[**AR 380-19 Information Systems Security**](http://www.fas.org/irp/doddir/army/ar380-19/toc.htm)

**Chapter 2 - Computer Security**

**Section 1 General Policy**

**2-1. Overview**

a. This chapter addresses ISS requirements which apply uniquely to AIS. Security policy for an AIS will be defined at the beginning of concept development. Security requirements based on this policy will be considered throughout the life cycle. A DAA will be responsible for the overall security of each AIS.

b. The AIS developer must ensure the early and continuous involvement of the PEO, PM, the functional proponent, users, ISSOs, data owners, and DAAs in defining and implementing security requirements of the AIS. There will be a security plan for AIS processing classified and unclassified-sensitive information showing the steps planned to comply fully with stated security requirements.

c. Statements of safeguard 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 from DOD 5200.28-STD. No classified or unclassified-sensitive data will be introduced into an AIS without designating its classification and sensitivity. The data owner will approve entering the data where applicable.

**2-2. System sensitivity designation and mode of operation**

1. AIS will be designated, based on the highest classification or sensitivity of data processed, as follows:

(1) Classified sensitive 1 (CS1). The AIS processes any amount of SCI or SIOP-ESI.

(2) Classified sensitive 2 (CS2). The AIS processes any data which bears a security classification of top secret.

(3) Classified sensitive 3 (CS3). The AIS processes any data which bears a security classification of secret or confidential.

(4) Unclassified-sensitive 1 (US1). The AIS processes US1 data described in paragraph 1-5c(1).

(5) Unclassified-sensitive 2 (US2). The AIS processes US2 data described in paragraph 1-5c(2).

(6) Non-sensitive-In rare cases, Army AIS may be categorized as non-sensitive provided they do not fall in any of the above categories. Such a determination must be approved by the appropriate DAA who would otherwise accredit unclassified-sensitive AIS.

(7) AIS that process any data controlled under the caveat "Warning Notice-Intelligence Sources or Methods Involved (WNINTEL)," regardless of security classification, must be identified to meet reporting requirements contained in paragraph 3-9e. These systems will have an additional identifier associated with the applicable sensitivity designation above; for example. CS1-WNINTEL, CS2-WNINTEL, and so forth.

b. The security processing mode of an AIS will be determined based on the classification or sensitivity and formal categories of data and the clearance, access approval, and need-to-know of the users of the system. Formal categories of data are those for which a written approval must be issued before access (for example, SCI compartments, NATO information, or special access programs). 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 of the AIS possess the required personnel security clearance or authorization, formal access approval (if required), and need-to-know for all data handled by the AIS.

(2) Systems high security mode. A mode of operation wherein all users of the AIS possess the required personnel security clearance or authorization, but not necessarily a need-to-know, for all data handled by the AIS. If the AIS processes formal categories of information, all users must have formal access approval.

(3) Partitioned security mode. A mode of operation wherein all users of the AIS possess the required personnel security clearance or authorization, but not necessarily formal access approval and need-to-know, for all information handled by the AIS. For systems designated as CSI, this mode is equivalent to the compartmented mode defined in Director, Central Intelligence Directive (DCID) 1/16.

(4) Multilevel security mode. A mode of operation wherein not all users of the AIS possess the required personnel security clearance for all data being processed by the AIS.

(5) Controlled security mode. The controlled mode is no longer authorized. Systems accredited previously in the controlled mode will be considered to be in the multilevel mode if they continue to operate with users who are not cleared for all data processed on the system. These systems do not need to be reaccredited solely because of this change in mode of operation, provided they were accredited under prior versions of this regulation, and the system meets the security requirements previously detailed for the controlled mode. However, when these systems become due for reaccreditation, they will be accredited to operate in one of the above security modes.

c. When determining the security processing mode, consider only the classification and formal categories of data on the AIS and the clearance, authorization, and need-to-know of all users. If the system is properly sanitized between periods of processing, these factors may be considered independently for each period involved.

**2-3. Minimum requirements**

a. All AIS processing classified or unclassified-sensitive 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 the risk analysis.

(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 glossary), an audit trail will provide a documented history of AIS use. The audit trail will be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise 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. 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 device having access to the AIS.

(b) The 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, the changing of security levels, or categories of information.

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

(3) Security training and awareness. All persons accessing an AIS will be part of a 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 of this regulation will be covered.

(4) Physical controls. AIS hardware, software, documentation, and all classified and unclassified-sensitive data handled by the AIS will be protected to prevent unauthorized (intentional or unintentional) disclosure, destruction, or modification. 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 if that software will be used for handling classified or unclassified-sensitive data.

(5) Marking. Marking on classified and unclassified-sensitive output will reflect the sensitivity of the information as required by existing directives. For example, AR 380-5 contains requirements for security classification and applicable markings for classified information, and AR 340-17 governs "for official use only" information. The markings will be applied through either an automated means (that is, the AIS has a feature that produces the markings) or manual procedure. 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 security class B1, as specified in DOD 5200.28-STD. If B1 is not met, but automated controls are used, all classified output will be protected at the highest classification level 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 caveats. All media will be marked and protected commensurate with the requirements for the highest security classification level and 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 all the information he or she is entitled to (by virtue of clearance and formal access approval), but no more. In the case of need-to-know for classified information, access must be essential to accomplish lawful and authorized Government purposes.

(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, and need-to-know as appropriate.

(8) Data integrity. There will be appropriate safeguards in place to detect and minimize inadvertent or malicious modification or destruction of data.

(9) Contingency planning. A contingency plan will be developed so that if data is modified or destroyed unexpected, recovery procedures are available.

(10) Accreditation. Before operation, each AIS will be accredited under a set of security safeguards approved by the DAA. See chapter 3 for additional information.

(11) Risk management. A risk management program will be put in place to determine how much protection is required, how much exists, and the most economical way of providing the needed protection. See chapter 5.

(12) Security planning. An AIS security plan will be developed and maintained for the life of the AIS. The security plan evolves into the accreditation document. See appendix C for format.

b. In addition to the requirements above, AIS operating in other than the dedicated security mode must provide security features which meet the trusted system class from DOD 5200.28-STD as determined by the procedures in appendix B. The following instructions for implementation of these provisions apply:

(1) All AIS that process or handle classified or unclassified-sensitive information and that require at least Controlled Access Protection (that is, class C2 security protection), based on the procedure described in appendix B, will implement required security features by Dec 31, 1992.

(2) If the procedures in appendix B require a trusted systems class above class C2, a timetable for meeting this requirement will be determined individually for each system. This timetable will be part of the accreditation, and the DAA will approve it.

(3) These requirements will be met either by using trusted computer products listed on the NCSC's Evaluated Products List (EPL), using a product not on the EPL 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 the requirements in DOD 5200.28-STD are met.

(4) There are cases where introduction of additional computer-based security features according to the schedule given in 2-3b(1) and (2) (for an existing AIS or an AIS under development) may be prohibitively expensive, time-consuming, unsound technically, or may adversely affect operational effectiveness to an unacceptable degree. In such cases, the following will apply:

(a) Other safeguards (for example, physical controls or administrative controls) may be substituted as long as the necessary level of system security or protection, as determined by the accreditation authority, is attained.

(b) Only MACOM commanders or the AA to the Secretary of the Army (acting as the MACOM commander for all HQDA activities) may authorize exceptions. Such authorizations will be based on a written determination that one or more of the conditions in 2-3b(4) exists. Exceptions will be reviewed during each reaccreditation.

**Section II
Software Security**

**2-4. Software controls**

a. Safeguards implemented in software will protect against compromise, subversion, or unauthorized manipulation.

b. Only software that has been specifically developed or approved for use, or has been purchased or leased by an authorized U.S. Government representative, will be used with Army AIS.

c. Army activities that operate or propose to operate a central database of executable software (to include public domain software or shareware) for other Army activities to use must have approval from their parent MACOM or MACOM designee. Requests must include a description of countermeasures employed to reduce the risk of introducing malicious software. Public domain, shareware, or other privately purchased software (whether obtained from an approved database or from another source) will not be used on Army AIS unless approved locally under AR 25-1, paragraph 2-7.

d. Each Army AIS will include an identified set of executable software that is authorized to be run on that AIS. Such software will be protected from authorized modification to the maximum extent possible by the hardware and software mechanisms of the AIS. To the extent that the risk analysis reveals the AIS to be vulnerable to attacks from malicious software, additional measures such as checksums, commercial "anti-rival" programs, and cryptographic seals will be employed to ensure the integrity of the software.

e. Valid documentation will support software used by programming, operations, and user personnel. Only personnel performing official duties should be allowed access to this documentation.

f. Upon acceptance for operational use, whether after development for a specific application or purchased "off-the-shelf," 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.

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

**2-5. Database management systems**

a. Protecting shared databases is essential, as they present a significant asset and frequently reveal considerably more information taken as a whole than can be obtained from their individual parts. Commercial database management systems have different characteristics affecting their security stability that must be considered when acquiring a system for handling classified or unclassified-sensitive information. Generally, they are as follows:

(1) Database access and manipulation methodology.

(2) Database integrity.

(3) Save, recovery, and restart.

(4) Audit mechanisms and utilities.

b. When database management systems are used with classified defense information, the lowest identifiable element with a unique classification within the database must be protected according to its security classification. If the database cannot provide field protection, then it should provide record protection. For database systems which do not provide protection at the record or field level, operation of the system will be restricted to the dedicated security mode.

c. Database 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 integrity of the automated system and the data contained therein.

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

**2-6. Software security packages**

a. Software security packages are available from various commercial vendors. Many of these packages have been evaluated, or are currently being evaluated, by the NCSC. Products other than those evaluated by the NCSC and included on the EPL may be used; however, such products should be used only with a valid justification (for example, cost, required functionality not available on the list, or a similar reason) for using non-evaluated products.

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

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

d. For products not listed on the EPL, HQDA (SAIS-ADS) must approve purchase or annual lease costs that exceed $50,000.

**2-7. Software design and test**

a. Examination of the control over the procedures used to develop computer programs will be 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.

b. 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.

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

**Section III
Hardware Security**

**2-8. Hardware-based security controls**

a. Hardware resident architecture features are important to total AIS security. Depending upon the age, sophistication, and design of the system, hardware-based security controls represent an important factor when evaluating the security environment of any Army system. Conversely, 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 as well as software 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 processed if they in any way access this data during their maintenance operations.

b. Maintenance personnel who do not access classified data during their maintenance operations should nevertheless be cleared for the highest level of data processed on the system. However, if this is not economically or otherwise feasible, maintenance personnel will be observed during their maintenance operations by individuals with the technical expertise to detect obvious unauthorized modifications.

c. Non-U.S. citizens will not perform maintenance on CSI or CS2 accredited AIS or on AIS which 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 ISSO.

**Section IV
Physical Security**

**2-10. Security objectives and safeguards**

a. A balanced AIS security program must include a firm physical security information. The objectives are to-

(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 which 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. Buildings which house AIS, computer rooms, and related sensitive areas may be designated as restricted areas, mission essential, or vulnerable areas under AR 190-13. Mainframe facilities 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.

d. Facilities housing systems processing SCI material (CS1) will be subject to the provisions in Defense Intelligence Agency Manual (DIAM) 50-3.

e. For facilities (CS2 and CS3) where both the routine processing and discussion of sensitive top secret or secret information (as defined in AR 381-14) take place, the provisions of AR 381-14 will apply fully to the facility.

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

g. The number and diversity of Army AIS 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, local criminal and intelligence threat, and the value of the automated equipment.

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

i. Physical and 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) which support or affect the overall operation.

j. 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. Location and construction standards of a central computer complex**

Site selection is a key factor in the establishment and maintenance of a secure operating environment. Ideally, any location selected to house an automated system would support an effective physical security system. Architectural design is an equally important aspect of the site selection and security relationship. Physical provisions for restricting access should be incorporated into the initial design. While it is not practical to establish firm Army-wide standards governing the location of such systems, the factors below will be considered and will be implemented in the site selection process when appropriate and feasible.

a. Below-ground-level installations or other locations subject to flooding require special design features.

b. Buildings constructed or selected must be made of noncombustible materials (for example, brick, hardened poured concrete, or cement block and steel).

c. Ground floor windows should be kept to a minimum because of their vulnerability to forcible entry. These windows will be covered with grills, steel screens, secure shutters, or other similar protective material.

d. Locating the equipment room in the center of the building is highly desirable to obtain maximum protection from the building. A location that is easily accessible to the public should be avoided to minimize the exposure from such traffic. The environment immediately above, below, and adjacent to the facility must also be considered.

e. Protection (including fire protection) for media libraries, data preparation areas, and environmental support equipment must also be considered in site selection and complex design.

f. All doors to the computer complex will be substantially constructed of solid core wood or metal, have a 1 and 1/2 hour fire rating, and be designed to complement the security provided by the exterior walls of the complex. Hinges will be mounted on the inside; or, if this is not possible, the hinge pins must be welded, pinned, or brazed to hinder removal. Computer complex doors, other than doors used for primary access, will be secured from the inside at all times and devoid of external locking hardware. These doors will be equipped with appropriate hardware to permit rapid opening during fires or other emergencies.

**2-12. Mainframe computer equipment room standards**

a. The room which will house mainframe computer equipment will have four solid, windowless walls which extend from true floor to true ceiling.

b. All unnecessary openings into the computer equipment room will be sealed with a fire-rated material. Other openings, such as heating and cooling vents or ducts already installed, will be protected by mechanical fire and smoke dampers. Openings made for cables will be protected by a sealant that maintains the appropriate fire rating of the wall.

c. All doors to the equipment room will be solid core or metal clad, windowless, have the appropriate underwriter's laboratory fire rating based on the character and location of the wall, and be equipped with a deadbolt having a 1-inch throw. These doors must also be equipped with heavy-duty pneumatic door closers.

d. Appropriate security controls will be implemented during operational hours to assure that only authorized persons are permitted to enter the computer room and supporting offices. This may be achieved by using one or more of the following: physical barriers (which include counters), locked doors equipped with electrical release or cipher lock, or a receptionist. A badge system may supplement one of the above methods. When structurally feasible, a buffer or control zone will be created immediately outside of the primary entrance to the equipment room. Use of secondary entrances or emergency exits will be strictly controlled and monitored.

e. All computer rooms and support facilities will be secured at the end of the duty day or any other time the facilities are unoccupied, such as during a fire drill, bomb threat, and so forth. Although more stringent requirements may be in effect as dictated by the sensitivity level or separate security regulations (AR 380-5, AR 381-14, and DIAM 50-3), computer facilities designated as "mission essential or vulnerable areas" will have all entrances protected by a minimum of two independent barriers or other security systems. In addition to locked doors to the computer room (or building, if automated systems are housed in a dedicated building), any one of the following measures may be used to provide the required dual level of protection:

(1) Second access doors, separated from the first, which can be securely locked.

(2) A chain-link fence external to the computer facility, the entrances to which can be securely locked. Exterior lighting will be installed to complement the protection provided by the fencing.

(3) For sites where the installation of second access doors or fencing is deemed impractical, any one or more of the additional protective measures listed in paragraph 2-12f may be substituted when authorized in writing and included in the site's accreditation document.

f. Should circumstances warrant a higher degree of protection than that required above, implementation of one or more of the following is recommended:

(1) Dedicated guard service.

(2) Continuous access monitoring by closed-circuit television.

(3) Intrusion detection systems.

(4) Exterior lighting for use during hours of darkness.

g. Appropriate measures will be implemented at each site to control visitor access to sensitive areas within the complex. This restriction includes equipment maintenance personnel and other individuals not directly involved with the operations of the facility. However, different procedures and restrictions will be required for various categories of visitors. All visits by non-U.S. citizens and others whose identities are not known to the commander or manager will be coordinated with the cognizant command security manager. A visitor control log will contain the identity of all persons granted access to the computer room (including vendor and maintenance personnel). This log will be retained for 90 days. h. Key and lock control will be per AR 190-51, appendix C.

**2-13. Physical security standards for small computers and other automated information systems**

a. There are many AIS that are not mainframe computers and clearly do not warrant the physical protection detailed in paragraphs 2-11 and 2-12 of this regulation. These include small computers as well as other AIS where the computing environment is essentially superimposed within the work environment. Whether or not to apply 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 of this paragraph will be followed.

b. Extravagant and costly security items such as alarms or secure rooms are usually not cost-effective for other than mainframe computers and, depending on the local threats, usually are not needed. Physical security requirements must be considered and selected based on the sensitivity of the data protected.

c. Equipment will be protected as follows:

(1) AIS that have nonremovable media upon which classified files reside must be stored in an area or container approved for safekeeping of classified information per AR 380-5.

(2) AIS that do not have classified files on nonremovable media should be in a locked office or building during nonduty hours, or otherwise secured to prevent loss or damage. Users will log off the computer when they leave the area.

**Section V
Procedural Security**

**2-14. 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 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's adversely affecting the entire system operation. Checks and balances will be established so that deviations from assigned duties can be detected.

(2) The ISSO must report directly to the responsible manager of the AIS on security-related matters. The ISSO should be positioned organizationally so that he or she does not have 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 confidential AR 380-19-1, a new Facility TEMPEST Assessment/Risk Analysis will be processed.

(4) 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.

**2-15. Password control**

a. User identification and password systems support the minimum requirements of accountability, access control, least privilege, and date integrity contained in paragraph 2-3a of this regulation. These mechanisms, while not always appropriate for stand-alone small systems or other systems operating in the dedicated mode, are often the most cost-effective and efficient methods of achieving these minimum security requirements. Other techniques (for example, biometric access control devices or smart cards) are increasingly providing practical alternatives for use in conjunction with, or in place of, password systems.

b. Due to the volume of information that may be exposed, the potential value of passwords to foreign intelligence or other unauthorized users usually far exceeds that normally assigned to safe combinations used to protect information of equivalent classification.

c. The ISSO oversees generation, issuance, and control of all passwords. Users will not have any control over choosing their passwords, unless such a choice is from one or more randomly generated by the system. The TASO may assist in issuing passwords in his or her respective area. All passwords must be generated and installed on the system by the ISSO, ISSO-approved assistants, or ISSO-approved software.

d. All passwords should be generated by random generator software and must not be obtained from commonly used words or phrases.

e. After generation, passwords will normally 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 classified according to the level of system access the user is authorized to have and the terminal from which the activity is initiated. Knowledge of individual passwords will be limited to a minimum number of persons and passwords will not be shared. Passwords will be issued only if the user has authorization to access the system and perform required functions.

f. Method of password distribution will be appropriate to the level of the data that they protect.

g. At the time of password issuance, individual users will be briefed on-

(1) Password classification and exclusiveness.

(2) Measures to safeguard classified and unclassified passwords.

(3) The prohibition against disclosure to other personnel. This applies even though they may be assigned to the same project and hold identical clearances.

(4) The requirement to inform a TASO or the ISSO immediately of password misuse or other potentially dangerous practices.

h. 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 function for which the password was required. Passwords, as unique identifiers of individual authority and privilege, must not be allowed to migrate between individuals even though those individuals are employed on the same project.

i. Passwords on systems designated as "Classified Sensitive" will be changed at least semiannually. Passwords on all other systems will be changed at least annually.

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

k. Passwords must be generated with, as a minimum, five-character strings using the 36 alphabetic-numeric characters, or six-character strings using only alphabetic characters.

**Section VI
Personnel Security**

**2-16. Training and awareness program**

All personnel who manage, design, develop, maintain, or operate AIS will undergo a training and awareness program consisting of-

a. An initial security training and awareness briefing for AIS managers and users. This briefing can use training material governing ISS in general, but must also be tailored to the systems the employee will be managing or using. The briefing will cover, as a minimum-

(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 associated with the system security.

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

(5) Physical and environmental considerations 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-

(1) Self-placed or formal instruction.

(2) Security education bulletins.

(3) Security posters.

(4) Training films and tapes.

(5) Computer-aided instruction.

**2-17. Personnel security standards**

a. Personnel who require access to classified defense information because of their duties with an AIS will possess a security clearance based on the appropriate investigation per AR 380-67.

b. Civilian, military, consultant, and contractor personnel meeting the requirements of an automatic data processing (ADP) I, II, or III position (see AR 380-67, app K) will, as a minimum, be submitted for a security investigation as listed below. Unless other requirements apply, such as the need to access classified or sensitive material, the investigation need not be completed before the individual is placed in an ADP position.

(1) ADP-I. Background investigation or Special Background Investigation.

(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. Civilian positions will, as a minimum, be designated as critical-sensitive for ADP-I, noncritical-sensitive for ADP II, and non-sensitive for ADP III per AR 380-67, paragraph 3-101.

d. The provisions of 2-17b and c apply to personnel who occupy such positions, regardless of whether or not the information processed by the AIS is classified.

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 AR 380-67, to include suspension from duties (see AR 380-67, para 8-102) as appropriate. Suspensions or other more permanent adverse actions will be based on the normal security clearance determination process contained in AR 380-67.

f. Additional guidance for personnel managing, supervising and occupying ADP I, II, and III positions are found is AR 380-67, chapter 9.

**2-18. Foreign national employees**

a. Using foreign national employees in positions that have access to AIS is discouraged. However, when theater manpower ceilings or other factors necessitate this practice, requirements in this paragraph apply.

b. AR 380-67, paragraph 3-608, requires certain pre-employment checks of prospective foreign nationals who will not require access to classified information to perform their duties. Before employment, or as soon as possible thereafter, 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 that will afford access to classified defense information except in extremely rare circumstances 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 United States personnel. Access must be limited to that described in the approved LAA, and the foreign national must be supervised at all times by appropriately cleared United States 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. LAAs always will be kept to the minimum, consistent with mission requirements, and will be terminated when no longer required.

**Section VII
Automated Information System Media**

**2-19. Protection requirements**

a. For the purpose of this section, AIS media consist of any substance or material on which information is represented or stored, used for input or output to an AIS or as an integral part of the AIS.

b. Classified AIS media must be protected according to AR 380-5 unless properly declassified or destroyed under this regulation, or approved declassification or destruction procedures from the NCSC.

c. AIS printer ribbons must be controlled and destroyed according to AR 380-5, paragraph 5-201c.

**2-20. Labeling and marking media**

a. All classified media that are not integral parts of the AIS will be marked or labeled according to the highest classification of the data contained thereon. This includes integral AIS components when they are removed for repair or exchange. For non-paper media, Standard Form (SF) 706 (Top Secret), 707 (Secret), or 708 (Confidential) will be used for this purpose. SCI media will have two labels affixed, SF 712 (Classified SCI) and a completed SF 711 (Data Descriptor). The completed SF 711 will indicate the security classification of the data.

b. Unclassified media that contain data representations that cannot be read by the human eye will be labeled "unclassified" when stored, transmitted, or otherwise intermingled with classified media. SF 710 (Unclassified) will be used for this purpose. SF 710 is not required in a totally unclassified environment.

c. Punched cards and printouts will be marked as required in AR 380-5, Chapter 4.

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

**2-21. Clearing, purging, declassifying, and destroying media**

a. Clearing of media means erasing or overwriting all information on the media, but 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 of media means to erase or overwrite totally and unequivocally any and all information stored on the media (that is, all storage locations). 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 unauthorized personnel; for example, for maintenance operations. Tables 2-1 and 2-2 list approved clearing and purging techniques.

|  |
| --- |
| Table 2-1Memory clear and purge methods  |
| **Media**  | **Clear**  | **Purge**  |
| Magnetic Bubble Memory  | 2  | 1 or 2  |
| Magnetic Core Memory  | 2  | 1 or 4  |
| Magnetic Plated Wire  | 2  | 3 and 5  |
| Magnetic-Resistive Memory  | 2  | X  |
| Read-Only Memory (ROM)  | X  | X  |
| Random Access Memory (Volatile)  | 2 or 7  | 4 or 7, and 6  |
| Programmable Read-Only Memory (PROM)  | X  | X  |
| Erasable PROM  | 8  | 9, then 3, and 6  |
| Electrically Alterable PROM  | 10  | 10, then 3, and 6  |
| Electrically Erasable PROM  | 11  | 11, then 3, and 6  |

Legend:
1. Degauss with a Type I degausser.
2. Overwrite all locations with any character.
3. Overwrite all locations with random characters.
4. Overwrite all locations with a character, its complement, then with a random character.
5. Purge not authorized if data resided in same location for more than 72 hours; purge not complete until overwrite has resided as long as classified data resided.
6. If CS1 data is involved, check with the ISSO or SSO to see if additional procedures are required.
7. Perform a power on/off cycle; not authorized for purge if classified data resided undistributed in the same location for more than 27 hours.
8. Perform an ultraviolet erase according to manufacturer's recommendation.
9. Perform 8 above, but increase time requirements by factor of three.
10. Pulse all gates.
11. Perform a full chip erase (see manufacturer's data sheet for procedure).
X. Not authorized/possible.

|  |
| --- |
| Table 2-2Secondary storage clear and purge methods |
| **Media**  | **Clear**  | **Purge**  |
| Magnetic Tape:  |
| Type  | 1 or 2  | 1 or 2  |
| Type II  | 1 or 2  | 2  |
| Type III  | 1 or 2  | X  |
| Magnetic Disks:  |
| Floppies or other "soft" disk technology  | Any numbered note.  | 1 or 2  |
| Hard disks-removable or non-removable  | Any numbered note.  | 1 or 2 or 4  |
| Magneto-optic Disks:  |
| Read Only  | X  | X  |
| Write Once, Read Many (WORM)  | X  | X  |
| Read Many, Write Many  | 3  | X  |

Legend:

1. Degauss with a Type I degausser.
2. Degauss with a Type II degausser.
3. Overwrite all locations with any character.
4. Overwrite all locations with a character, its complement, then with a random character.
X. Not authorized/possible

b. There are some inherent risks involved with declassifying media. For example-

(1) Magnetic media that have been stored for extended periods or in high-temperature conditions (120 degrees Fahrenheit or greater) become more difficult to erase completely.

(2) Overwrite procedures may be affected by equipment failures or an inability to overwrite bad sections of the media. Inter-record gaps created by the formatting process may not be overwritten unless the process is continuous.

(3) If the media are released outside a controlled environment, sophisticated signal recovery techniques could be employed in an attempt to recover data.

c. The decision to declassify media will be made only after comparing the inherent risks in 2-21b with the financial or operational benefit of media declassification. For example, even though floppy disks are listed in table 2-2, destruction is normally more appropriate than declassification and reuse, given the low cost of the media.

d. Media can be declassified only after purging. The appropriate ISSO must verify that the technique chosen for the purge meets the requirements of table 2-1 or 2-2. Additionally, the ISSO must establish a method to verify periodically, through at least a random sampling, the results of the purge.

e. Degaussing, as used in this paragraph and tables 2-1 and 2-2, refers to the proper use of equipment approved by the NSA and placed on its Degausser Products List, a portion of the Information Systems Security Products and Services Catalogue. Personnel who need to obtain such degaussers will consult the list, or determine the necessary information, through their information systems security management structure. Some listed products may be used only to degauss magnetic media that have coercivity no greater than 350 oersteds (also known as Type I media), while others are approved for media that have coercivity no greater than 750 oersteds (also known as Type II media). Certain tape media have coercivity greater than 750 oersteds (also known as Type III media) and cannot, at this time, be completely degaussed.

f. AR-380-5, chapter 9 and appendix K govern destruction or AIS media.

**2-22. Nonremovable storage media**

a. Using an AIS with nonremovable, nonvolatile media for processing classified information in 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, appendix H, 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 paragraph 2-21 during all periods when not attended by properly cleared individuals.

b. If the conditions of 2-22a are not met, and the DAA elects to approve the user of nonremovable, nonvolatile media on AIS processing classified information, specific countermeasures must be implemented to ensure that classified information is not written on such media (for example, after installing unclassified system data, rendering the nonremovable media "read-only," or artificially filling the device to capacity). 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 nonremovable media of its files.

**Section VIII
Network Security**

**2-23. Two views of a network**

a. The provisions of this regulation are applicable to networks, that 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 in which the network is treated as an interconnection of separately created, managed, and accredited AIS. IAA consist 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 and have not been accredited.

(2) The single trusted system (STS) view in which the network is accredited as a single entity by one DAA. The STS view is virtually always appropriate for local area networks, but can also be applicable to wide-area networks where a single agency or official is responsible.

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, Defense Communications Agency, that has overall control and publishes security parameters for use of the Defense Data Network (DDN)). However, a central focal point cannot always be identified (for example, when public carriers are utilized). In this latter case, the individual AIS DAA must establish procedures to protect the data contained in the AIS, and to ensure only authorized data is transmitted on the IAA network.

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

(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. In those cases where standard procedures for connecting to the network have been defined by a network DAA, these procedures (coupled with the approval of the network DAA to connect) will serve as the memorandum of understanding.

(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) is authorized, but only non-sensitive data may be transmitted to and from such AIS.

(7) National Computer Security Center-Technical Guideline-005 (NCSC-TG-005) contains additional restrictions that apply to connecting AIS to an IAA when the AIS is accredited in the multilevel or partitioned mode.

c. The following security provisions are applicable to the STS view network:

(1) The STS view 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. Minimum requirements of paragraph 2-3 are fully applicable, including the minimum trusted class requirement, if the network operates in other than the dedicated mode. NCSC-TG-005, Part I, 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. These are-

(a) Communications integrity, including authentication capability, field integrity, and ability of the network to enforce nonrepudiation of a message.

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

(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 2-23c(2) can only be addressed in a subjective manner, and may not be applicable or desirable in all situations. Nevertheless, NSOs 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**

**2-24. 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. A remotely accessed computer system must possess features to identify users and substantiate their identifications. The system will contain features that positively identify users before processing. For dial-up systems, a call-back identification mechanism is preferable.

c. Safeguards will be implemented to ensure that only authorized persons use remote terminal equipment. Exercise care so only authorized persons receive and remove sensitive hard copy output from the terminal 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. A remote terminal that accesses a system containing classified information 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 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 recording of an audit trail record for the ISSO to use. The 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 terminal must remain active 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 final.

e. Systems that process classified or unclassified-sensitive information will limit the number user log-on attempts to three before access by that user is inhibited. Users will not be reinstated until the ISSO or his or her designee has verified the reason for failed log-ons.

**2-25. Employee-owned and off-site processing**

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

b. AR 25-1, chapter 5, also contains policy on approval to use computers, employee-owned or government-owned, for off-site processing. Additional security policy is contained in paragraph 2-27 of this regulation.

**2-26. Tactical or battlefield automation systems (BAS)**

a. Although BAS often have unique purposes, the provisions of this regulation must nevertheless be applied. When one or more of the minimum security requirement from paragraph 2-3 are impractical because the function or design of the BAS is special purpose (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 describe how that particular requirement is not applicable and does not present an unacceptable risk to the information. Embedded systems that is, those that are part of a larger entity, are not easily removed and have no users), are exempt from the requirements of paragraph 2-3b.

b. BAS will normally be addressed by a generic accreditation. (See chap 3.)

c. BAS which also function as peacetime systems must fully comply with this regulation, and 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) Measures enforced to enhance security during transportation of the BAS.

(2) Mechanisms available to render the BAS inoperable in case of imminent capture. Methods of destroying classified information (both in hard copy and on AIS media) must be developed.

**2-27. Laptop or portable automated information systems**

a. Laptop computers, or any other computers that are designed to allow periodic relocation, must be accredited according to chapter 3 by the appropriate DAA. The grouping of numerous computers in a single accreditation document is acceptable. The accreditation must address all aspects of security and must specifically indicate the approved processing locations (in general terms such as "work site," "residence," "TDY location," and so forth), any authorized connectivity, and the extent to which processing of classified or unclassified-sensitive data is permitted. In no case will classified processing be authorized at any other than U.S. Government- or U.S. contractor-approved locations. AR 380-5, paragraph 5-200 contains stringent prohibitions concerning removal of classified information from designated work areas.

b. If the accreditation document so provides, classified processing may be done on laptop computers if it occurs in normal work areas otherwise acceptable for the storage, preparations, 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 (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 in an approved storage area when left unattended. The provisions of paragraph 2-22 also apply to configurations that include nonremovable media.

d. Accreditations for laptop 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 requirements must be addressed for the normal work location. When approval has been granted to process classified information at a temporary location for longer than 90 days. TEMPEST requirements for that location will apply.

e. Personnel will not be allowed to enter and exit sensitive compartmented information facilities with laptop or other portable computers unless a specific exception has been granted by Headquarters, U.S. Army Special Security Group according to their guidelines.

**2-28. Automated information system security incidents**

a. AIS security incidents will be investigated to determine their cause, and cost-effective action will be taken to prevent recurrences. Suspected or actual incidents will be reported to the appropriate ISSO, who will notify the ISSM and initiate an investigation. If appropriate, preliminary inquiry under AR 380-5 and AR 15-16 will be initiated. If there is any indication of foreign intelligence involvement, the incident must be reported to the supporting counterintelligence office per AR 381-12. AIS security incidents reported under AR 381-12 will not be reported under 2-28d, unless cleared by the supporting counterintelligence office. Any indication that the incident involves access or attempted access to Army AIS for the purpose of committing fraud, extortion, or theft will be referred to appropriate law enforcement activities for investigation. Examples of the types of incidents that will be reported to the ISSO include, but are not limited to-

(1) Unexplainable output received at a terminal (such as, receipt of unrequested information).

(2) Inconsistent or incomplete security marking on output, extraneous data included in output, or failure to protect output properly.

(3) Abnormal system response.

(4) Any indication of an unauthorized user attempting to access the system, including unexplained attempts to log-on unsuccessfully from a remote terminal.

(5) Any indication of unexplained modification of files or unrequested, abnormal "writes" to media.

b. ISSOs will review all incident reports and related documentation and, in cooperation with other security and investigative personnel, advise the commander or manager having system jurisdiction about the possibility of a system penetration or security violation. The ISSO 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 ISSO must formally advise all users of the problem and the action taken or expected.

d. If the cause of the incident cannot be directly attributed to administrative error and readily corrected (that is, tampering, system penetration, malicious acts by an employee, and similar actions cannot be ruled out), the incident will be reported to the Commander, U.S. Army Intelligence and Security Command. ATTN: IAOPS-CI-TO, Ft. Belvoir, VA 22060-5370.

(1) The initial notification will be within 5 working days and will include a brief statement containing the location, system concerned, a description of the suspected or confirmed incident, action taken, and point of contact.

(2) A final report of a confirmed AIS security incident will be submitted to the address in 2-28d within 2 months from the discovery of the incident. The final report will contain all relative documentation, including the corrective action taken.

e. In cases where serious vulnerabilities have been revealed, support is available from INSCOM under the AISSAP. (See para 2-30.)

f. When the incident is also reportable as a generic technical vulnerability as described in 2-29 as follows, required reports to INSCOM may be consolidated and will cite both applicable portions of this regulation.

**2-29. Technical vulnerability reporting (RCS: NSA/CSS 1057)**

The Computer Security Technical Vulnerability Reporting Program (CSTVRP) provides for the collection, consolidation, analysis, reporting, or notification of generic technical vulnerabilities and corrective measures in support of the DOD computer security requirements. The program focuses on technical vulnerabilities in commercially available hardware, firmware, and software products acquired by the DOD and those altered commercial products supporting standard military applications. Research prototypes, preproduction commercial products, and site-specific vulnerabilities are specifically excluded from this program.

a. INSCOM is the Army executive agent for reports of technical vulnerabilities under the CSTVRP. As the executive agent, INSCOM will-

(1) Screen the reported vulnerability for technical validity and determine the extent of risk presented by the vulnerability to the operation of the activity or to other activities.

(2) Submit reports to NSA. (See para 2-29b.)

(3) Disseminate information about confirmed vulnerabilities to Army activities having a valid clearance and a need-to-know.

(4) Disseminate information about solutions to reported vulnerabilities. Ensure such solutions have been field-tested, when feasible.

b. Technical vulnerabilities will be expeditiously reported through command channels to Commander, INSCOM, ATTN: IAOPS-CI-TO, Ft. Belvoir, VA 22060-5370, with information copies to HQDA (DAMI-CIC-AS) WASH DC 20310-1055, and HQDA (SAIS-ADS) WASH DC 20310-0107 (RCS: NSA/CSS 1057). Reports should be of sufficient detail so the vulnerability can be demonstrated and repeated.

c. Reports will include the following:

(1) General information.

(a) Report date.

(b) Contact name and position, organization, mailing address, and telephone number.

(c) Hardware and software configuration, including type of operating system (with release number), and any unique attributes such as special security properties.

(2) Executive summary. A description of the nature and effect of the vulnerability in as general terms as possible.

(3) Description of technical vulnerability.

(a) A scenario that describes specific conditions to demonstrate the weakness or design deficiency. The description should sufficiently describe the conditions so the weakness or design deficiency can be demonstrated without further information.

(b) A description of the specific impact or effect of the weakness or design deficiency in terms of denying service, altering information, and compromising data.

(c) An indication whether or not the vendor has been notified.

(4) Suggested correction. Any code or procedure that will reduce the impact of, or eliminate the defined technical vulnerability.

(5) Additional information. System location, owner, network connections, system use, highest classification of data, and any other clarifying information.

d. All reports of technical vulnerabilities will be initially classified at least "confidential." INSCOM, in coordination with NSA, will determine if the report should be declassified to facilitate dissemination.

e. Within contractual limitations, vendors may be provided the technical details of vulnerabilities to make corrections, but will not be provided information about the specific sites concerned, methods of discovery, or other information that could lead to increased site vulnerability, without the express written approval of the accreditation authority.

**2-30. U.S. Army Automated Information Systems Security Assessment Program (AISSAP)**

INSCOM manages and implements the AISSAP. This program includes teams available to visit Army and selected DOD and contractor-operated facilities to provide technical advice and assistance on AIS security as well as an AIS Security Testing, Analysis, and Support Center.

a. The AISSAP teams provide support worldwide. Each evaluation identifies potential security vulnerabilities with a comprehensive analysis of the total system. This includes the areas of security management, software, hardware, procedures, communications, media, network, personnel, and physical security. This evaluation may be supplemented by the results of separate INSCOM crypto facility and TEMPEST inspections or tests, as applicable. The team will assess the threats to the system and analyze the vulnerabilities. Countermeasures will be prescribed that must be implemented, or the vulnerability must be incorporated into the risk management program.

(1) Three distinct types of support are offered under the program.

(a) AIS security support. This is an evaluation of all aspects of AIS security pertaining to an automated system. This evaluation is intended to supplement the commander's risk assessment program.

(b) Immediate security support. This is a limited investigation of a specific problem; for example, a suspected security incident, hazard, violation, or misuse of Army computer resources. Further action will be referred to the appropriate authority.

(c) Physical and environmental engineering security support. This support consists of a consultative review oriented toward assisting users to incorporate security guidelines into the development of physical facilities. This support must be conducted during the planning phase for new facilities or existing facilities requiring major revision.

(2) INSCOM will conduct an annual data call to rank and schedule support described in 2-30a(1) of this regulation. Nominations will be consolidated at Army MACOM level and submitted to Commander, U.S. Army Intelligence and Security Command, ATTN: LAOPS-CI-TO, Ft. Belvoir, VA 22060-5370. INSCOM will provide specific instructions with each data call. Requests for immediate support may be made at any time, but must be submitted through the MACOM ISSPM to the address above. Additionally, HQDA (DAMI-CIC-AS) may direct an evaluation when security or counterintelligence information indicates that the security posture of the site or command could benefit from the assessment.

(3) In addition to the support scheduled through the annual data call or as a result of an immediate request, systems processing SCI data must receive AIS security support to complement their accreditation. Requests will be forwarded to the address in 2-30a(2), and a copy of the request will be a mandatory enclosure to the accreditation documentation. This requirement does not apply to AIS accredited by DIA, nor does it apply to small computers.

(4) A copy of the report of AIS security support will be furnished to the visited site and the MACOM ISSPM within 60 days of the actual visit. Within 60 days of receipt of a report, the visited site will complete and return the "evaluation of service form" provided with the report to the address in 2-30a(2), with a copy furnished to the MACOM ISSPM.

b. As part of the AISSAP, INSCOM also operates the AIS Security Testing, Analysis, and Support Center.

(1) The support center provides on-line analysis capabilities to the AISSAP teams, test and evaluation of non-RDTE Army-owned software, support in analyzing CSTVRP submissions, and internal training for AISSAP teams.

(2) Army activities can request support center security testing of Army-owned software through the MACOM ISSPM to the address in 2-30a(2). Identification of the software, complete documentation, system hardware and software configuration, and a point of contact must accompany the request.