/2–90 and or DCI policies as defined in DCID 1/21.

2–19. Labeling and marking media

a. Personnel will mark and label all media that are not integral parts of the AIS according to the highest accreditation level of the system in which they were operated in accordance with AR 380–5. Personnel must label components with memory capabilities according to the highest accredited classification of the system when they remove the component for repair or exchange. Personnel will use Standard Form (SF) 706 (Top Secret), SF 707 (Secret), or SF 708 (Confidential) to mark non-paper collateral classified media. Personnel will affix two lables to SCI media, SF 712 (Classified SCI), and a completed SF 711 (Date Descriptor). The SF 711 will indicate the security classification of the data. The SF 712 is provided by the Defense Intelligence Agency, Application Division, Bolling Air Force Base, Washington, DC.

b. Personnel will use the label SF 710 (Unclassified) to label unclassified media that contain data representatives that cannot be read by the human eye when media are stored, transmitted, or otherwise intermingled with classified media.

c. Personnel will mark paper printouts from AIS in accordance with AR 380–5, chapter 4.

d. General requirements for accountability, receipting, transmission, and all other measures for classified material prescribed in AR 380–5 will apply to AIS media as appropriate to its classification.

e. Personnel will mark and label all compact disks (CDs) for AIS according to the highest classification level of the system in which they were operated. Personnel will mark the non-readable side of the CD with permanent ink to the case and the accreditation level of the system in which it was operated.

2–20. Clearing, purging, declassifying, and destroying media

a. Clearing of media means erasing or overwriting all information on the media without the totality and finality of purging. The clearing procedure is adequate when the media will remain within the facility; however, removable media must continue to be controlled at their prior classification or sensitivity level. Purging or sanitizing of media means to erase or overwrite, totally and unequivocally, all information stored on the media. Declassifying of media refers to the administrative action taken after it has been purged. Declassifying is required when the media must leave the facility under the control of uncleared personnel; for example, for maintenance operations.

b. The decision to declassify media will be made only after comparing the inherent risks (in the Magnetic Media Remanence Guide - Rainbow Series) with the financial or operational benefit of media declassification. For example, destruction of media is normally more appropriate than declassification and reuse, given the low cost of the media.

c. Media can be declassified only after purging. The appropriate ISSO must verify that the technique chosen for purging (or sanitizing) meets applicable requirements. Additionally, the ISSO must establish a method to periodically verify the results of the purging. As a minimum, a random sampling will be taken to verify each purge.

d. Degaussing must be accomplished using NSA-approved equipment from the Degausser Products List of the Information Systems Security Products and Services Catalogue. Information on degaussers is available through the information systems security management structure. Some listed products may be used only to degauss magnetic media that has coercivity no greater than 350 oersteds (also known as type I media), while others are approved for media with coercivity no greater than 750 oersteds (also known as type II media). Certain tape media have a coercivity greater than 750 oersteds (also known as type III media) and cannot, at this time, be completely degaussed. (See app F for more information.)

e. AR 380–5 governs destruction of most AIS media. Appendix F (of this document) and DCID 1/21 provides guidance on destruction of laser printer cartridges. A CD–ROM will be destroyed by scratching both surfaces with some abrasive substance to render the CD unreadable prior to breaking the CD into numerous pieces with some type of impact devices.

f. Storage media containing Sensitive Compartmented Information (SCI) will be handled as stated in appendix F of this document.

2–21. Non-removable storage media

a. Using an AIS with non-removable, non-volatile media for processing classified information is discouraged. Classified information may not be stored on such media except under one of the following conditions:

(1) The AIS is housed in an area approved under AR 380–5 for open storage at the highest classification level processed.

(2) The AIS can be secured when unattended in a storage container approved for the highest classification level of information processed.

(3) The AIS is continually controlled by individuals cleared for the highest level of material stored.

(4) The media are declassified according to this paragraph during all periods when they are not attended by properly cleared individuals.

b. If the conditions of paragraph *a* (above) are not met and the DAA elects to approve the use of non-removable, nonvolatile media on AIS processing classified information, specific countermeasures must be implemented to ensure that classified information is not written on such media. These countermeasures must be identified in the accreditation documentation. Administrative techniques, such as an SOP requiring users to write classified information only to removable media, are not sufficient to meet the requirements of this paragraph, due to the high possibility of user error and the possibility of systems or application software using the non-removable media for its files.

c. Appendix F of this document provides additional information concerning fixed storage media containing sensitive compartmented information.

Section VIII
Network Security

2–22. Two views of a network

a. The provisions of this regulation apply to networks, which are included in the definition of an AIS. However, for the purpose of applying these standards and identifying responsible officials, the following views of a network must be considered:

(1) The Interconnected Accredited AIS (IAA) view is one in which the network is treated as an interconnection of separately created, managed, and accredited AIS. An IAA consists of multiple systems that have been accredited to operate within a range of values and may include systems that do not fall under DOD directives.

(2) The Single Trusted System (STS) view is one in which the network is accredited as a single entity by one DAA. The STS view is normally appropriate for local area networks but can also be applicable to wide-area networks for which a single agency or official has responsibility.

b. The following security provisions are applicable to the IAA view network:

(1) Even though there are multiple individually accredited AIS, there should still be a single identified network DAA (for example, DISA has overall control and publishes security parameters for use of the Defense Data Network (DDN)). However, a central focal point cannot always be identified. In this latter case, each individual AIS DAA must establish procedures to protect the data contained in the AIS and to ensure that only authorized data are transmitted on the IAA network.

(2) The DAA of the individual AIS must specifically approve connection of the AIS to an IAA. This approval will be part of the AIS accreditation. It will be made only after assessing the additional risks involving the potential exposure of data within the larger community of AIS infrastructure.

(3) The DAA's approval will include a description of the classification and categories of information that can be sent over the IAA. Unless the AIS is accredited for multilevel operations and can reliably separate and label data, the AIS is assumed to be transmitting the highest level of data present on the system during network connection.

(4) The DAAs of the participating AIS and the DAA of the overall network (if one has been designated) will sign a Memorandum of Understanding (MOU). In those cases where standard procedures for connecting to the network have been defined by a DAA, those procedures, coupled with the approval of the DAA to connect, will serve as the MOU.

(5) Connections between accredited AIS must be consistent with the mode of operation, sensitivity level or range of levels, and any other restrictions imposed by the accredited AIS.

(6) Connections to unaccredited AIS (that is, from other agencies or non-governmental entities) are authorized, but only nonsensitive unclassified and SBU data may be transmitted to and from such AIS. Data that are SBU must be afforded the proper protection requirements (data confidentiality, data integrity, and data availability) to ensure compliance to paragraph 1–5*b* of this regulation.

(7) National Computer Security Center - Technical Guidance

(NCSC–TG) –005 contains additional restrictions that apply to connecting AIS to an IAA when the AIS is accredited in the multi-level or compartmented mode.

c. The following security provisions apply to the STS view of a network:

(1) The STS view of a network provides the greatest probability that security will be adequately addressed in a network, and it will be used in lieu of the IAA view whenever possible.

(2) Sensitivity category and mode of operation of the STS network will be determined as described in paragraph 2–2 above. Minimum requirements of paragraph 2–3 are fully applicable, including the minimum trusted class requirement when the network operates in other than the dedicated mode. Part I of the NCSC–TG–005 can be used to determine how to interpret DOD 5200.28–STD for an STS network. Additionally, part II describes three other security services (each with three sub-elements that must be addressed in the STS network accreditation):

(a) Communications integrity, including authentication capability, field integrity, and ability of the network to enforce non-repudiation of a message;

(b) Denial of service characteristics, including continuity of operations, protocol-based protection against denial of service, and adequacy of network management; and,

(c) Compromise protection, including data confidentiality, traffic flow confidentiality, and the ability to route transmissions selectively in the network.

(3) The security services described in paragraph (2) above can be addressed only in a subjective manner and may not be applicable or desirable in all situations. Nevertheless, ISSOs and network DAAs must consider each of them in defining their network security requirements and develop countermeasures for those services that are required but not present.

Section IX
Miscellaneous Provisions

2–23. Remote devices

a. Remote terminal devices must be secured consistent with the mode of operation and information that the remote terminal is authorized to access.

b. Remotely accessed computer systems and file servers must possess features to positively identify users and authenticate their identification before processing.

c. Physical safeguards will be implemented to ensure that only authorized persons use remote terminal equipment and that only authorized persons receive and remove sensitive information from the remote access areas. During periods when effective monitoring cannot be maintained, the doors to these terminal areas will be locked or the terminals otherwise secured, to prevent loss, damage, or unauthorized access.

d. An AIS with remote terminal access containing classified data will have a “time-out” protection feature that automatically disconnects the remote terminal from the computer after a predetermined period has passed without communication between the terminal and the computer. The system should make periodic checks to verify that the disconnect is still valid. The automatic disconnect must be preceded by a clearing of the remote terminal’s screen followed by the recording of an audit trail record for the System Administrator to use. The time period should not exceed 15 minutes but may vary depending on the sensitivity of the data, the frequency of use and location of the terminal, the strength of the audit mechanism, and other physical or procedural controls in place. The time-out feature is not required if the accreditation authority determines the AIS must remain active because it is being used as a communications device. However, physical security for the terminal will meet the requirements for storage of data at the highest level that could be received at the terminal.

e. Systems that process classified or SBU information will limit the number of user log-on attempts to three before denying access to that user. Users will not be re-instated until the ISSO or his designee has verified the reason for failed log-on attempts.

2–24. Employee-owned computers and off-site processing

a. Army Regulation 25–1, chapter 5, contains policy on approval to use employee-owned computers. If approved for use, employee-owned computers must also comply with all provisions of this regulation, including accreditation. Classified information will not be processed on employee-owned computers.

b. Army Regulation 25–1, chapter 5, also contains the policy for obtaining approval to process Government information at locations other than at the normal work site.

2–25. Tactical or Battlefield Automation Systems

a. The requirements of this regulation apply to Battlefield Automation Systems (BAS), to include all systems developed under the PEO/PM structure. When one or more of the minimum security requirements from paragraph 2–3 are impractical because of the function or design of the BAS (that is, it is not intended for, nor can it be converted to, a general purpose garrison environment), the generic accreditation will address this situation and will describe how that particular requirement is not applicable and does not present an unacceptable risk to the information.

b. Prior to deployment or fielding, BAS will be generically accredited in accordance with chapter 3.

c. Any BAS which also function as peacetime systems must fully comply with this regulation. Their accreditation must address operation in both garrison and deployed modes.

d. The following additional items must be considered in the security planning for BAS:

(1) Physical security objectives and safeguards (para 2–10) and physical security standards (para 2–13) must be employed to enhance security during transportation of BAS.

(2) Mechanisms must be available to render the BAS inoperable in case of imminent capture. Methods of purging (or sanitizing) classified AIS media (per para 2–21) and methods of destroying hard copy and AIS media (per AR 380–5) must be developed.

(3) For systems processing SCI or SIOP–ESI, the system architecture, security classification level processed, security safeguards, and intended use of BAS, deployable AIS, and networks must be included in the System Security Plan and Security Concept of Operations documents. The DAA (both generic and operational, as appropriate) may accredit the BAS to operate in-garrison, in-transit, and while deployed for exercises and operational missions.

2–26. Laptop, notebook, or portable automated information systems

a. Laptop/notebook computers or any other computers designed to allow periodic relocation must be accredited in accordance with chapter 3 of this regulation by the appropriate DAA. The DAA may accredit more than one computer on one document. The DAA will indicate on the accreditation document exactly where the computer may be taken and the kind of classified material that may be stored on the computer. Users of the portable computer must follow the accreditation instructions at all times, and users must possess a copy of the accreditation documentation at all times when the computer is removed from their regular place of work. Any media or other material produced by the computer must be handled and stored by users of computers in accordance with AR 380–5. If a computer contains a non-removable hard disk that stores classified material, the entire computer must be stored in an approved storage area at all times that the computer is not in the possession of the user. Users of portable computers must not enter SCIFs with the computer without the approval of the local special security officer.

b. If the accreditation document so provides, classified processing may be done on laptop or notebook computers if it occurs in normal work areas otherwise acceptable for the storage, preparation, or discussion of classified material. The accrediting authority may limit the classified processing to the user’s regular place of work or, in cases of compelling operational need, may include approved areas while at a Temporary Duty (travel) (TDY) location. In the latter case, the user will carry a copy of the accreditation statement while on TDY. Media or output products produced must be handled per this regulation and AR 380–5, including marking and storage standards.

c. If the computer configuration includes nonremovable hard disks that store classified material, the entire system must be stored in an area approved for storage of the highest classification of information the system is accredited to process when left unattended. The provisions of paragraph 2–22 above also apply to configurations that include non-removable media.

d. Accreditation for laptop or notebook computers generally must address processing in the user's normal work location and in the official travel location. If classified processing is included in the accreditation, TEMPEST (inspectable space) requirements must be addressed for the normal work location. When approval has been granted to process classified information at a temporary location for more than 90 days, a TEMPEST Countermeasures Review must be performed for that location per AR 381–14 (S).

e. Personnel will not be allowed to enter and exit sensitive compartmented information facilities with laptop/notebook or other portable computers unless approval has been granted by the local special security officer (SSO), after coordination with the site ISSO.

2–27. Automated information system security incidents

a. Any AIS security incidents will be investigated to determine their cause and the cost effective actions required to prevent reoccurrence. Suspected or actual incidents will be reported to the appropriate ISSO, who will notify the ISSM. Concurrently, the operator and ISSM will notify the Army Computer Response Team/ Coordination Center (ACERT) or its subordinate CERT infrastructure and request immediate technical assistance. The LIWA will notify HQ, CID; DISA/automated systems security incident support team (ASSIST); and ACCO INSCOM of actual penetrations of Army AIS. The ISSO or ISSM should also notify the supporting CID and INSCOM offices if an unauthorized person successfully penetrated the AIS. The two commands will coordinate to determine investigative jurisdiction, with CID taking the lead if there are no indications of foreign intelligence service (FIS) involvement. If FIS involvement is suspected or known, INSCOM will initiate a Subversion and Espionage Directed Against the Army (SAEDA) report per AR 381–12. The U.S. Army Intelligence and Security Command will notify the FBI if FIS involvement is known or strongly suspected. The CID will investigate fraud, extortion, theft, and other criminal acts involving Army AIS. If CID, INSCOM and the FBI rule out FIS or criminal activity and decline investigative jurisdiction, the reporting command or agency is authorized to initiate a preliminary inquiry per AR 380–5 or AR 15–6 to determine and fix the security vulnerabilities contributing to the security incident. The LIWA ACERT may request assistance from the DISA/ASSIST. Examples of the types of incidents that will be reported include but are not limited to the following:

(1) Known or suspected intrusions or attempted intrusions into classified and unclassified AIS by unauthorized users or by authorized users attempting unauthorized access.

(2) Unauthorized access to data, files, or menus by otherwise authorized users.

(3) Indications of an unauthorized user attempting to access the AIS, including unexplained attempts to log-on unsuccessfully from a remote terminal.

(4) Indications of unexplained modifications of files or unrequested "writes" to media.

(5) Unexplained output received at a terminal, such as receipt of unrequested information.

(6) Inconsistent or incomplete security markings on output with extraneous data included in the output, or failure to protect the output properly.

(7) Abnormal system response.

(8) Malicious software.

(9) Alerts by network intrusion detection (NID) systems installed to detect "hackers" and other unauthorized personnel attempting system penetration.

b. The ISSOs will review all incident reports and related documentation and, in cooperation with other security and investigative personnel, advise the ISSM and commander or manager having jurisdiction over the possible system penetration or security violation. The ISSM will ensure that all available audit trail information is maintained until the incident is resolved.

c. In those cases where AIS security incidents affect the supported user community, the ISSM must formally advise all users of the problem and the action taken or expected. The centralized incident reporting activity for the Army will, through the ISSM or ISSO, as appropriate, provide the user with guidance and instructions received from the CID or CI.

d. If the cause of the incident can be directly attributed to administrative error and be readily corrected then no further action is required. Otherwise the incident will be reported by the ISSO to the centralized incident reporting activity for the ACERT and to the appropriate ISSM. The initial notification will be within 24 hours and will include a brief statement containing the location affected, system, a description of the suspected or confirmed incident, action taken, and point of contact. The centralized reporting activity will provide further guidance on any reporting requirements.

e. In cases where vulnerabilities have been revealed, support is available from ACERT and DISA.

f. When the incident is also reportable as a generic technical vulnerability as described above, required reports to Army's centralized reporting activity may be consolidated and will cite both applicable portions of this regulation.

Chapter 3
Automated Information System Accreditation

3–1. Accreditation overview

a. This chapter outlines policies governing the security accreditation of Army AIS and networks. Basic goals include ensuring that accreditation efforts will be appropriate for the system being evaluated as well as cost-effective. Accreditation is based on the process of collecting and analyzing information pertaining to the security of an Army AIS.

b. The DAA will be identified for each AIS or for networks processing classified or SBU information. The DAA will ensure the following actions are accomplished:

(1) The requirements of this regulation and other applicable procedures dealing with ISS are followed.

(2) Accreditation statements issued by the DAA are based on the DAA's review and approval of the system security countermeasures employed.

(3) The countermeasures approved by the DAA in the Accreditation Statement are implemented and maintained.

(4) A program of recurring reviews exists for reaccrediting the AIS when significant changes to the system occur.

(5) The AIS or networks that they accredit do not process data with a sensitivity level beyond the scope of the accreditation.

(6) The security countermeasures selected and applied are sufficient and necessary to counteract the identified risk to the system and are cost-effective relative to other equally effective measures.

(7) Security requirements are incorporated in the planning for system expansion.

(8) A security education and awareness program is in place that meets the minimum requirements of this regulation.

(9) An ISSM or ISSO with adequate training to carry out the duties of this function is named for each AIS or network.

(10) A security plan is prepared and maintained in accordance with this regulation.

c. Accreditation is the DAA's formal declaration that an AIS or network is approved to operate as follows:

(1) In a particular security mode of operation and security classification level.

(2) With a prescribed set of minimum environmental, technical, and non-technical security countermeasures.

(3) Against a threat assessed by the supporting intelligence staff office.

(4) In a properly secured area in a clearly defined operational environment.

(5) Under stated short- and long-term goals.

(6) With stated interconnections to other AIS or networks.

(7) At an acceptable level of risk for which the accrediting authority has formally assumed responsibility.

d. Accreditation is the official management authorization to operate an AIS or network and is based, in part, on the formal certification of the degree to which a system meets a prescribed set of security requirements. The accreditation statement affixes security responsibility with the accrediting authority.

e. Accreditation addresses the system's perimeter, its boundary, and its relationship to other AIS and networks in a particular infrastructure. The perimeter surrounds the specified set of equipment and peripherals under the control of the DAA. The boundary encompasses what may be a much larger environment that includes, for example, remote users, dial-in users or global network users, access to other AIS that are not controlled by a single DAA. The boundary may encompass numerous systems, users, organizations, and networks that support a similar mission objective. The collection of all potential users of the AIS (that is, users within the system boundary) is used to determine the security mode of operation. Only AIS equipment and peripherals within the perimeter of the AIS must be specifically identified in the accreditation document. However, security requirements for AIS equipment or peripherals accessing the system from outside the AIS perimeter, not controlled by the DAA, will also be addressed in the accreditation.

f. Accreditation must address each operational environment of the AIS for both fixed and deployable configurations. For example, an AIS may operate at one sensitivity level or mode of operation in a standalone mode and connect to a global network with another mode or sensitivity level. The accreditation must clearly establish procedures for transition between the two environments. Multiple operational environments can result in multiple accreditation for a single AIS if different DAAs are involved. However, in the concept of the operations document, a single accreditation that addresses all variations is sufficient.

g. The AIS which provide remote access to a larger, clearly defined system do not require individual accreditation, but they must follow the security requirements of the larger system accreditation. When such AIS will be used to process data unrelated to the larger system, they must be accredited before processing the unrelated data.

h. There are two general categories of acceptable AIS accreditation within the Army: generic accreditation of centrally fielded AIS and operational accreditation of AIS that are procured or obtained locally. Centrally fielded systems will be accredited under the generic approach unless DISC4 approves an exception for unusual circumstances. In the latter case, developer preparation of a users security guide, security certification, and all other portions of paragraph 3–2 (except the actual accreditation statement) are still applicable.

3–2. Generic accreditation

a. Under the generic approach, systems fielded to multiple users are accredited as a single entity prior to fielding. While generic accreditations will lessen the administrative burden for the field users, local ISS officials must still ensure that AIS under their purview are operating under the terms of the generic accreditation.

b. The generic accreditation will be applied to AIS fielded under the PEO/PM structure. Additionally, generic accreditation are appropriate whenever a single office or agency is responsible for fielding an AIS to multiple Army users. The ISSO will integrate new AIS into the established architecture and ensure that the new AIS do not adversely affect previously certified and accredited AIS.

c. The generic accreditation will address the projected local operating and risk environment for the system. The using activities should not normally be required to take significant additional steps to accredit the system. If additional security measures are necessary for a particular operating environment, they will be added as a supplement to the generic accreditation by the using command. The following must be accomplished in support of a generic accreditation:

(1) Clearly define the environment in which the system is to operate at the beginning of concept development. This facilitates an orderly analysis of the threats to which the system will be exposed and the subsequent determination of the appropriate security requirements for the system. Environmental factors that influence the security requirements include the users and their level of clearance; source, frequency, and types of input or output; levels of classification of the data; communications requirements; and physical protection afforded the system.

(2) Establish and integrate security milestones into the life-cycle plan of the AIS. The AIS developer will ensure that users, data owners, system security officers, and accreditation authorities are involved in defining and implementing security requirements and that a security plan for meeting these requirements is prepared and implemented.

(3) Incorporate in procurement and acquisition documents applicable security requirements and requirements of DOD 5200.28–STD and its interpretations (the Rainbow Series) as they apply to the proposed mode of operation.

d. Identify the following during the initial stage of system design:

(1) The accreditation authority: the DAA will be designated before the system design process begins to ensure applicable security requirements are integrated into the proposed AIS.

(2) The ISSM for the system during pre-deployment: the pre-deployment ISSM ensures that the provisions of this regulation are met before system fielding. The pre-deployment ISSM will be distinct from the using activity ISSM who has purview over system security after the system is operational.

(3) The classification of information to be processed.

(4) The security mode of operation.

(5) The required minimum evaluation class from DOD 5200.28 STD (see app E).

e. The following pre-fielding milestones will be developed:

(1) *A definition of the security requirements of the system.* This will be based on the minimum evaluation class and on a detailed risk analysis that addresses all projected employment options for the system.

(2) *A plan to test and certify that the system meets the technical security requirements.* In addition to the technical security requirements, a plan to ensure that environmental and physical security requirements are satisfied must be prepared prior to fielding. This certification testing should be part of the overall testing of the system. The DAA will coordinate with ODISC4 for planning, conduct, and approval of certification testing. (For DODIIS Core Product testing, see para 3–9, below.) The test report is an integral part of the accreditation.

(3) *An accreditation document paragraph.* The accreditation document will be fielded with the system as either a separate entity or a distinct part of the system documentation. It will incorporate the technical certification with the nontechnical security measures and will address the items contained in the accreditation format at appendix D.

(4) *A security SOP for users, operators, and ISSOs.* The security SOP will be fielded with the system as either a separate entity or a distinct section of the system's operating manuals. This SOP will identify all required security measures that must be enforced to operate the system at the level of classification and in the mode of operation for which it is accredited. It will incorporate all the countermeasures appropriate for the system and will address, as a minimum, the physical, personnel, hardware, software, communications, procedural, and emissions security countermeasures upon which the accreditation is based.

(5) *A security classification guide.* These security classification

guides (SCGs) will be fielded either as a separate entity or as a distinct part of the system's documentation when the system will process classified information. This will conform with the headquarters classification guide and is highly important for systems supporting a tactical force.

f. The generic accreditation documentation will be forwarded to the ISSPM of each Army MACOM and each major installation or activity ISSM receiving the system following DAA approval. The MACOM ISSPM, together with the command information manager and command functional user representative, will either accept the generic accreditation or prescribe additional measures or procedures to meet the needs of a unique operating environment. Such additional measures will be appended to the generic accreditation to constitute the system accreditation in that MACOM.

g. The AIS subject to generic accreditation will not be fielded or operated in a MACOM until the cognizant ISSPM has granted an approval to operate on behalf of the MACOM commander.

3–3. Operational accreditation

Operational accreditation is applicable to all AIS that have not been accredited by a generic accreditation. Operational accreditation is also required for AIS covered by a generic accreditation if the AIS operates beyond the security bounds of the generic accreditation. Operational accreditation may apply to the following areas:

a. A single AIS.

b. A grouping of more than one AIS sharing the following characteristics:

(1) The same DAA.

(2) Common risks and countermeasures to combat these risks, as determined by the risk management process.

(3) Common data sensitivity. All AIS with differing data sensitivity may be grouped in a single accreditation provided that paragraphs *a* and *b* above apply and that the accreditation documentation clearly segregates the different levels and the security measures applicable to each level.

3–4. Certification

a. Certification is a technical evaluation of the effectiveness of AIS security features and supports the accreditation decision. Certification verifies that the AIS security functions are correctly implemented and sufficient to support the mode of operation and the security policy for the system in an intended operational environment.

b. The DISC4 will coordinate with technical personnel who will conduct a certification test under a certification plan to determine if an unclassified, SBU, or collateral system adequately meets prescribed security requirements. Commander, INSCOM, will coordinate with technical personnel for certification of SCI systems.

c. Certification primarily addresses software, hardware, and firmware security measures. It must also consider procedural, physical, personnel, and emissions security to the extent that these measures are employed to enforce security policy.

d. Using products or systems listed in the NSA Information Systems Security Products and Services Catalogue will not negate the requirement for certification. However their use can greatly reduce the testing required for certification approval. In many cases, using NSA-approved products can reduce the certification effort to simply establishing that the product is installed and implemented according to the specifications. Since only a limited number of NSA-approved products are available that can satisfy user's requirements, other COTS and GOTS products should be integrated into the AIS. Certification testing of COTS and GOTS products must be performed to ensure that the infrastructure security posture is maintained per DOD 5200.STD, TCB C2 level of compliance.

e. Certification is a key element of generic accreditation. The security certification testing will be performed as part of the overall system testing. However, security-relevant test objectives will be identified as separate events. Where practical, individuals who complete the certification should be independent from the developer's staff.

f. The DAA, or a person appointed by the DAA, approves the results of the certification. For generic accreditation, the certification testing and approval must be a separate, distinct event in the accreditation process.

g. For operational accreditation, the ISSM or ISSO preparing the accreditation will supervise security certification.

h. The extent of the certification effort will vary with the security mode of operation of the system as follows:

(1) *Dedicated security mode.* The certification will focus on the physical, procedural, and personnel security measures that ensure that all users have the appropriate clearance, access approval, and need-to-know for all data on the system. The certification effort will not be extensive, since the system is not required to separate users and data with technical security measures.

(2) *Systems high and compartmented security mode.* The certification will cover the same factors as the dedicated mode. It will also establish that the hardware and software reliably separate users from any data for which they do not have a "need-to-know" or for which they do not have formal access approval.

(3) *Multilevel security mode.* The certification will address the same factors as (1) and (2), above. It will also assure that the system software and hardware can reliably separate users from data on the system for which they are not properly cleared.

3–5. The accreditation process

a. The time and manpower expended in the accreditation process must be proportional to the system size, criticality, mode of operation, data sensitivity, and number of users. The process may be significantly streamlined if the accreditation addresses small computers or other AIS operating in the dedicated mode. Appendix D contains the security plan format, which is the basis for the accreditation documentation. The depth of treatment for each element of the security plan should vary with the factors discussed below.

b. The accreditation process that leads to either generic or operational accreditation involves the following steps:

(1) Develop a security plan. Refine the plan throughout the accreditation process.

(2) Determine accreditation goals and objectives. Include a review and validation of the need for the subject operations.

(3) Define the proposed AIS operations. Define the key security features forming the basis of the accreditation and identify the security mode of operation.

(4) Conduct a risk management review to identify risks and countermeasures (chap 5).

(5) Select the security countermeasures required by the risk management review.

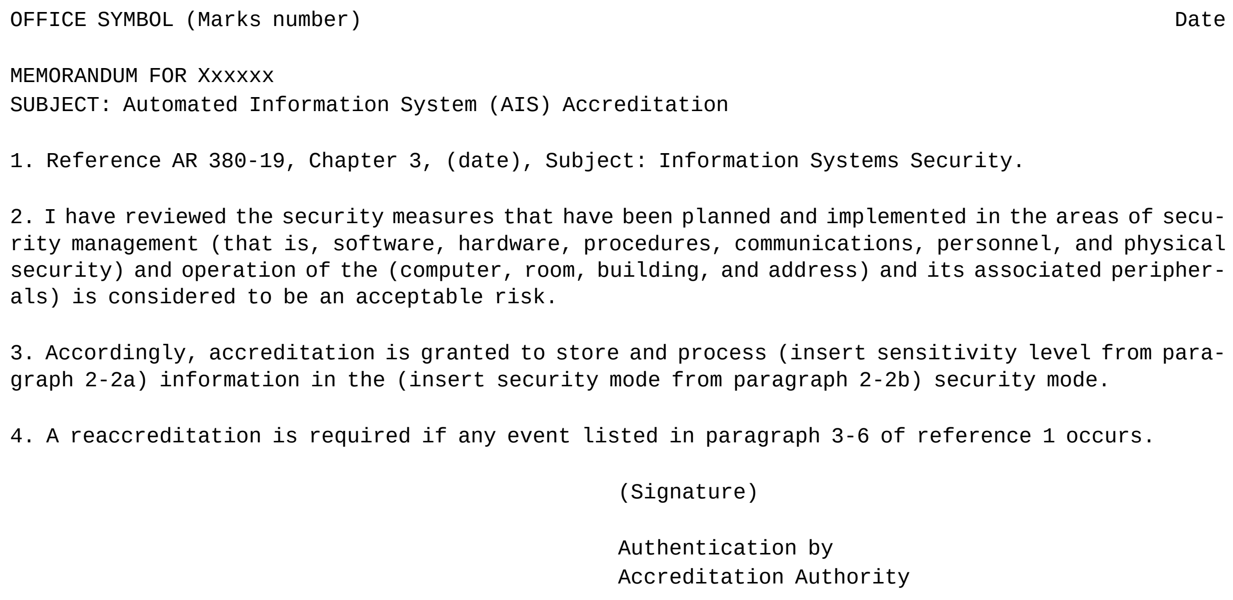
(6) Employ a Certification Plan to establish that the AIS performs the security functions that support the mode of operation and security policy for the system.

(7) Develop a security guide to provide security instructions for AIS users, operators, and the ISSO.

(8) Modify the security plan as appropriate, add relative attachments, and forward the plan to the DAA for approval (see fig 3–1 for an example of the format of an accreditation approval statement).

c. Accreditation documentation describes the system in detail. The documentation must be protected to the degree that its compromise would jeopardize the security of the information contained in the system, since it reveals system vulnerabilities. The documentation will be handled as stated in AR 25–55. Accreditation documents should be written so they do not reveal vulnerabilities requiring the documents to be classified higher than Secret.

d. Documentation will be forwarded to the accreditation authority in sufficient time to be acted upon before operation of the system or the expiration of any existing accreditation.



OFFICE SYMBOL (Marks number) Date

MEMORANDUM FOR Xxxxxx
SUBJECT: Automated Information System (AIS) Accreditation

1. Reference AR 380-19, Chapter 3, (date), Subject: Information Systems Security.

2. I have reviewed the security measures that have been planned and implemented in the areas of security management (that is, software, hardware, procedures, communications, personnel, and physical security) and operation of the (computer, room, building, and address) and its associated peripherals) is considered to be an acceptable risk.

3. Accordingly, accreditation is granted to store and process (insert sensitivity level from paragraph 2-2a) information in the (insert security mode from paragraph 2-2b) security mode.

4. A reaccreditation is required if any event listed in paragraph 3-6 of reference 1 occurs.

(Signature)

Authentication by
Accreditation Authority

Figure 3-1. Example of the format of an accreditation approval statement

3–6. Reaccreditation

a. All AIS accredited under this regulation will be reaccredited within 3 months following any event below:

(1) Addition or replacement of a major component or a significant part of a major system.

(2) A change in classification level of information processed.

(3) A change in security mode of operation.

(4) A significant change to the operating system or executive software.

(5) A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation.

(6) A significant change to the physical structure housing the AIS that could affect the physical security described in the accreditation.

(7) The passage of 3 years since the effective date of the existing accreditation.

(8) A significant change to the threat that could impact Army systems.

(9) A significant change to the availability of safeguards.

(10) A significant change to the user population.

b. Reaccreditation will include the same steps accomplished for the original accreditation; however, those portions of the documentation that are still valid need not be updated.

c. Reaccreditation of AIS and networks that have been included in an infrastructure under the site-based accreditation (SBA) concept (para 3–11 below) is not required. The AIS and networks will be maintained under the configuration management requirements and compliance validation techniques provided in the SBA concept.

3–7. Accreditation records

A copy of the AIS accreditation or re-accreditation documentation will be maintained with the system and should be retained by the accreditation authority or the ISSM.

a. Copies of accreditation documentation to support site-based accreditation or systems processing SCI must be provided to the designated accreditation authority.

b. Copies of generic accreditation documentation must be maintained by the systems developers.

3–8. Designated approving authorities

a. The DAA will be appointed for operational accreditation, as follows:

(1) The following individuals are accreditation officials for SCI and SIOP–ESI systems:

(a) Dedicated SCI with no network connections. The MACOM commanders are the accreditation authorities for systems that process SCI and operate in the dedicated mode, provided these systems do not include external connections. General officers or a senior intelligence officer (SIO) authorized to authenticate correspondence for a MACOM commander may sign accreditation statements. A copy of each accreditation statement will be furnished to Commander, INSCOM (IAFM–TA), 8825 Beulah Street, Fort Belvoir, VA 22060–5246. The DCSINT is the accreditation authority for SCI systems not under the purview of a MACOM commander.

(b) Systems high SCI with no network connections. Systems high SCI with no network connections can be accredited by the MACOM. The DCSINT is the accreditation authority for systems that process SCI in the systems high security mode with connection to external networks.

(c) Compartmented/multilevel or network connection SCI. The Director, DIA, is the accreditation authority for all systems that process SCI not covered by (*a*) or (*b*) above. The Director, NSA, is the DAA for cryptologic systems under this mode of operation.

(d) SIOP–ESI. The Director, Joint Staff, is the accreditation authority for systems processing SIOP–ESI data. Requests for accreditation will be prepared per MJCS 75–87 and forwarded through the Deputy Chief of Staff for Intelligence (DAMI–IM), 1000 Army Pentagon, Washington, DC 20310–1000.

(2) MACOM commanders and the Administrative Assistant to the Secretary of the Army (acting as the HQDA MACOM) are the accreditation authorities for Top Secret collateral systems operating in the dedicated, systems high, or compartmented security mode. The MACOM commanders and the Administrative Assistant to the Secretary of the Army may further delegate, in writing, accreditation authority to general officers, a MACOM SIO, or to Senior Executive Service personnel within their commands or agencies. Such delegation may be by name or by established position titles.

(3) The MACOM commanders and the Administrative Assistant to the Secretary of the Army are the accreditation authorities for

Secret/Confidential systems operating in the dedicated, systems high, or compartmented security mode. The MACOM commanders (and the Secretary of the Army's Administrative Assistant) may further delegate, in writing, the accreditation authority to personnel at the minimum rank of colonel, GM–15, or GS–15 and who are occupying a position of command or of principal staff officer at an installation or general officer command. Such delegation may be by name or by established position titles.

(4) The MACOM commanders and the Administrative Assistant to the Secretary of the Army are the accreditation authorities for SBU systems operating in the dedicated or system high mode of operation. Additionally, MACOM commanders and the AA to the Secretary of the Army may delegate, in writing, accreditation authority to other personnel who are in the minimum rank of lieutenant colonel, GM–14, or GS–14.

b. The DAAs will be appointed for generic accreditation as follows:

(1) The Director, DIA, is the DAA for systems processing SCI that meet the following criteria:

(a) Operate or are planned to operate in the compartmented or multilevel security mode or that require connection to an external network, regardless of security mode.

(b) Have received special approval from DIA for a generic accreditation. This approval will apply only to systems being fielded in identical configurations at a large number of sites. The DIA may require additional measures such as configuration control.

(2) The DCSINT is the DAA for SCI systems not covered by (*a*) and (*b*) above.

(3) The DISC4 is the DAA for Top Secret and below AIS in the multilevel security mode.

(4) The applicable PEO, with concurrence from DISC4, is the DAA for systems in the dedicated, systems high, or compartmented security mode. When a generic accreditation is appropriate and the AIS is not being fielded through the PEO structure, a general officer or a member of the Senior Executive Service who has responsibility for fielding the system may be appointed as the DAA with concurrence from DISC4.

c. If a generic accreditation is appropriate and the DAA is not readily apparent from the above guidance, DISC4 should be contacted for assistance to determine the DAA.

d. Accreditation of the Signal Intelligence (SIGINT) system is the responsibility of the Director, NSA.

3–9. Accreditation of sensitive compartmented information (sci) systems

a. The AIS or networks that process noncryptographic SCI data are subject to this regulation and DIAM 50–4 and, for contractor operations, DIAM 50–5 or their successors.

b. Accreditation by a DAA within the Department of the Army will be prepared and processed under this regulation. Documentation will be forwarded through command channels to the appropriate DAA. Accreditation documentation for systems processing SCI will include the written concurrence of the local supporting SSO and a statement of hostile threat from the local counterintelligence support activity.

c. Accreditation for all SCI systems with DIA as the accreditation authority will be prepared and processed in accordance with DIAMs 50–4 and 50–5 or their successor(s).

d. Defense Intelligence Agency Manual 50–4 provides guidance for establishing accredited sites. When AIS support a particular mission and are connected via networks, an infrastructure has been created that can be accredited as a site. This concept accommodates integration of all types of AIS and networks into a single accreditation document after certification and allows those systems to operate in different security modes of operation at all classification levels. The site infrastructure is not limited to a particular geographic location. The site is focused on mission responsibilities and command structures created by the network capabilities and unique requirements of various MACOM missions. A site may include non-SCI systems that directly and indirectly support the common mission of the site or that do not support the common mission of the site but are geographically located within the site. Once site boundaries have been established, a request for approval must be submitted to DCSINT prior to designating a site and certifying the systems within the site. The request must define the physical locations and inter-connectivity of the AIS and networks. Documentation for sites certified and accredited under the site concept will be maintained through the configuration management process and security compliance reviews. The ISSM will integrate new AIS into the established site baseline and ensure that they do not adversely affect previously certified and accredited AIS.

e. Integration of DODIIS Core Products is considered a form of generic accreditation. The DODIIS Core Product program officer is responsible for Core Products design, test, and evaluation.

3–10. Interim approval to operate before accreditation

A DAA may grant an interim approval to operate for a 90–180 day period before a generic or an operational accreditation is issued, provided the following conditions are satisfied:

a. A security survey has been performed and measures to prevent compromise, loss, misuse, or unauthorized alteration of data are deemed adequate. Some limitations on operations may be necessary during the period of interim approval.

b. A security plan has been developed and procedures, manuals, or SOPs are provided to instruct the users on secure AIS operations.

c. Applicable COMSEC (chap 4) and TEMPEST (AR 381–14) requirements have been met.

d. A test schedule is established and agreed to by the DAA.

e. An interim approval to operate (IATO) may be granted to support a specific date or event (such as an exercise or awaiting Site Based Accreditation).

3–11. Site-based accreditation

a. Under the system-based approach, the certification and accreditation focus may include a single system or network (as in the case of a complex, newly deployed system) or it may include smaller groupings of equipment as listed below:

(1) A LAN can be accredited as a single unit. Individual personal computers and work stations on a LAN need not be accredited individually.

(2) Groups of stand-alone personal computer systems, work stations, and office automation systems located in the same general area and performing the same general functions may be accredited as a single unit.

b. Under a site-based approach, the entire site as defined and documented may be certified and accredited as a unit if the individual AIS and components have been appropriately certified or accredited by a DAA. A site boundary is not limited to a specific geographic location and more than one site may be established at a single location (for example, Fort Bragg, NC, has five sites). A site may contain one or more systems and may also contain systems previously accredited by another DAA (for example, CIA, NSA, other MACOM commanders, or their representatives).

c. All DODIIS AIS and networks processing SCI for which DIA is the DAA will be certified and accredited using the site-based accreditation methodology detailed in DIAM 50–4. Specific guidance for establishing DODIIS COMPUSEC sites is provided in DIAM 50–4 and its three supplemental documents:

(1) Site Information System Security Officers (SITE ISSO) Handbook.

(2) Developers Guide for Building a Certifiable and Accreditable System.

(3) A Certifier's Guide.

d. When practical, the Army will establish sites composed of nonsensitive, SBU, collateral, and SCI systems.

e. The ODCSINT Intelligence Information Management Directorate (DAMI–IM), in conjunction with the accrediting authority, cognizant ISSPM, and site security personnel, will determine whether a system or site-based approach will be applied to any given location.

This determination will be based on several factors, including but not limited to the following site criteria:

(1) Organizational structure and relative size.

(2) AIS/network architecture density and complexity.

(3) ISSM staff capabilities.

(4) Commonality or uniqueness of AIS/network components.

(5) Anticipated near-term and future AIS/network modifications.

f. The following actions are required to establish a site:

(1) The ISSM and ISSO, in conjunction with the appropriate commander, will establish a Configuration Management/Control Board to ensure that AIS and networks included in the Site baseline can be securely maintained. The Configuration Management/Control Board will consist of information management, acquisition, operations, security, and user management personnel and ISS personnel.

(2) New SCI systems integrated into the site baseline will meet the certification requirements of the DIAM 50–4.

(3) The site may include stand-alone systems and networked systems that directly and indirectly support an organization's mission.

(4) Site boundaries may include AIS and networks not geographically located at the site if those systems are accessible via accredited network.

g. The AIS, guard devices, or networks intended to operate in the compartmented or multilevel security mode will be given the highest priority for certification and accreditation due to the increased risk associated with their operation.

h. The AISs and networks must be certified and/or accredited on an individual basis to determine whether they operate at an acceptable level of risk under both the system and site-based approach.

Chapter 4 Communications Security

4–1. Overview

Communication security policies establish requirements designed to deny unauthorized persons access to classified or SBU information during electrical transmission from sender to the receiver. They also establish requirements designed to prevent the derivation of valuable information from other aspects of communications (for example, traffic flow and message analysis) and to enhance the authentication of communications.

a. Communications security techniques will be applied to the extent necessary to deny information to unauthorized personnel and to effectively defend against interception, traffic analysis, and imitative deception.

b. The objectives of COMSEC will be an integral part of program planning for all telecommunications systems (including those integral to weapons systems and weapons support systems) and will be addressed throughout a system's life cycle. Systems planning shall include threat analysis and vulnerability assessments to support operational requirements and to establish resource allocation priorities and satisfy requirements for countermeasures.

c. Only approved cryptographic systems will be used within the Army. Approved cryptographic systems include—

(1) Government-developed and -produced systems (electronic, automanual, or manual).

(2) Government developed cryptographic equipment, produced commercially under the NSA-authorized vendor program.

(3) Commercially developed and produced cryptographic equipment using an algorithm approved by NSA.

d. Commercially developed equipment, using the data encryption standard (DES) or other commercially developed algorithm will not be used to protect classified information.

e. Systems will be designed and deployed using embedded cryptography to the maximum extent possible. When embedded cryptographic equipment is not employed, off-line electronic, automanual, or manual systems will be used to provide the required security, if the transmission is not otherwise protected.

f. Army system COMSEC requirements will emphasize small, reliable, lightweight, low-powered equipment that is unclassified when not keyed and will be achieved with no increase in the frequency band width required by the equipment being supported. Requirements must address interoperability for both routine and contingency operations.

g. Only keying material produced by NSA or generated by NSA approved key generators will be used to key cryptographic systems which protect classified or SBU information.

h. Maximum use will be made of electronic key generation as well as remote electronic keying and re-keying of cryptographic systems with that capability.

i. Classified and SBU communications between Army activities and contractors will be protected per this regulation. Procedures for contractors to procure the necessary equipment will be published by DISC4.

j. Authentication methods will be used to defend against imitative communications deception and to authenticate stations, transmissions, and communicators. The authentication process may be embedded in the communications equipment.

k. Safeguarding and controlling COMSEC material, including CCI, is governed by AR 380–40 and DA Pam 25–380–2.

l. Notification procedures, per AR 380–53, will be established to ensure that all users of official DOD systems within the Army understand that their use of DOD systems constitutes consent to security monitoring. The following banner will be included as part of the log-on screens on all computer systems:

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 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.

4–2. Protection of transmitted information

Classified and SBU information will be transmitted only by secure means. When information transits an area not under access controls as stringent as required for that classification of the information, it will be secured by encryption or a protected distribution system. Fiber optic lines can be adequately protected by Intrusion Detection Optical Communications systems approved by NSA and listed in the NSA Information Systems Security Products and Services Catalogue.

4–3. Protection of Sensitive but Unclassified Information

a. The security safeguards applied to SBU information during transmission will be consistent with the need for protection against disclosure, loss, misuse, alteration, destruction, or non-availability.

b. Sensitive but Unclassified information as described in paragraph 1–5*b* will be protected in transmission by an NSA approved technique unless a waiver is granted under procedures established by DISC4.

c. NSA-approved techniques, which may be used separately or in various combinations, to protect the transmission of SBU, are listed below:

(1) *Encryption.* A number of cryptographic products are acceptable for this purpose and are listed in NSA Information Systems Security Products and Services Catalogue.

(a) Type I products. These products may be used to protect both classified and SBU defense information.

(b) Type II products. These products may be used to protect only SBU information; they are handled as an Endorsed for Unclassified Cryptographic Item (EUCI). A FORTEZZA card is an exception to this policy when used in“FORTEZZA for classified applications.”

(c) Data encryption standard equipment. Unclassified cryptographic equipment employing the DES algorithm, which meets the requirements of Federal Standard 1027, may be used to protect only the transmission of unclassified information.

(d) Commercial equipment. As other equipment is developed and available, when approved by NSA (for example, RSA), it can be used to protect SBU information.

(2) *Unencrypted cable circuits.* Although encryption is the preferred protection, unencrypted cable circuits of copper or fiber optics may be used. The degree of protection provided will depend on the type of cable used. The cable least vulnerable to exploitation is fiber optic cable, followed by copper coaxial cable and copper strand cable. Cable protection can be enhanced by burying the cable underground or in walls or floors and providing access controls for entry to cable vaults, rooms, and switching centers. Unencrypted cable circuits can be employed to transmit SBU information under the following two conditions:

(a) The cables are used only within the geographic boundaries of the United States or within areas totally within U.S. control overseas.

(b) Adequate measures are implemented such that circuits are maintained on cable and not converted to unencrypted radio transmission.

(3) *Protected services.* Commercial telecommunications companies offer services that are endorsed to protect the transmission of unclassified information. The companies authorized to offer such services are listed in NSA Information Systems Security Products and Services Catalogue.

4–4. Radio systems

a. All voice or data military radio systems used for transmitting classified or SBU information will be secured or securable by an approved cryptographic system. Military radios are those radios built or adopted for use as standard military communications systems with a type classification or military nomenclature.

b. Electronic, automanual, or manual cryptosystems will be used to provide the needed security for existing radio systems that do not have embedded or electronic cryptosystems. However, all future procurements must comply with 4–3*c* above.

c. Commercial non-encrypted radio systems will not be used in support of command and control functions.

d. Excluded from the requirements of paragraphs *a* and *b*, above, are—

(1) Radios that only relay encrypted information.

(2) Commercial systems purchased or obtained to fulfill an operational function.

(3) Radios used for public safety communications with civil agencies or to communicate on civil aviation channels. This exclusion does not apply to communications dealing with aviation combat operations.

4–5. Protected distribution systems

a. Communications circuits can be protected by appropriate physical, acoustical, electrical, or electromagnetic safeguards such that classified data can be transmitted on these lines in clear text. These circuits must be formally approved as a protected distribution system (PDS).

b. A PDS will be used only if cost-effective and sufficiently controlled to prevent covert penetration and interception.

c. The AIS that include a PDS to transmit data will not be accredited to operate until the PDS has been approved. The PDS approval will be cited in the COMSEC portion of the accreditation packet and a copy of the approval will be attached.

d. A PDS must be constructed according to criteria published by HQDA DISC4.

e. A PDS may not be required if fiber optic cable is installed in a controlled environment and if the system design is approved by the DAA prior to installation.

4–6. Approval of protected distribution systems

a. Authority to approve a PDS for the clear text transmission of classified information within fixed plant and garrison installations is delegated as follows:

(1) Principal HQDA officials for activities under their staff supervision, direction, or control.

(2) Commanders of MACOMs or their designees at MACOM level, for their organic activities.

b. Requests for approval of a PDS to transmit top secret information must include an evaluation by the appropriate support element. Approval authorities may request technical assistance from INSCOM, 902nd MI Group, Fort Meade, MD 20755, in applying security criteria and processing the approval action for other PDS.

c. Commanders of battalion and higher echelons may approve circuits for clear text electrical transmission of Secret and Confidential information in tactical environments. Under combat conditions, commanders may delegate this authority to the company level. Tactical PDS will not be approved for clear text transmission of Top Secret information.

d. Once a PDS is approved, no changes in installation, additions, or use may be made until approval for such changes has been granted by the approval authority.

e. Requests to approve a PDS will be submitted through channels to the appropriate approval authority. Requests will be classified at least confidential and will contain the following information:

(1) Full identification and location of the requesting organization.

(2) A statement of the classification of information to be transmitted on the PDS.

(3) A copy of the building floor plan (or a diagram of the field area as appropriate) designating the following:

(a) Proposed cable route and location of subscriber sets, distribution frames, junction boxes, and any other components associated with the circuit.

(b) Other wiring along the PDS route.

(4) Description of the cable installation (for example, 24 pairs of shielded cable in rigid steel conduit, 6 pairs of shielded cable in floor, or fiber optic cable). Indicate the cable length.

(5) Description and nomenclature of terminal and subscriber equipment to be used.

(6) Clearance of individuals having access to the circuit.

(7) Type of guards (for example, U.S. military, U.S. civilian, foreign civilian) and their security clearance or access authorization status.

(8) Description of access control and surveillance of uncleared personnel who may be allowed entry into the area housing any part of the PDS.

(9) Identification of the power source to be used for the PDS and a statement of the distance to the nearest point where undetected tampering would be possible.

(10) A justification for using the proposed PDS.

(11) A statement concerning any deviations from the established PDS criteria, and an evaluation of their security implications.

(12) A copy of the security evaluation for PDS used with Top Secret information.

Chapter 5
Risk Management

5–1. Risk management overview

a. The most effective protection for AIS handling classified or SBU information is through a risk management program. The objective of risk management is to achieve the most effective safeguards against deliberate or inadvertent activities as listed below:

(1) Unauthorized disclosure of information.

(2) Denial of service or use and running in a degraded mode.

(3) Unauthorized manipulation of information.

(4) Unauthorized use.

b. Risk management of information systems is the process of identifying, measuring, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. The potential cost for broadly applied, marginally effective security features is enormous and underlines the need for effective risk management. Its application assists in optimizing the security return for each dollar invested.

c. There are three basic choices in risk management:

(1) *Risk avoidance.* This choice is the most costly and should not be considered, since it requires the implementation of exorbitant countermeasures to nullify the risk and to protect information.

(2) *Risk reduction and residual risk acceptance.* This choice supports applying cost effective security measures to AIS operations. The amount of risk that remains after the selection of a safeguard or countermeasure is known as residual risk.

(3) *Total risk acceptance.* While providing the least costly alternative at the onset, this choice may cost significantly more in the long run. Failure to implement security safeguards on an AIS leaves its vulnerabilities open to exploitation by the local threats. In an operational combat environment, however, this level of risk may be acceptable to the combat commander in the short-term.

5–2. Risk management program

a. An effective risk management program entails a four-phased evaluation effort:

(1) *Phase 1.* Risk analysis of resources, controls, vulnerabilities, and threats.

(2) *Phase 2.* Management decision to implement security countermeasures and to accept residual risk.

(3) *Phase 3.* Implementation of countermeasures.

(4) *Phase 4.* Periodic review of the risk management program.

b. The areas of software, hardware, procedures, communications, emanations, personnel (the highest risk), and physical security should be included in the risk analysis. Whenever possible, specialists or risk management software will be used to enhance the process.

c. Risk analysis involves estimating or determining loss potential that exists as the results of threats and vulnerabilities matching one another and causing some form of impact on the system. Using mathematical tools and statistical analysis techniques to determine the overall risk of operating a particular AIS or network would seem to be a logical methodology to employ. However, experience shows that attempts to develop absolute models, performance simulators, or descriptive algorithms have been, at best, only marginally successful. These techniques should not be employed except when their value has been established. In many cases, qualitative or subjective techniques will be more applicable to risk assessments performed for AIS.

5–3. Risk analysis

a. Areas of analysis. Risk is determined from the analysis of vulnerabilities, threats, security requirements, and available safeguards for AIS assets. After the analysis is complete and the chosen safeguards are in place, a security posture statement and recommendations to the DAA are written. Many automated tools are available to perform the risk analysis. These tools can reduce the manpower required to perform a risk analysis. The steps below provide a brief summary of the entire risk analysis process.

b. Resource identification. The cornerstone of any risk analysis depends on accurate identification of assets requiring protection.

c. Vulnerabilities identification. System vulnerabilities are weaknesses in design, system security procedures, implementation, and internal controls that could be exploited by authorized or unauthorized users. Vulnerabilities identified either by inspection or notification and which are not corrected must be identified in all future risk assessments (for example, reports of The Inspector General, provost marshal, management review teams, evaluation teams, or OPSEC evaluations).

d. Threat identification. Threat identification must account for both known and reliably projected threats. A threat may be defined as an event or method that can potentially compromise the integrity, availability, or confidentiality of automated information systems. Threats include but are not limited to the following items:

(1) *Foreign intelligence services, which may recruit authorized users or employ unauthorized users to penetrate the system's safeguards.* The Defense information infrastructure and Army systems that contain research and development, new technology, economic, and military operations data are of great interest to FIS organizations. The local counterintelligence field office and local office of the Federal Bureau of Investigation must be contacted during the risk analysis process to assist in properly identifying all threats posed by foreign intelligence services.

(2) *Deliberate or inadvertent error by authorized or unauthorized users.* Computer viruses, malicious software, and programs designed to bypass security programs are examples of deliberate error. Accidental erasure of data by an authorized user is an example of an inadvertent error.

(3) *Curious unauthorized intruders who have no FIS connections.*

(4) *Manmade or natural disaster.*

e. Threat and vulnerability matching. Threats are always present but can only affect an AIS when a vulnerability or security weakness is present. The matching or pairing of a vulnerability with a threat must be evaluated to determine the level of impact of risk. The level of risk may be measured by determining the possible rate of occurrence.

f. Security requirements identification. Each security requirement drives the implementation of a countermeasure to reduce the occurrence of a vulnerability. The security requirement is the justification for the implementation of a safeguard.

g. Safeguard selection. At least one safeguard or countermeasure should be developed for each threat and vulnerability match. A cost for each safeguard will be estimated. Such safeguards should not be limited to hardware and software fixes. Personnel, physical, and other possible procedural solutions should also be explored.

h. Security posture comments and recommendations. A security posture statement is developed by summarizing the safeguards selected to meet the security requirements. This statement will be provided to the DAA with comments and recommendations such as those listed below:

(1) Accredit the AIS or LAN for processing in a particular mode of operation for a certain classification level. (This should be recommended when the security posture of the AIS or LAN is very high and when the residual risk is at an acceptable level.)

(2) Grant an IATO for a period of 90 days while additional security safeguards are installed. (This recommendation should be made when the security posture of the AIS or LAN requires enhancement due to a high level of residual risk.)

(3) Deny approval to operate. (This recommendation should be made when the AIS or LAN has a very low security posture and the residual risk is unacceptable.)

5–4. Management decision to implement countermeasures

a. The review of the security posture statement and recommendations are a responsibility of commanders or managers who rely on advice from ISS, counterintelligence, physical security, and other functional area experts. Identifying areas of exceptional or unacceptable risk is directly related to the organizational mission, goals, and objectives as stated by the commander or manager. At this point in the risk management process, commanders can influence the commitment of resources to obtain the most effective security safeguard and financial return on the investment. This analysis may reveal areas where reduced security is appropriate, based upon a low level of risk to mission objectives. These savings may then be applied to other security requirements.

b. The selection of security controls must include a consideration of functional, technical, and economic feasibility and operational efficiency. Security requirements generally broaden managerial, operational, and administrative procedures, and in some cases, separate expenses occur that are directly attributable to these requirements. Only the commander or DAA can properly judge and balance the additional expense of security against operational efficiency. Commanders and organizational leadership must completely understand the impact of AIS on mission accomplishment and the risks involved in operating the AIS. The commander or DAA must, therefore, resolve any perceived conflict between operational and security considerations.

c. If existing risks are determined to be unacceptable and require countermeasures impractical or impossible to implement, the commander or DAA should terminate the operation of the system.

d. If penetration testing is a countermeasure to be employed, see AR 380–53 for policy requirements.

5–5. Implementation of safeguards

An effectively applied risk analysis should lead to a series of interrelated countermeasures to be implemented according to a plan approved by the commander or DAA. The commander or DAA must always participate in this process because of the risk resulting from growing dependence upon AIS.

5–6. Periodic review of the Risk Management Program

Organizational and operational dynamics demand a continuous review of the risk management program for effectiveness. Commanders must be assured that controls are providing the desired results. This process is an important step in ensuring the documented security techniques have not created a more serious vulnerability or risk. The collective effectiveness of applied countermeasures is the basis for future security actions that assist in identifying problem areas and additional security requirements.

Appendix A References

Section I Required Publications

AR 380–5
Department of Army Information Security Program. Cited in paras 1–6*d*(2)(*f*), 2–3*a*(5), 2–10*f*, 2–12*e*, 2–13*c*(1), 2–19*b*, 2–19*c*, 2–20*c*, 2–20*d*, 2–21*f*, 2–22*a*(1), 2–27*a*, 2–27*b*, and 2–28*a*.

AR 380–67
Department of the Army Personnel Security Program. Cited in paras 2–17*a–c*, 2–17*e*, 2–17*f*, and 2–18*b* through *d*.

(C) DIAM 50–4
Security of Compartmented Computer Operations (U). Cited in paras 3–9*a*, 3–9*d*, 2–30*a–b–d*, 3–11*h*(2)–(5)–(8). This publication may be obtained from DIA (SY–ID), Bolling Air Force Base Building 6000, Washington, DC 20340–001.

(C) DIAM 50–5
Sensitive Compartmented Information (SCI) Contractor Administrative Security VOL I and VOL II (U). Cited in paras 3–9*a* and 2–30*d–f*. This publication may be obtained from the DIA address above.

(C) DOD Pub C–5030.58–M
Security Criteria and Telecommunications Guidance. Cited in para 1–1*c*(4). This publication may be obtained from the Deputy Assistant Secretary of Defense for Command, Control Communications and Intelligence (Intelligence and Security).

DOD 5200.28–STD
Department of Defense Trusted Computer System Evaluation Criteria. Cited in paras 2–1*e*, 2–3*a*(5), 2–3*b*, 2–3*b*(3), 2–23*c*(2), 3–2*c*(3), 3–2*d*(5), and 3–9*d*(3). This publication is available from the National Computer Security Center, Office of Standards and Products, ATTN: Chief of Computer Security Standards, Fort Meade, MD 20755–6000.

Information Systems Security Products and Services Catalogue
Cited in paras 4–3*e*(1) and 4–3*e*(3). This publication may be obtained from the Superintendent of Documents, U.

JCS 6–03.7
Security Policy for the GCCS Intercomputer Network. Cited in para 1–1*c*(2). The point of contact for this publication is Joint Chiefs of Staff, Information Management Division, Pentagon, Room 2B941, Washington, DC 20318–0400

NCSC–TG–005
Trusted Network Interpretation. Cited in paras 2–23*b*(7) and 2–23*c*(2). This publication may be obtained from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

Section II Related Publications

A related publication is merely a source of additional information, which the user does not have to read to understand this regulation.

AR 15–6
Procedures for Investigating Officers and Boards of Officers.

AR 25–1
The Army Information Resources Management Program.

AR 25–12
Criteria for Insuring the Competency of Personnel to Install, Repair, and Maintain Communications Security Equipment.

AR 25–55
The Department of the Army Freedom of Information Act Program

AR 25–400–2
The Modern Record Keeping Systems (MARKS)

AR 70–1
Systems Acquisition Policy and Procedures.

AR 105–64
U.S. Army Communications Electronics Operation Instructions Program (CEOI).

AR 190–13
The Army Physical Security Program.

AR 190–51
Security of Unclassified Army Property (Sensitive and Nonsensitive).

AR 310–25
Dictionary of United States Army Terms.

AR 340–21
The Army Privacy Program.

(C) AR 380–28
Department of Army Special Security System.

AR 380–40
Policy for Safeguarding and Controlling Communication Security (COMSEC) Material.

AR 380–53
Information Systems Security Monitoring.

(C) AR 380–381
Special Access Programs (SAPs).

AR 381–10
U.S. Army Intelligence Activities.

AR 381–12
Subversion and Esponiage Directed Against U.S. Army (SAEDA).

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

AR 381–20
U.S. Army Counterintelligence Activities.

AR 525–20
Information Warfare/Command and Control Warfare (IW/C2W) Policy.

AR 530–1
Operations Security (OPSEC).

CSC–STD–003–85
Computer Security Requirements.

CSC–STD–004–85
Technical Rationale Behind CSC–STD–003-85: Computer Security Requirements.

DA Pam 25–380–2
Security Procedures for Controlled Cryptographic Items (CII).

(S) DCID 1/16
Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U). This publication may be obtained from DIA (SY–ID), Bolling Air Force Base (Building 6000), Washington, DC 20340-001.

DCID 1/21
Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF), 29 July 1994.

DIAM 50–24
Secure Communications for the Operations of Secure Telephone Units (STU–III) and Modems with a Sensitive Compartmented Information Facility (SCIF). Available from the DIA (SY–ID), address above.

DOD 5200.1
DOD Information Security Program

DOD Instruction 5215.2
Physical Security Technical Vulnerability Reporting Program

DOD 5200.22–M
Industrial Security Manual for Safeguarding Classified Information.

DOD 5220.22–R
Industrial Security Regulation.

(S/NF/WN) DST–1750S–208–93
Threats to U.S. Army Tactical, Strategic, and Sustaining Base Information

Director of Information Systems for Command, Control, Communications, and Computers
Keeping the Highway Open and Secure for Force XXI. Vol. I: The Army C2 Protect Program Management Plan (PMP); Vol. II: The Army C2 Protect Master T

Executive Order 12958
Classified National Security Information, 17 April 1995.

Federal Standard 1027
General Security Requirements for Equipment Using the Data Encryption Standard.

FIPS Pub 31
Guidelines for Automatic Data Processing Physical Security and Risk Management.

FIPS Pub 65
Guidelines for Automatic Data Processing Risk Analysis.

JER2–301
Joint Ethics Regulation, 2nd Amendment, March 1996.

(S) MJCS 75–87
Safeguarding the Single Integrated Operational Plan (U).

NCSC–TG–001
A Guide to Understanding Audit in Trusted Systems.

NCSC–TG–003
A Guide to Understanding Discretionary Access Control in Trusted Systems.

NCSC–TG–006
A Guide to Understanding Configuration Management in Trusted Systems.

NCSC–TG–007
A Guide to Understanding Design Documentation in Trusted Systems.

NCSC–TG–025, Version 2
A Guide to Understanding Data Remanance in Automated Information Systems.

NSTISSI No. 4009
National Security Telecommunications and Information Systems Security (NSTISS), National Information Systems Security (INFOSEC) Glossary

NTISSM 2–90
COMPUSEC

ODCSINT Pamphlet 380–25–1
Accreditation Handbook for U.S. Army DOD Intelligence Information Systems (DODIIS) Intelligence Automated Information Systems (AIS) and Networks Processing Sensitive Compartmented Information (SCI)

(S/NF/WN) SPB 145–95
Intelligence Community and Related Automated Information Systems and Networks: Vulnerabilities and Threats (U)

17 USC 506
Copyright Infringement

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

DA Form 11–2–R
Management Control Evaluation Certification Statement

DD Form 254
Contract Security Classification Specifications

SF 706
Top Secret (Label for ADP Media)

SF 707
Secret (Label for ADP Media)

SF 708
Confidential (Label for ADP Media)

SF 710
Unclassified (Label for ADP Media)

SF 711
Data Descriptor (Label for ADP Media)

SF 712
Classified SCI

Appendix B
Army-Sponsored Use of the Internet Computer Systems

This policy covers Army-sponsored use of the Internet computer systems. It provides the minimum guidelines for such use and does not preclude MACOMs from imposing more stringent local procedures. The MACOMs may further delegate responsibilities to the appropriate designated approval authorities, as desired. However, the ultimate responsibility for securing systems remains with the MACOM.

B–1. Internet access

Many unclassified Army systems allow users to access the Internet. While the Army promotes the use of the Internet to achieve Army goals, appropriate safeguards must be established to prevent and detect technical attacks made on Army systems and to ensure classified or sensitive information is not inadvertently released to unauthorized personnel.

B–2. Authorized use

Users will employ Internet access for authorized, unclassified U.S. Government business. The Joint Ethics Regulations now allow users to make limited use of DOD telephones, E-mail systems, and Internet connections for personal use, so long as such uses are on a not-to-interfere basis and are not for an improper purpose (such as conducting a private business or reviewing pornography). Users are not to use their own private accounts for Army-related business unless specifically authorized to do so by their director of information management/deputy chief of staff for information management (DOIM)/(DCSIM). Users are authorized to download and upload programs, graphics, and textual information between the Internet and an unclassified Government-owned personal computer. Personnel will scan all files for viruses before storing, transmitting, or processing information within Army computers, systems, or networks.

B–3. DAA approval

DAA approval is required before connection of any system to the Internet. DAAs (in coordination with DOIMs) will ensure adequate firewalls are in place to prevent the contamination of Army systems and/or possible denial of service. Systems containing classified information will not be connected to the Internet. Systems containing SBU information will employ the DES Standard 1027 during transmission of information. Users of any system connected to the Internet must be provided and must read a copy of these guidelines. The ISSMs are responsible for ensuring that authorized users are trained and briefed on the use of such systems.

B–4. Shared accounts

Personnel will not share E-mail and Internet accounts with other persons. However, MACOMs may establish group E-mail/group accounts as a cost-saving measure. The system ISSO must maintain a list of users who may access the group account and must restrict access of the account to authorized users. The individual user is responsible for all activity during access to the account. The user will not attempt to “talk around” classified topics while communicating on the Internet. Personnel may only conduct classified discussions on systems approved for the appropriate classification level (SIPRNET, JWICS, and so forth).

B–5. Home pages and web sites

Pursuant to the 18 July 1997 policy statement from the Office of the Secretary of Defense, entitled “Establishing and Maintaining a Publicly Accessible Department of Defense Web Information Service” or its subsequent implementation, home pages and web sites may be created allowing access to the public at large or to a limited audience. The links to information on web sites intended for limited audiences should have access controls. These controls should be administered by the web-master or system administrator per paragraph 2-3 of this regulation. Web-masters or systems administrators shall develop and publish local policies for the submission of information onto the organization’s home page. Publishing Army information onto electronic bulletin boards or World-wide Web home pages constitutes the public release of information and must comply with the established policy for the release of specific information. Persons wishing to release Army information must first ensure that they have public release authority. Clearance of specific information should be directed to the appropriate proponent, the local public affairs office, or foreign disclosure office.

B–6. Reporting suspicious activity

Army Internet sites are considered as lucrative intelligence sources and are targeted for information collection efforts. As stated in AR 380–12, Army personnel must report suspicious activity through Counterintelligence (SAEDA) and OPSEC channels. The Copyright Act, the Freedom of Information Act, the Privacy Act, and statutory Federal records requirements also contain provisions with which users must comply. Users should consult these guidelines and the office the local staff judge advocate regarding any Internet activity that raises legal concerns.

B–7. Requests for information

The MACOMs are responsible for any search and review of their holdings of Internet data for purposes of responding to requests for information pursuant to the Freedom of Information Act or Privacy Act or congressional or other investigative inquiry.

Appendix C
Management Control Evaluation Checklist

C–1. Function

The function covered by this checklist is the administration of the Army Information System Security Program.

C–2. Purpose

The purpose of this checklist is to assist Assessable Unit Manager and Management Control Administrators in evaluating the key management controls outlined below. It is not intended to cover all controls.

C–3. Instruction

Answers must be based on the actual testing of key management controls (for example, document analysis, direct observation, sampling, simulation, or others). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key management controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2–R (Management Control Evaluation Certification Statement). A locally reproducible copy of this form is located at the back of this publication.

C–4. Test questions

a. Are appropriate security personnel (for example, ISSPM, ISSM or ISSO) appointed?

b. Are risk analysis/vulnerability assessments performed at the appropriate levels for systems that process Army information?

c. Are the appropriate leadership/management personnel aware of the results of risk analysis/vulnerability assessments?

d. Are countermeasures identified based on the results of risk analysis/vulnerability assessments?

e. Are countermeasures in place commensurate with risk/vulnerability?

f. Is there a written security plan to document implementation of countermeasures?

g. Has leadership/management formally accepted the risk to process the information involved? (Are the systems accredited?)

h. Are countermeasures routinely tested (for example, user IDs, passwords, audit trails)?

i. Is Information System Security training performed at appropriate levels?

j. Are MACOMs, installations, or activities funding their INFOSEC requirements under the appropriate MDEP?

k. Are security incidents/violations (for example, viruses, unauthorized entries or attempts) reported and investigated?

l. Have plans been developed to ensure continued operation in the event of major disruption (for example, fire, natural disaster, bomb threat, civil disorder)?

m. Has a configuration control board approved each network? Is there an appropriate security official as a member of each board?

C–5. Supersession

This checklist replaces the checklist for Intelligence Activities/Army Information System Security Program (AISSP) previously published in DA Circular 11–92–1.

C–6. Comments

Help to make this a better tool for evaluating management controls. Submit comments to: Director of Information Systems for Command, Control, Communications, and Computers (SAIS–PAC), 107 Army Pentagon, Washington, DC 20310–0107.

Appendix D
Security Plan/Accreditation Document

The paragraphs in this appendix are to be used as an outline when preparing accreditation documentation. Each paragraph of the outline must be addressed with the exception of accreditation for small computers. The asterisk (*) at a paragraph indicates that the requirement is optional for accreditation of small computers. The degree of detail required in each paragraph can and should vary with the system's size, complexity, sensitivity designation, mode of operation, and number of users. If a system processes Sensitive Compartmented Information (SCI) and is being accredited or reaccredited, all documentation must comply with DODIIS site-based accreditation requirements using the guidance provided in DIAM 50–4 and paragraph 3–11 of this regulation.

D–1. Basic system(s) information and identification

a. System name or title. (If the system does not have a name or title, use the manufacturer and model number for the main processing units.)

b. System category. (Indicate whether or not the system(s) is a general AIS support system or has a specific application; for example, intelligence, personnel, financial, and so forth.)

c. Type accreditation. (Indicate whether this is a generic or operational accreditation. For operational accreditation, indicate whether or not a single identifiable system or a group of similar systems are covered.)

d. System status. (Indicate either "developmental" or"operational" as appropriate.)

e. System overview. (Provide a description of the function and purpose of the system.)

f. System environment and special considerations. (Describe physical, operational, or other factors external to the system which affect its security. Describe system interfaces to other systems or networks.)

g. Information contacts. (As a minimum, list the name and telephone number of the appointed ISSO. Other personnel with technical knowledge of the system may be listed.)

h. System identification. (The system(s) must be identified in the accreditation in a manner sufficient to determine which system(s) are governed by that particular accreditation. For operational accreditation, this will be done through a serial number listing of the central processing units of the AIS accredited or through another means that clearly defines the systems accredited. A separate enclosure may be used. For generic accreditation, use military nomenclature, a commonly accepted system acronym, or other method determined by the DAA.)

i. Near- and long-term goals. (Describe near- and long-term goals of the system and the contribution of this accreditation to accomplishing these goals.)

D–2. Sensitivity, protection requirements, security mode, and minimum trusted class

a. Sensitivity designation. (List the sensitivity designation from para 2–2*a*. Further describe, in general terms, the nature of the information and the reason it requires protection. Cite appropriate laws requiring protection of the information, such as the Privacy Act, if applicable.)

b. Protection requirements. (Indicate whether the system protection requirements are based on the need for confidentiality, integrity and/or availability of the information. For each of these three categories, indicate whether they are of primary, secondary, or no concern. There may be more than one primary concern designated. For example, confidentiality and integrity may both be primary concerns and availability of information of no concern.)

c. Security mode of operation. (Indicate the security mode of operation from para 2–2*b*.)

d. Minimum trusted class. (Enter the required minimum trusted system class as determined from appendix E. Indicate how the system meets the class or include a timetable for meeting the required class per para 2–3*b*. Include any applicable information regarding use of approved NSA products.)

D–3. Risk management review

(Include in this section a risk management review which includes an examination of threats, vulnerabilities, and the resulting risks in accordance with chapter 5. After determining risks, indicate in the next paragraph the selected countermeasures that result in acceptable risk. For small computers, reference may be made to a single command-wide or installation-wide risk management review, if one exists.)

D–4. Implementation of controls and countermeasures

(Include a description of measures taken in the areas of personnel, physical, environmental, procedural, hardware, software, TEMPEST, and communications security as required in AR 381–14 (S). This section must indicate how the control measures support the mode of operation listed above. Include contingency planning information or attach a separate contingency plan.)

D–5. Certification*

(Describe the certification testing which was accomplished to support the accreditation. Attach the certification plan for generic accreditation. For operational accreditation, attach a certification plan or describe the certification process in this paragraph.) This is not required in a collateral PC environment.

D–6. Facility information

(As with all the documentation associated with accreditation, the facility information should be tailored to the size, criticality, mode of operation, data sensitivity, and number of users for the AIS.) The following paragraphs will be addressed in compiling facility information:

a. Facility identification and location.

b. Architectural drawings or building plans. (Plans of the building housing the facility should show the location of exits, guard posts, fire alarms and hoses, master utility panels, and facilities adjacent to, above, and below the facility.

c. Facility floor plan. (The floor plan will show placement of all equipment, fire extinguisher and sprinklers, smoke and motion detection devices, emergency lighting, and so forth.)

*d. System interface description.** (Include a diagram or a description of interfaces for all major equipment, processing units, terminals, peripherals, communications modems, controllers, concentrators, encryption devices, and other connections.)

e. Other diagrams. (If applicable, diagrams will show specialized displays of communication, electrical wiring, special communication switching, or patching panels.)

*f. Operating system.** (List the release or level number and date first put into operation on the system.)

g. Applications software. (List the major applications programs or systems.)

D–7. Network considerations

(For systems being accredited as a separate AIS in the IAA view (para 2–23), indicate the network DAA (if identifiable) and describe the conditions under which connection to the IAA has been approved. For STS view networks, this section should address the network's capability to provide communications integrity, protection against denial of service, and compromise protection. See para 2–22.)

D–8. Attachments

(This section is not applicable while the document is serving as the security plan; however, when used as an accreditation document and forwarded to the DAA, the below items should be attached as applicable.)

a. Users security manual/SOP. (This is a mandatory and extremely critical item for generic accreditation. Recommended for operational accreditation although such procedures may be incorporated in other documents.)

b. Appointment orders for the ISSO.

c. Approved waivers. Approved waivers (for example, COMSEC waivers approved in accordance with chap 4, TEMPEST waivers approved in accordance with AR 381–14 (S), trusted computer class waivers approved in accordance with para 2–3*b*, and so forth).

d. Certification plan.

e. Security classification guide.

f. Contingency plan.

Appendix E
DOD 5200.28-STD Guidelines for Determining Minimum AIS Requirements

Minimum security requirements for all AIS are listed in paragraph 2–3*a*. Additionally, systems operating in the systems high, compartmented, or multilevel security modes must include features which meet the appropriate trusted systems class from DOD 5200.28–STD. Use this appendix to determine which class is required.

E–1. Mode of operation

Determine mode of operation in accordance with paragraph 2–2*d* of this regulation. Determine if the system processes formal categories of data and, if so, whether or not all users have been granted formal access to all categories of data. Formal categories of data are categories for which a written approval must be issued prior to access, for example: SCI compartments, NATO information, and SAPs.

E–2. Dedicated mode

If the mode of operation is dedicated, there is no further requirement beyond those contained in paragraph 2–3*a*.

E–3. Systems high mode

If the mode of operation is systems high, a class C2 minimum evaluation class is required.

E–4. Compartmented mode

If the mode of operation is compartmented—

a. A class B1 minimum evaluation class is required if no user lacks formal access approval for more than one category.

b. A class B2 minimum evaluation class is required if at least one user does not have formal access approval for more than one category being processed.

E–5. Multilevel mode

If the mode of operation is multilevel, determine minimum evaluation class according to table E–1.

a. Enter the Maximum Data Classification column at the highest classification of data processed.

b. Find the minimum clearance level of users, defined to be the maximum clearance of the least cleared user. Although a clearance does not exist for SBU information, users usually have at least this level of access if they are U.S. Government employees or work on behalf of the U.S. Government on official business and have been processed for ADP III position, per paragraph 2–17.

c. Use the column for case one if there are no formal categories of information involved or if all users have formal access approval for all categories of data processed by the system. Use the column for case two if no user lacks formal access approval for more than one category. Use the column for case three if at least one user lacks formal access approval for more than one category being processed.

d. If SCI data are being processed and all users have not been granted access to SCI based on a Single Scope Background Investigation (SSBI), the mode of operation is multilevel. Enter table E–1 as if the user's clearance is SECRET even if the actual clearance is TOP SECRET based on a background investigation. In no case may a system process SCI data unless the minimum clearance level of all users is at least SECRET.

e. Entries marked N/A in table E–1 mean these combinations of user clearance, access, and data classification are prohibited for Army AIS.

Table E–1
Determining minimum evaluation class from DOD 5200.28-STD for multilevel operations

Maximum data classification	Minimum clearance level of users	Case 1	Case 2	Case 3
TS	S	B2	B3	A1
	C	B3	A1	N/A
	Unclas, Sen	A1	N/A	N/A
	Uncleared	N/A	N/A	N/A
S	C	B1	B2	B3
	Unclas, Sen	B2	B3	A1
	Uncleared	B3	A1	N/A
C	Unclas, Sen	B1	B2	B2
	Uncleared	B2	B3	A1

Appendix F
Clearing, Sanitizing, and Releasing Computer Components

F–1. Purpose

The purpose of this appendix is to provide guidance and procedures to clear and sanitize magnetic storage media that are no longer useable, require transfer, or should be released from control. Personnel needing to destroy, degauss, overwrite, declassify, downgrade, release, or ship media from AISs for all classification levels (to include COMSEC keying material) must follow the rules and table F-1 of this appendix. If an item is not contained in table F-1, the headquarters level ISSPM must be contacted for directions.

F–2. Scope

These procedures are effective in the following life-cycle phases:

CONCEPTS DEVELOPMENT PHASE	NO
DESIGN PHASE	NO
DEVELOPMENT PHASE	YES
DEPLOYMENT PHASE	YES
OPERATIONS PHASE	YES
RECERTIFICATION PHASE	YES
DISPOSAL PHASE	YES

F–3. Implementing security measures

The information systems security manager (ISSM) is responsible for the security of all ISs and media assigned to the organization and under his/her purview. To protect these assets, he/she must ensure the security measures and policies contained within this appendix are followed. Additionally, the ISSM will publish supplemental organizational procedures (standing operating procedures (SOPs), and so forth), if needed, to implement the requirements herein.

F–4. Procedures

The procedures contained below meet the minimum security requirements for the clearing, sanitizing, releasing, and disposal of magnetic media. These procedures will be followed when it becomes necessary to release magnetic media, regardless of classification, from Sensitive Compartmented Information (SCI) channels. Media that have ever contained SCI, other intelligence information, or Restricted Data cannot be sanitized by overwriting; such media must be degaussed before release. Media that have ever contained Cryptographic (CRYPTO) material cannot be sanitized at all; such media must be destroyed.

a. Review of terms. To better understand the procedures contained herein, it should be understood that overwriting, clearing, purging, degaussing, and sanitizing are not synonymous with declassification. Additionally, the following definitions should be reviewed:

(1) *Clearing.* Clearing is the process of eradicating the data on the media before the media are reused in an environment that provides an acceptable level of protection for the data that were previously on the media before clearing. In general, laboratory techniques allow the retrieval of information that has been cleared, but normal operations do not allow such retrieval. Clearing can be accomplished by overwriting or degaussing.

(2) *Sanitizing (also purging).* Sanitizing is the process of removing the data on the media before the media are reused in an environment that does not provide an acceptable level of protection for the data that were on the media before sanitizing. In general, laboratory techniques cannot retrieve data that have been sanitized/purged. Sanitizing may be accomplished by degaussing.

(3) *Destroying.* Destroying is the process of physically damaging the media to the level that the media are not usable as media, and so that there is no known method of retrieving the data.

(4) *Declassification.* Declassification is a separate administrative process for which the result is a determination that the given medium no longer requires protection as classified information. The procedures for declassifying media require Designated Approving Authority (DAA) or Service Certifying Organization (SCO) approval.

b. Overwriting media. Overwriting is a software process that replaces the data previously stored on magnetic storage media with a predetermined set of meaningless data. Overwriting is an acceptable method for clearing. However, the effectiveness of the overwrite procedure may be reduced by several factors, including: ineffectiveness of the overwrite procedures, equipment failure (for example, misalignment of read/write heads), or inability to overwrite bad sectors or tracks or information in inter-record gaps.

(1) *Overwriting procedure.* The preferred method to clear magnetic disks is to overwrite all locations three times (the first time with a random character, the second time with a specified character, the third time with the complement of that specified character).

2. Overwrite verification. The overwrite procedure must be verified by the ISSM or designee.

c. Degaussing media. Degaussing (that is, demagnetizing) is a procedure that reduces the magnetic flux on media virtually to zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used in the sanitization process. Degaussing is more effective than overwriting magnetic media.

(1) Magnetic media are divided into three types (I, II, III) based on their coercivity. Coercivity of magnetic media defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. The level of magnetic media coercivity must be ascertained prior to executing any degaussing procedure.

(2) The individual performing the physical degaussing of a component must ensure that the capability of the degausser meets or exceeds the coercivity factor of the media, and that the proper type of degausser is used for the material being degaussed. The three types of degaussers are—

(a) Type I. Used to degauss Type I media (that is, media for which coercivity is no greater than 350 oersteds (Oe)).

(b) Type II. Used to degauss type II media (that is, media for which coercivity is no greater than 750 Oe).

(c) Type III. Used to degauss type III media (that is, media for which coercivity is in excess of 750 Oe). Currently, there are no degaussers that can effectively degauss all Type III media. Some degaussers are rated above 750 Oe, and their specific approved rating will be determined prior to use.

(3) Refer to the current issue of the National Security Agency (NSA) Information Systems Security Products and Services Catalogue (Degausser Products List Section), for the identification of degaussers acceptable for the procedures specified herein. These products will be periodically tested to assure continued compliance with the appropriate specification. National specifications provide a test procedure to verify continued compliance with the specification.

(4) Once a degausser has been purchased and has become operational, the gaining organization must establish a SOP explaining how it will be used.

d. Sanitizing media. Tables F–1 and F–2 provide instructions for sanitizing data storage media and system components.

e. Destroying media. Data storage media will be destroyed in accordance with DAA/SCO approved methods.

(1) *Expendable item destruction.* Expendable items (for example, floppy diskettes) are not authorized to be released for reuse outside of the SCI community. If these items are damaged or no longer deemed usable, they will be destroyed. When destroying, remove the media (magnetic mylar, film, ribbons, and so forth) from any outside container (reels, casings, hard cases or soft cases, envelopes, and so forth) and dispose of the outside container in a regular trash receptacle. Cut the media into pieces (a crosscut chipper/shredder may be used to cut the media into pieces) and then burn all pieces in a secure burn facility. If applicable environmental laws do not permit burning of a particular magnetic recording item, it will be

degaussed, cut into pieces (a chipper/shredder preferred) and disposed of in a regular trash receptacle.

(2) *Destruction of removable hard disks and disk packs.*

(a) Removable hard disks. Removable hard disks are expendable items and are not authorized to be released for reuse outside of the SCI community unless they have been degaussed and declassified. Each item is considered classified to the highest level of data stored or processed on the IS in which it was used. If removable hard disks are damaged, or no longer deemed usable, they will be destroyed. If the platter(s) of the defective unit can be removed and the removal is cost effective, then destruction of a removable hard disk consists of dismantling the exterior case and removing the platter from the case. Local destruction of the platter consists of removing the magnetic surface by sanding.

Table F–1
Sanitizing data storage media

Media type	Procedure(s)
Magnetic tape	
Type I	a or b
Type II	b
Type III	Destroy
Magnetic disk packs	
Type I	a or b
Type II	b
Type III	Destroy
Magnetic disks	
Floppies	Destroy
Bernoullis	Destroy
Removable hard disks	a or b or c
Non-removable hard disks	a or b or c
Optical disks	
Read Only (including CD-ROMs)	Destroy
Write Once, Read Many (WORM)	Destroy
Read Many, Write Many	Destroy

Procedures

These procedures will be performed or supervised by the ISSO.
a. Degauss with a Type I degausser.
b. Degauss with a Type II degausser.
c. Overwrite all locations three times (first time with a random character, second time with a specified character, third time with the complement of the specified character).

Table F–2
Sanitizing system components

Type of component	Procedure
Magnetic bubble memory	a or b or c
Magnetic core memory	a or b or d
Magnetic plated wire	d or e
Magnetic-resistive memory	Destroy
Solid state memory components	
Dynamic random access memory (DRAM) (Volatile)	Destroy
if RAM is functioning	d, then e and i
if RAM is defective	f, then e and i
Static random access memory (SRAM)	j
Programmable ROM (PROM)	Destroy (see h)
Erasable programmable ROM (EPROM/UVPROM)	g, then c and i
Electronically erasable PROM (EEPROM)	d, then i
Flash EPROM (FEPROM)	d, then i

Procedures

These procedures will be performed or supervised by the ISSO.
a. Degauss with a Type I degausser.
b. Degauss with a Type II degausser.
c. Overwrite all locations with any random character.
d. Overwrite all locations with a random character, a specified character, then its complement.
e. Remove all power, including batteries and capacitor power supplies from RAM circuit board.
f. Perform three power on/off cycles (60 seconds on, 60 seconds off each cycle, at a minimum).
g. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.
h. Destruction required only if ROM contained a classified algorithm or classified data.
i. Check with the DAA/SCO to see if additional procedures are required.
j. Store a random unclassified test pattern for a time period comparable to the normal usage cycle.

(b) Disk packs. Each item is considered classified to the highest level of data stored or processed on the IS in which it was used. If disk packs are damaged, or no longer deemed usable, they will be destroyed. Local destruction of the platter consists of removing the magnetic surface by sanding.

f. Malfunctioning media. Magnetic storage media that malfunction or contain features that inhibit overwriting or degaussing will be reported to the Information System Security Officer (ISSO). The ISSO will coordinate the repair or destruction of the media with the ISSM and responsible DAA/SCO.

g. Release of memory components and boards. Prior to the release of any malfunctioning components, the following requirements will be met in respect to coordination, documentation, and written approval. This section applies only to components identified by the vendor or other technically knowledgeable individual as having the capability of retaining user-addressable data. It does not apply to other items (for example, cabinets, covers, electrical components not associated with data), which may be released without reservation. For the purposes of this annex, a memory component is considered to be the lowest replacement unit (LRU) in a hardware device. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies. Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing components for release (see table F–2). Memory components are specifically handled as either volatile or nonvolatile, as described below.

(1) *Volatile memory components.* Memory components that do not retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system do not contain residual data, are considered volatile memory components. Volatile components that have contained extremely sensitive or classified information may be released only in accordance with procedures developed by the ISSM or designee and stated in the Accreditation Support documentation. A record must be maintained of the equipment release indicating that, per a best engineering assessment, all component memory is volatile and that no data remain in or on the component when power is removed.

(2) *Nonvolatile memory components.* Components that do retain data when all power sources are discontinued are nonvolatile memory components - including Read Only Memory (ROM), Programmable ROM (PROM), or Erasable PROM (EPROM), and their variants - that have been programmed at the vendor's commercial manufacturing facility, and are considered to be unalterable in the field, may be released. All other nonvolatile components (for example, removable/non-removable hard disks) may be released after successful completion of the procedures outlined in table F–2. Failure to accomplish these procedures will require the ISSM, or designee, to coordinate with the DAA/SCO to determine releasability.

(3) *Other nonvolatile media.*

(a) Visual displays. A visual display may be considered to be sanitized if no sensitive information is etched into the visual display phosphor. The ISSO should inspect the face of the visual display without power applied. If sensitive information is visible, destroy the visual display before releasing it from control. If nothing is visible, the ISSO shall apply power to the visual display; then vary the intensity from low to high. If sensitive information is visible on any part of the visual display face, the visual display shall be destroyed before it is released from control.

(b) Printer platens and ribbons. Printer platens and ribbons shall be removed from all printers before the equipment is released. One-time ribbons and inked ribbons shall be destroyed as sensitive material. The rubber surface of platens shall be sanitized by wiping the surface with alcohol.

(c) Laser printer drums, belts, and cartridges. Laser printer components containing light-sensitive elements (for example, drums, belts, complete cartridges) shall be sanitized before release from control.

1. Elements containing information that is classified, but is not intelligence information, can be considered sanitized after printing three printer font test pages.

2. Elements containing intelligence information shall be sanitized in accordance with the policy contained in the Director of Central Intelligence Directive (DCID) 1/21.

h. Release of systems and components. The ISSM, or designee, shall develop equipment removal procedures for systems and components and these procedures shall be stated in the Accreditation Support documentation. When such equipment is no longer needed, it can be released if—

(1) It is inspected by the ISSM, or designee. This inspection will assure that all media, including internal disks, have been removed or sanitized.

(2) A record is created of the equipment release indicating the procedure used for sanitization and to whom the equipment was released. The record of release shall be retained for a period prescribed by the DAA/SCO.

(3) Procedures specified by the DAA/SCO are used. Following release, administratively notify the DAA/SCO. The National Security Agency/Central Security Service (NSA/CSS) Form G6522 or similar form or documentation will be used to document the local release or disposal of any IS or component.

Appendix G
Information Systems Security Monitoring Capabilities and Restrictions

All Army users of information systems have a responsibility to ensure the security of these systems. The Army relies on a layered approach for security of these systems placing responsibility at the user, system administrator, network administrator, and ACERT levels. As part of this approach, the Army recognizes the need for administrators and the ACERT to implement procedures that assist in the identification of system vulnerabilities. Neither administrators nor the ACERT through the Computer Defense Assistance Program (CDAP) have unlimited latitude to conduct these assessments. AR 380–19 concerns vulnerability analysis, which is systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

In fact, procedures that verify the vulnerabilities through the use of "hacker" techniques are governed by AR 380–53. AR 380–53 concerns penetration testing, which concerns security testing in which evaluators attempt to circumvent the security features of an automated information system 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 the automated information system vulnerabilities.

This appendix, therefore, discusses assessment capabilities both as responsibilities and restrictions for the administrators and the ACERT.

G–1. System administrator's tasks

a. Objective. The two main goals of the system administrator (SA) are to keep the AIS operational and the system secure. The following tasks are essential in accomplishing these goals:

(1) Ensure that the operating system for the AIS is configured properly and that the security features appropriate to the intended level of system operation are properly set. Such settings should be periodically reviewed; such reviews will not involve looking at information or data contained in the files of individual users other than system configuration files. Examples of these files in UNIX include the following: .rhost, .profile, .history and .forward files.

(2) Use approved C2 Protect tools to periodically review system security. These may be security utilities provided with network software. At no time will the utilities be used to review user data even if the tool is capable of this function. The C2 Protect tools are approved by DISC4.

(3) Periodically check with the operating system manufacturer, the LIWA, and/or the DISC4 in order to keep informed of system security problems and patches as they are developed, and apply them as appropriate in order to maintain AIS security.

(4) Ensure audit software is properly configured and audit trail reports are periodically reviewed in accordance with this regulation.

(5) Review file names, length, permissions, and directories. If any of this information leads a SA to suspect that an individual user is misusing the system or engaging in other misconduct, the SA will notify, concurrently, the chain of command and contact LIWA/ACERT. The appropriate individual within the chain of command will contact CI and CID. At no time with the SA specifically target or track an individual's activities except as part of a properly authorized investigation.

(6) If a SA suspects an unauthorized user is attempting to access the AIS, the SA is authorized to take the actions necessary to verify and limit the penetration attempt from an unauthorized user. Once verified, the SA will notify, concurrently, the chain of command and contact LIWA/ACERT. The appropriate individual within the chain of command will contact CI and CID. The SA may make system backups of appropriate log, history files, and user directories. Once the SA has determined that the anomaly is in fact an unauthorized intrusion, and CI and CID have been notified, the SA will not in any other manner specifically target, track or attempt to investigate a suspected intruder's activities except as part of a properly authorized investigation.

b. Restrictions on system administrators in the normal performance of their duties. The SA does not have unlimited authority in operating the AIS. While security of the system is an important component of the administrator's job, there are restrictions on actions that an administrator may take in accomplishing the security function:

(1) The SA is NOT authorized to view, modify, delete, or copy data files that are stored on the AIS which are not part of the operating system except when—

(a) Authorized by the user or file owner.

(b) Performing system backup and disaster recovery responsibilities.

(c) Performing antivirus functions and procedures.

(d) Performing actions which are necessary to ensure the continued operation and system integrity of the AIS.

(e) Performing actions as part of a properly authorized investigation.

(2) The SA is NOT authorized to browse or read a user's E-mail. The SA may intercept, retrieve, or otherwise recover an E-mail message upon the written or verbal authorization of the parties involved or as part of a properly authorized investigation. When the SA must remove an E-mail message that is interfering with the operation of the AIS, the SA will make reasonable effort to notify the originator of the E-mail.

(3) The SA is NOT authorized to use hacker techniques in an attempt to penetrate his or her AIS. Such penetration testing will be authorized only in accordance with AR 380–53. Techniques include but are not limited to—

(a) The use of network analyzers, sniffers, or similar network monitoring systems to monitor the activities of specific system users. The use of these devices is authorized to perform valid system troubleshooting and diagnostics of network problems.

(b) "Keystroke monitoring" software of any kind will not be used either resident on the user's computer, or by monitoring computer network communications.

(c) The use of keyboarding or automated techniques to exploit/verify vulnerabilities identified by the C2 Protect tools.

c. Management searches. In the absence of a user, the SA is authorized to grant the user's supervisor temporary access to the user's data files, in order to allow access to data for official purposes. When such access is granted—

(1) The SA will brief the supervisor as to the limits of accessing the user's data files. This will include a warning that the search must be limited in scope to those files that could reasonably be related to the objective of the search (that is, E-mail access would NOT be reasonable when searching for a word processing file).

(2) Searches will be limited to the time necessary to locate the required data.

(3) Such access will not be used to circumvent regulatory or statutory requirements for investigations.

d. Assistance to law enforcement and counterintelligence. The SA is authorized to provide technical assistance as requested by the investigating agent when part of a properly authorized investigation.

G–2. Network administrator's tasks

a. Objectives. The network administrator (NA) operates under similar broad authority and restrictions as the SA. While it is the NA's responsibility to keep the networking infrastructure operational and secure, they operate under the same constitutional and statutory controls as the SA. These restrictions represent a balance between the actions necessary to provide a reliable and secure communications backbone for AIS, while at the same time ensuring the privacy rights of the users. It is the goal of the NA to ensure the continued operation infrastructure is composed of two major components–the communications medium (that is, wiring, fiber optics, and so forth) over which the AIS communications travel; and the network hardware (that is, hubs, concentrators, and so forth) which make up the physical equipment of the network. The following tasks are critical in achieving the goals of continuity and security:

(1) Ensure that all hardware and software components of the network infrastructure are properly configured and the security features and controls appropriate to the intended level of system operation are properly set. Such settings should be periodically reviewed to ensure that they are set correctly and have not been modified without the network administrator's knowledge.

(2) Only the use of approved C2 Protect tools is authorized to periodically review network security. These may be security utilities provided with network software. At no time will the utilities be used to review user data even if the tool is capable of this function. The general use of these tools will be to map the network and to conduct automated scans of individual machines for configuration errors that could lead to unauthorized access to individual machines and/or the network. The C2 Protect tools are approved by DISC4.

(3) Periodically check with the maker of the network components, the LIWA, and/or the DISC4, in order to keep informed of system security problems and patches as they are developed, and apply them as appropriate to maintain the integrity of the network.

(4) Use network management systems to monitor the operational status of the network, and to collect statistics on bandwidth utilization and error rates.

(5) If the NA suspects that an individual user is engaging in any misuse or misconduct the NA will notify, concurrently, the chain of command and contact LIWA/ACERT. The appropriate individual within the chain of command will contact CI and CID. The NA will not specifically target or track an individual's activities except as part of a properly authorized investigation.

(6) If the NA suspects an unauthorized user is attempting to access a system on the network, the NA will notify, concurrently, the chain of command and contact LIWA/ACERT. The appropriate individual within the chain of command will contact CI and CID. After the NA has determined that an anomaly is in fact an unauthorized intrusion, and CI and CID have been notified the NA will not specifically target, track, or attempt to investigate a suspected intruder's activities except as part of a properly authorized investigation.

(7) Use sniffers or network analyzers only as tools in diagnosing network problems (that is, to identify the source of bad ETHERNET packets).

b. Restrictions on network administrators in the normal performance of their duties.

(1) The NA is NOT authorized to view, modify delete or copy user data files which are in transit on the network or are stored on an AIS unless one of the following apply:

(a) Authorized by the user or file owner.

(b) Incidental to performing diagnostics functions to correct network problems.

(c) Incidental to performing actions which are necessary to ensure the continued operation and system integrity of the network.

(2) Only the use of approved C2 Protect tools is authorized to periodically review network security. These may be security utilities provided with network software. At no time will the utilities be used to review user data even if the tool is capable of this function. The general use of these tools will be to map the network and to conduct automated scans of individual machines for configuration errors that could lead to unauthorized access to individual machines and/or the network. The C2 Protect tools are approved by DISC4.

(3) The NA is NOT authorized to use hacker techniques in an attempt to penetrate their networks. Such activities will be conducted only in accordance with 380–53. Techniques include but are not limited to—

(a) The use of network analyzers, sniffers, or similar network monitoring systems to monitor the activities of specific system users. The use of these devices is authorized to perform valid system troubleshooting and diagnostics of network problems.

(b) "Keystroke monitoring" software of any kind will not be used either resident on the user's computer, or by monitoring computer network communications.

(c) Exploiting/Verifying through keyboarding or automated techniques, vulnerabilities identified by the C2 Protect tools.

c. Assistance to law enforcement and counterintelligence. The NA is authorized to provide technical assistance as requested by the investigating agent when part of a properly authorized investigation.

G–3. Land Information Warfare Activity tasks

a. Objectives. The Land Information Warfare Activity (LIWA) through its Army Computer Emergency Response Team (ACERT) provides the SA and the NA with assistance in reviewing security of Army networks and computers. This assistance is provided through a number of programs including the Computer Defense Assistance Program (CDAP). The procedures to identify AIS vulnerabilities are governed by this regulation, and the procedures to verify vulnerabilities are governed by AR 380–53. Section G–4 outlines the CDAP process. While the LIWA provides support to the SA and NA, they operate under the same constitutional and statutory controls as both the SA and NA. The following are functions which ACERT is permitted under this regulation:

(1) Assist the SA and NA in ensuring that all hardware and software components of the network infrastructure are properly configured and the security features and controls appropriate to the intended level of system operation are properly set. Such settings should be periodically reviewed to ensure that they are set correctly and have not been modified. This review may be accomplished through the use of manual means or automated means to check system configurations.

(2) Only the use of approved C2 Protect tools is authorized to periodically review security. These may be security utilities provided with network software. At no time will the utilities be used to review user data even if the tool is capable of this function. The general use of these tools will be to map the network and to conduct automated scans of individual machines for configuration errors that could lead to unauthorized access to individual machines and/or the network. The C2 Protect tools are approved by DISC4.

(3) Ensure audit software is properly configured.

(4) Review file names, length, permissions, ownership and directories.

(5) ACERT is authorized to take the actions necessary (automated or manual) to verify a penetration attempt from an unauthorized user. This includes the use of intrusion detection devices that may record network connections and protocols used/attempted. Once an unauthorized user has been verified, the ACERT will coordinate with the appropriate Army elements for action. The ACERT may make system backups of appropriate log, history files, and user directories.

(6) The authorized actions above will not be used to circumvent regulatory or statutory requirements for investigations.

b. Assistance to law enforcement and counterintelligence. The ACERT is authorized to provide technical assistance as requested by the investigating agent when part of a properly authorized investigation.

G–4. Program organization/structure

a. Introduction. The CDAP is organized and structured in phases (fig G–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 "rules of engagement." 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.

b. Phases.

(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/or provide the ACERT with specific authorization to analyze and penetrate the target network. The primary objectives of phase 1 are: Establish written request/authorization to conduct network security analysis 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. Establish priority for the effort and enter the request into the CDAP database for control, management, and scheduling. Establish operating/mission parameters for the target network or subnet.

(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. The primary objectives of phase 2 are: 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.

(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. The primary objectives of phase 3 are: Identify all machines on the network at the subnet level, identify all dial-in connections into the network at the machine, compare results with the documentation provided by the unit/activity, identify all paths of entry into each network subnet and flag risk areas.

(4) *Phase 4 - Network Scan.* The purpose of this phase is to assess intrusion susceptibility of the network at the machine level. The primary objective of phase 4 is: Identify all machines on the network which can be targeted for potential compromise/intrusion.

(5) *Phase 5 - Network Penetration.* This phase is authorized under AR 380–53 only and is provided here for reference only. 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. The primary objectives of phase 5 are: Exploit only vulnerabilities identified during the scanning phase, exploit vulnerabilities to the point of obtaining "superuser" access to the target machine or network.

(6) *Phase 6 - Penetration Verification.* This phase is authorized under AR 380–53 only and is provided here for reference only. The purpose of penetration verification is to provide positive verification

to the requesting unit or activity that system level compromise had been obtained and assess network intrusion detection. Due to the intrusive nature of this phase, this phase is optional. The primary objectives of phase 6 is to provide positive verification of system or machine compromise in the form of a message or new user account.

(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. The primary objective of phase 7 is to assist the requesting unit or activity with security or configuration fixes needed to correct the vulnerabilities found during the vulnerability analysis and penetration phases.

(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.

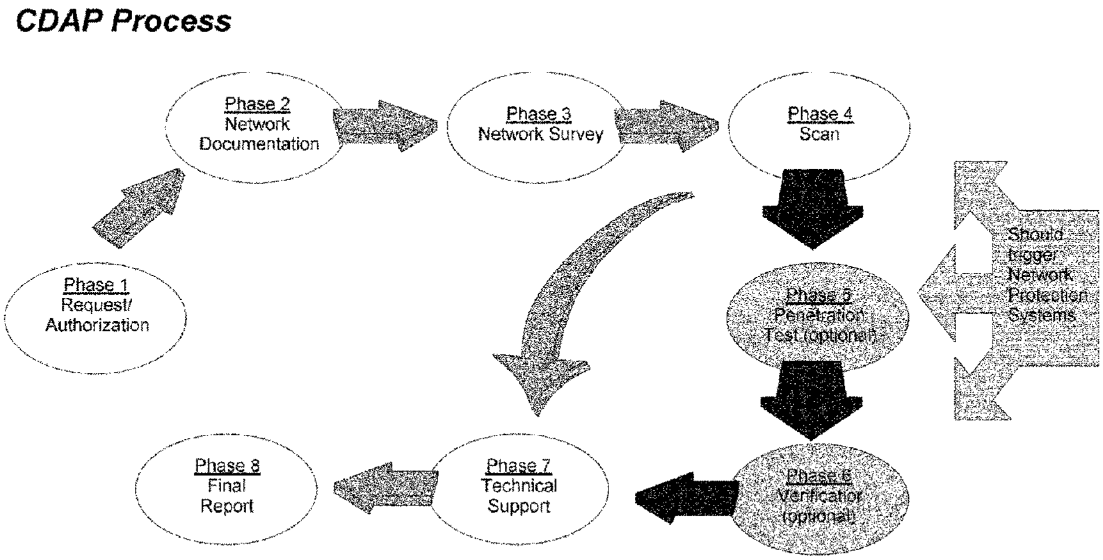


Figure G-1. Computer defense assistance program process

Legend for Figure G-1;
Black arrow: Authorized under AR 380–53 only.
Grey arrow: Covered under AR 380–19 only.

Glossary

Section I
Abbreviations

AA
administrative assistant

ACCLAIMS
Army COMSEC Commodity Logistics Accounting Information Management System

ADP
automated data processing

AIS
automated information system(s)

AISSP
Army information systems security program

AMC
Army Materiel Command

AMHS
Automated Message Handling System

AR
Army regulation

ARNGUS
Army National Guard of the U.S.

ARSTAF
Army Staff

ASA(RDA)
Assistant Secretary of the Army for Research, Development and Acquisition

AUTODIN
automatic digital network

BAS
Battlefield Automation Systems

C2
command and control

CCI
controlled cryptographic item

CDR USARCMD
Commander, United States Army Reserve Command

CG
commanding general

CI
counterintelligence

CID
criminal investigation division

CNG
Chief, National Guard Bureau

COMPUSEC
computer security

COMSEC
Communications Security

COOP
Continuity of Operations Plan

COTS
commercial off-the-shelf

CSTVRP
Computer Security Technical Vulnerability Reporting Program

CTTA
certified TEMPEST technical authority

DA
Department of the Army

DAA
designated approving authority

DAIG
Department of the Army Inspector General

DCI
Director of Central Intelligence

DCID
Director of Central Intelligence Directive

DCSINT
Deputy Chief of Staff for Intelligence

DCSLOG
Deputy Chief of Staff for Logistics

DCSOPS
Deputy Chief of Staff for Operations and Plans

DD
Department of Defense

DDN
Defense Data Network

DES
data encryption standard

DIA
Defense Intelligence Agency

DIAM
Defense Intelligence Agency manual

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

DMS
Defense Message System

DOD
Department of Defense

DSSCS
Defense Special Security Communications System

ECP
engineering change proposal

ESI
extra sensitive information

EUCI
Endorsed for Unclassified Cryptographic Item

FBI
Federal Bureau of Investigation

FIS
foreign intelligence service

FM
field manual

FOUO
For Official Use Only

FTA/RA
Facility TEMPEST Assessment/Risk Analysis

GSA
General Services Agency

HQDA
Headquarters, Department of the Army

IAA
Interconnected Accredited AIS

IAW
in accordance with

IM
information management

IMA
Information Mission Area

INSCOM
United States Army Intelligence and Security Command

IO
information operations

ISS
information systems security

ISSM
information systems security manager

ISSO
information systems security officer

ISSPM
information systems security program manager

JCS
Joint Chiefs of Staff

JROC
Joint Requirement Oversight Council

LAA
Limited Access Authorization

LAN
local area network

LRU
lowest replacement unit

MACOM
major command

MJCS
Memorandum, JCS

MOA
Memorandum of Agreement

MOU
Memorandum of Understanding

NATO
North Atlantic Treaty Organization

NCSC
National Computer Security Center

NISAC
National Information Security Assessment Center

NIST
National Institute of Standards and Technology

NSA
National Security Agency

NSA/CSS
National Security Agency/Central Security Services

OPSEC
operations security

PC
personal computer

PDS
protected distribution system

PEO
Program Executive Officer

PL
public law

PM
program manager;project manager;product manager

PMO
program management officer

PPL
Preferred Products List

PROM
programmable read only memory

RDTE
research, development, test and evaluation

SA
system administrator

SAEDA
Subversion and Espionage Directed Against the Army

SAP
Special Access Program

SCI
Sensitive Compartmented Information

SCIF
sensitive compartmented information facility

SF
standard form

SIGINT
Signal Intelligence

SOP
standing operating procedure

SSO
special security officer

STS
Single Trusted System

TASO
Terminal Area Security Officer

TCO
TEMPEST Control Officer

TDY
Temporary Duty (travel)

TRADOC
United States Army Training and Doctrine Command

TS
Top Secret

TS/SCI
Top Secret/Sensitive Compartmented Information

UCMJ
Uniform Code of Military Justice

USAR
United States Army Reserve

USC
United States Code

WAN
Wide Area Network

WWMCCS
Worldwide Military Command and Control System

Section II
Terms

Access
Ability and means to communicate with (that is, input to or receive output from), or otherwise make use of any information, resource, or component in an AIS. Capability and opportunity to gain knowledge or to alter information or material.

Access control
The process of limiting access to the resources of an AIS only to authorized users, programs, processes, or other systems.

Accountability
(AIS) Property that enables auditing of activities on an AIS to be traced to persons who may then be held responsible for their actions.

(COMSEC) Principle that an individual is responsible for safeguarding and controlling of COMSEC equipment, keying material, and information entrusted to his/her care and is answerable to proper authority for the loss or misuse of that equipment or information.

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

Accreditation authority
Synonymous with designated approving authority.

AIS security incident
An occurrence involving classified or SBU information being processed by an AIS where there may be a deviation from the requirements of the governing security regulations; a compromise or unauthorized disclosure of the information occurred or was possible; data or information integrity is in question (for example, unauthorized modification); or information was made unavailable for a period of time.

Approval to operate
A term which is synonymous with accreditation.

Army Information
Information originated by or concerning the U.S. Army.

Audit Review
The independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.

Audit trail
A chronological record of system activities to enable the reconstruction, reviewing and examination of the sequence of events and/or changes in an event.

Authenticate
To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to possible unauthorized modification in an automated

information system, or establish the validity of a transmitted message.

Authentication
Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Auto-manual system
Programmable, hand-held COMSEC equipment used to perform encoding and decoding functions.

Automated information systems
Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware. Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.

Automated information systems security
Synonymous with computer security.

Availability
The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

Category
Restrictive label that has been applied to both classified or unclassified data, thereby increasing the requirement for protection of, and restricting the access to, the data. Examples include sensitive compartmented information, proprietary information, and North Atlantic Treaty Organization information. Individuals are granted access to special category information only after being granted formal access authorization.

Central computer facility
One or more computers with their peripheral and storage units, central processing units, and communications equipment in a single controlled area. Central computer facilities are those areas where computer(s), other than personal computer(s), are housed to provide necessary environmental, physical, or other controls.

Certification
Comprehensive evaluation of the technical and nontechnical security features of an AIS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Classified defense information
Official information regarding the national security which has been designated top secret, secret, or confidential in accordance with Executive Order 12958.

Clearing
Removal of data from an AIS, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using normal system capabilities (that is, through the keyboard). An AIS need not be disconnected from any external network before clearing takes place. Clearing enables a product to be reused within, but not outside of, a secure facility. It does not produce a declassified product by itself, but may be the first step in the declassification process. See purge.

Commercial COMSEC Endorsement Program (CCEP)
Relationship between the National Security Agency and industry, in which the National Security Agency provides the COMSEC expertise (that is, standards, algorithms, evaluations, and guidance) and industry provides design, development, and production capabilities to produce a type 1 or type 2 product. Products developed under the Commercial COMSEC Endorsement Program may include modules, subsystems, equipment, systems, and ancillary devices.

Communications deception
Deliberate transmission, retransmission, or alteration of communications to mislead an adversary's interpretation of the communications.

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

Compartmented mode
AIS security mode of operation wherein each user with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts has all of the following:

a. Valid security clearance for the most restricted information processed in the system.

b. Formal access approval and signed nondisclosure agreements for that information to which a user is to have access.

c. Valid need-to-know for information to which a user is to have access.

Compromising emanations
Unintentional signals that, if intercepted and analyzed, would disclose the information transmitted, received, handled, or otherwise processed by telecommunications or automated information systems equipment (See TEMPEST).

Computer
A machine capable of accepting data, performing calculations on or otherwise manipulating those data, storing those data, and producing new data.

Computer facility
Physical resources that include structures or parts of structures that support or house computer resources. The physical area where the equipment is located.

Computer security
Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

Confidentiality
Assurance that information is not disclosed to unauthorized entities or processes.

Configuration control
Process of controlling modifications to a telecommunications or automated information systems hardware, firmware, software, and documentation to ensure the system is protected against improper modifications prior to, during, and after system implementation.

Controlled access protection
Log-in procedures, audit of security-relevant events, and resource isolation as prescribed for class C2 in the Orange Book.

Controlled cryptographic item
Secure telecommunications or information handling equipment, or associated cryptographic component, is unclassified but governed by a special set of control requirements. Such items are marked CONTROLLED CRYPTOGRAPHIC ITEM or, where space is limited, CCI.

Cryptographic
Pertaining to, or concerned with, cryptography.

Cryptographic equipment
Equipment that embodies a cryptographic logic.

Cryptography
Principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

Cryptology
The science and activities which deal with hidden, disguised, or encrypted communications.

Cryptosystem
Associated COMSEC items interacting to provide a single means of encryption or decryption.

Data security
Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Declassification (of magnetic storage media)
An administrative procedure resulting in a determination that classified information formerly stored on a magnetic medium has been removed or overwritten sufficiently to permit reuse in an unclassified environment.

Dedicated mode
AIS security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:

a. Valid security clearance for all information within the system.

b. Formal access approval and signed nondisclosure agreements for the information stored and/or processed (including all compartments, subcompartments, and/or special access programs).

c. Valid need-to-know for all information contained within the AIS.

When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

Degauss
Destroy information contained in magnetic media by subjecting that media to high-intensity alternating magnetic fields, following which the magnetic fields slowly decrease.

Denial of service
Result of any action or series of actions that prevents any part of a telecommunications or AIS from functioning.

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

DOD Trusted Computer System Evaluation Criteria
Document containing basic requirements and evaluation classes for assessing degrees of effectiveness of hardware and software security controls built into AIS. This document, DOD 5200.28 STD, is frequently referred to as the Orange Book.

Embedded cryptography
Cryptography which is engineered into an equipment or system the basic function of which is not cryptographic. Components comprising the cryptographic module are inside the equipment or system and share host device power and housing. The cryptographic function may be dispersed if identifiable as a separate module within the host.

Embedded (computer) system
Computer system that is an integral part of a larger system or subsystem that performs or controls a function, either in whole or in part.

Emission security
Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from cryptographic equipment, AIS, and telecommunications systems.

File server
Computer hardware used to provides storage user data and software applications and processing capabilities for user workstations and normally used for the connection and control for the workstations to the Local Area Network (LAN).

Firewall
A system or group of systems that enforces an access control policy between two networks with the properties of allowing only authorized traffic to pass between the networks from inside and outside the controlled environment and is immune to penetration.

Firmware
Software that is permanently stored in a hardware device which allows reading and executing the software, but not writing or modifying it.

Foreign national employees
Non-U.S. citizens who normally reside in the country where employed, though they may not be citizens of that country, and who are employed by the U.S. Government and the Department of the Army.

Formal access approval
Documented approval by a data owner to allow access to a particular category of information.

Information systems security (ISS)
The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. This regulation designates ISS as the security discipline which encompasses COMSEC, COMPUSEC, and control of compromising emanations (TEMPEST).

Integrity
The degree of protection for data from intentional or unintentional alteration or misuse.

Intelligence Information
Information collected and maintained in support of U.S. intelligence mission.

Key
Information (usually a sequence of random or pseudorandom binary digits) used initially to set up and periodically to change the operations performed in crypt-equipment for the purpose of encrypting or decrypting electronic signals, for determining electronic counter-measures patterns (for example, frequency hopping or spread spectrum), or for producing other key.

Key management
Process by which a key is generated, stored, protected, transferred, loaded, used, and destroyed.

Least Privilege
Principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. This also applies system privileges that might not be needed to perform their assigned job.

Note. Application of this principle limits the damage that can result from errors, accidental and unauthorized use of an AIS.

Machine cryptosystem
Cryptosystem in which the cryptographic processes are performed by crypt-equipment.

Mainframe
A computer system which is characterized by dedicated operators (beyond the system users); high capacity, distinct storage devices; special environmental considerations; and an identifiable computer room or complex.

Malicious software
Software that is intentionally introduced in a system to cause harm.

Manual cryptosystem
Cryptosystem in which the cryptographic processes are performed manually without the use of crypt-equipment or auto-manual devices.

Multilevel (security) mode
AIS security mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts:

a. Some users do not have a valid security clearance for all the information processed in the AIS.

b. All users have the proper security clearance and appropriate formal access approval for that information to which they have access.

c. All users have a valid need-to-know only for information to which they have access.

Multilevel security
Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances, but prevents users from obtaining access to information for which they lack authorization.

Need-to-know
Access to, or knowledge or possession of,

specific information required to carry out official duties.

Network
Communications medium and all components attached to that medium whose function is the transfer of information. Components may include AIS, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Noncommunications emitter
Any device which radiates electromagnetic energy for purposes other than communicating (for example, radars, navigational aids, and laser range finders). A noncommunication emitter may include features normally associated with computers, in which case it must also meet the requirements for an AIS.

Password
Protected/private character string used to authenticate an identity or to authorize access to data.

Personal Computer
A personal computer normally a small desktop type AIS which contains an operating system, software applications, firmware, and storage devices (fixed and removable features) with the capabilities of operating, processing, and storing information in a stand-alone mode. PCs can be connected to networks for access to other systems.

Note. The category of personal computers can include lap-tops, notebooks and workstations.

Personal E-Mail Account
An E-mail account acquired by an individual for personal use. Also know as a private account.

Private Account
See Personal E-Mail Account.

Protected distribution system (PDS)
Wireline or fiber-optic telecommunications system that includes terminals and adequate acoustic, electrical, electromagnetic, and physical safeguards to permit its use for the unencrypted transmission of classified information.

Purge
Removal of data from an AIS, its storage devices, or other peripheral devices with storage capacity in such a way that the data may not be reconstructed. An AIS must be disconnected from any external network before a purge. See clearing.

Remote terminal
A terminal which is not in the immediate vicinity of the AIS it accesses. This is usually associated with a mainframe environment and the use of a terminal. Terminals usually can not operate in a stand-alone mode.

Risk
The probability that a particular threat will exploit a particular vulnerability of an automated information system or telecommunications system.

Risk assessment
Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective measures.

Risk management
Process concerned with the identification, measurement, control, and minimization of security risks in information systems.

Security Guard/Filter
AIS trusted subsystem that enforces security policy on the data that pass through it.

Small computer
A small general purpose computer designed to support a single user at a time. Disk drives, printers, and other equipment associated with the small computer are considered part of the small computer and normally referred to as a personal computer. In addition to the above standard definition and the changing mission of the Army, the definition of a small computer has been enhanced so that a small computer or any PC or workstation that attaches to a Server via a LAN in a client server environment is considered to be a small computer.

Stand alone computer
An automated information system that is physically and electrically isolated from all other automated information systems.

Systems high (security) mode
AIS security mode of operation wherein each user, with direct or indirect access to the AIS, its peripherals, remote terminals, or remote hosts, has all of the following:

a. Valid security clearance for all information within an AIS.

b. Formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, subcompartments and/or special access programs).

c. Valid need-to-know for some of the information contained within the AIS.

Technical vulnerability
A hardware, firmware, communication, or software weakness which leaves a computer processing system open for potential exploitation or damage, either externally or internally, resulting in risk for the owner, user, or manager of the system.

Telecommunications
Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

Telecommunications and automated information systems (security)
Protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats and to ensure authenticity.

Note. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems that generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security material and technical security information.

Telecommunications system
Any system which transmits, receives, or otherwise communicates information by electrical, electromagnetic, electro-mechanical, or electro-optical means. A telecommunications system may include features normally associated with computers, in which case it must also meet the requirements for an AIS.

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

Terminal
Any device which is used to access an AIS, including ’dumb’ terminals, which only function to access another AIS, as well as personal computers or other sophisticated AIS which may access other AIS as one of their functions.

Threat
Capabilities, intentions, and attack methods of adversaries to exploit, damage, or alter or any circumstance or event with the potential to cause harm to information or an information system.

Threat agent
A means or method used to exploit a vulnerability in a system, operation, or facility.

Transmission security
The component of COMSEC which consists of all measures designed to protect transmissions from interception and exploitation by means other than cryptographic analysis.

Unclassified but sensitive (SBU) information
Unclassified information, that the loss misuse or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.

User
Person or process accessing an AIS by direct

connections (for example, via terminals) or indirect connections.

User ID
Unique symbol or character string that is used by an AIS to uniquely identify a specific user.

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

Vulnerability
Weakness in an information system, or cryptographic system, or components (for example, system security procedures, hardware design, internal controls) that could be exploited.

Section III
Special Abbreviations and Terms

This publication uses the following abbreviations, brevity codes, or acronyms not contained in AR 310–50. These special abbreviations include computer technology definitions.

ACCO
Army Case Control Office

ACERT
Army Computer Emergency Response Team

AISSRP
Army Information Systems Security Resources Program

AKMP
Army Key Management Program

ASSIST
automated systems security incident support team

ATD
advanced technology development

C2
command and control

C2W
command and control warfare

C4I
command, control, communications, computers, and intelligence

CAW
Certification Authority Workstation

CD
compact disk

CDAP
Computer Defense Association Program

CERT
computer emergency response team

CISS
center for information systems security

CM
configuration management

CSD
contractor support detachment

CSE
client server environment, contractor support element

DBA
data-base administrator

DBMS
data base management systems

DISA
Defense Information Systems Agency

DISA/CISS
Defense Information System Agency/Center for Information System Security

DSNET3
DOD Secure Network/3

DODIIS
Department of Defense Intelligence Information Systems

ETPL
endorsed TEMPEST product list

GCCS
Global Command and Control System

GOTS
Government off-the-shelf

IATO
interim approval to operate

INFOSEC
information security

ISSRP
information systems security resources program

IW
information warfare

JWICS
Joint Worldwide Intelligence Communication System

LIWA
Land Information Warfare Activity

MAN
metro area network

NACSIM
National Communications Security (COMSEC) Information Memorandum

NCSC-TG
National Computer Security Center-Technical Guidance

NID
network intrusion detection

NSAM
National Security Agency Manual

NSTISSAM
National Security Telecommunications and Information Systems Security Agency manual

NSTISSC
National Security Telecommunications and Information Systems Security Committee

Pam
pamphlet

PCMCIA
Personal Computer Memory Card International Association

ROM
read only memory

SAPI
Special Access Program for Intelligence

SBA
site-based accreditation

SBU
Sensitive But Unclassified

SCE
service cryptologic element

SCG
security classification guide

SII
statement of intelligence interest

SIMO
system integration management office

SIO
senior intelligence officer

SIOP–ESI
Single Integrated Operational Plan–Extra Sensitive Information

SIPRNET
secret internet protocol router network

SSA
system security administrator

SSBI
Single Scope Background Investigation

TAP
tactics, techniques, and procedures

TCB
trusted computing base

Index

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

MANAGEMENT CONTROL EVALUATION CERTIFICATION STATEMENT

For use of this form, see AR 11-2; the proponent agency is ASA(FM).

1. REGULATION NUMBER

2. DATE OF REGULATION

3. ASSESSABLE UNIT

4. FUNCTION

5. METHOD OF EVALUATION *(Check one)*

□ a. CHECKLIST

APPENDIX *(Enter appropriate letter)*

□ b. ALTERNATIVE METHOD *(Indicate method)*

6. EVALUATION CONDUCTED BY

a. NAME *(Last, First, MI)*

b. DATE OF EVALUATION

7. REMARKS *(Continue on reverse or use additional sheets of plain paper)*

8. CERTIFICATION

I certify that the key management controls in this function have been evaluated in accordance with provisions of AR 11-2, Management Control . I also certify that corrective action has been initiated to resolve any deficiencies detected. These deficiencies and corrective actions *(if any)* are described above or in attached documentation. This certification statement and any supporting documentation will be retained on file subject to audit/inspection until superseded by a subsequent management control evaluation.

a. ACCESSABLE UNIT MANAGER

(1) TYPED NAME AND TITLE

(2) SIGNATURE

b. DATE CERTIFIED

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.45

PIN:	049400–000
DATE:	06-15-98
TIME:	15:07:16
PAGES SET:	47

DATA FILE:	ar380-19.fil
DOCUMENT:	AR 380–19
DOC STATUS:	REVISION