Supersedes dtd. 6-1-91

STATE OF WEST VIRGINIA
ADJUTANT GENERAL'S DEPARTMENT
CHARLESTON, WEST VIRGINIA 25311-1085

Series 80

FILED
1991 OCT -1 PM 3:57
OFFICE OF SECRETARY OF STATE

WV MILITARY REGULATION (Army)
NUMBER 380-19

1 OCTOBER 1991

AUTOMATION SECURITY

CHAPTER 1

GENERAL

1-1. PURPOSE

The purpose of this regulation is to complement AR 380-19, to establish an Information Systems Security Plan for the implementation of the Army Information Systems Security Program (AISSP), and serve as the principle reference document for the implementation of automation security procedures by units of the WVARNG.

1-2. Applicability

This regulation is applicable to all automated mainframe, mini, micro, and personal computers, and memory typewriters utilized to support the mission requirements of the WVARNG, including any privately owned Automated Information Systems (AIS) which may be authorized for such use. In the event that a conflict should arise between this regulation and any of the cited references, the provision which provides for the greatest level of security shall apply.

1-3. References

All abbreviations and terminology are as listed in the glossaries of the listed references, unless specifically cited in this document.

a. AR 380-19 Information Systems Security.

b. AR 380-5 Department of the Army Information Security Program.

c. AR 340-21 The Army Privacy Program.

d. National Guard Bureau, Mobilization and Readiness Division, Information Paper, 12 Sept 86, Subject: Processing Unit Status Report (USR) on Microcomputers.

e. ARNG Regulation 340-1, Privacy Act Information.

f. Department of Defense Directive, Number 5200.28, 21 Mar 88, Subject: Security Requirements for Automated Information Systems.

1-4. UPDATES

This regulation is to be reviewed annually, to evaluate its effectiveness and conformance to applicable regulations. Updates, changes, and revisions will be made as required. Users of this regulation are invited to send comments and suggestions to: Office of The Adjutant General ATTN: WVAR-DOIM, 1703 Coonskin Drive, Charleston, WV 25311-1085.

1-5. EFFECTIVE DATE

This regulation becomes effective upon receipt.

CHAPTER 2
CHAIN OF COMMAND / RESPONSIBILITIES

2-1. THE ADJUTANT GENERAL (TAG)

TAG has overall responsibility for automation security within the state. TAG will:

a. Appoint an Information System Security Manager (ISSM) to act as the focal point for all AIS security matters.

b. Serve as the accreditation authority for those systems designated as Classified Sensitive (CS) as delegated from the Chief, National Guard Bureau. TAG may further delegate this authority as defined by Chief, National Guard Bureau and AR 380-19.

c. Ensure that each site handling information designated as sensitive or above implements an effective risk management program.

d. Serve as the authorizing authority for the use of privately owned AIS to support mission requirements of the ARNG.

2-2. DIRECTOR OF INFORMATION MANAGEMENT (DOIM)

The DOIM will serve as the focal point and principle advisor to TAG on all matters pertaining to AIS management. The DOIM will:

a. Represent TAG in all matters pertaining to AIS management.

b. Serve as the ISSM unless otherwise directed.

c. Determine and coordinate automation security requirements, and develop the Information Systems Security Plan (ISSP).

d. Establish and manage the AIS security planning cycle to provide for:

(1) Continual analysis of security needs.

(2) Review of current policies and procedures.

(3) Develop and update security policies.

(4) Determination of funds for security requirements.

e. Serve on the Program Budget Advisory Council as the program manager for information systems security, to coordinate funds, financial planning, and administration for automation security.

f. Establish educational and training objectives for the implementation of the ISSP.

g. Recommend, evaluate and approve software and hardware for automation security applications.

h. Serve, as required, as the Contracting Officer's Technical Representative on automation security issues.

2-3. INFORMATION SYSTEM SECURITY MANAGER (ISSM)

The duties of the ISSM will be performed by the DOIM. The ISSM will:

a. Serve as the focal point and principle advisor to the TAG on automation security matters.

b. Chair the STARC Automation Security Committee.

c. Appoint recommended personnel as ISSOs, and maintain a roster of appointed ADPSSOs and the AIS for which they are responsible.

d. Exercise staff supervision over the responsibilities and duties of ISSOs.

e. Ensure that ISSO security actions are integrated, and that they receive adequate local support to meet automation security requirements.

f. Maintain a file of all security incidents involving AIS, direct investigations IAW AR 380-19, and analyze such incidents for trend indication.

g. Issue and control security systems for AIS, and serve as the controlling authority for operating system access.

h. Maintain files for accredited AIS which contain:

(1) AIS Facility Security Profile (FSP).

(2) Continuity of Operations Plan (COOP).

(3) AIS installation/location diagram.

(4) TASO appointment orders.

(5) AIS hand receipt.

(6) Security inspection reports.

2-4. COMMANDERS AND SPECIAL STAFF

Commanders, and special staff, who supervise activities or organizations which utilize AIS, have overall responsibility for automation security within their commands and organizations. Personnel assigned such positions will:

a. Familiarize themselves with this regulation.

b. Recommend personnel, as required, for appointment as Information System Security Officers (ISSO), IAW the following criteria:

(1) Must be a member of the full time support force.

(2) Must possess a security clearance equivalent to that of the most highly classified AIS for which they will be responsible.

(3) If recommended for appointment as the senior ISSO for organizations above company level, must be in the grade of E-7 or above and possess sufficient rank to effectively supervise all subordinate ISSOs/TASOs within the organization.

c. Appoint, in writing, personnel to serve as Terminal Area Security Officers (TASO) for each terminal or group of terminals in the command, IAW the following criteria:

(1) Must be a member of the full time support force.

(2) Must possess a security clearance equivalent to that of the most highly classified AIS for which they will be responsible.

d. Forward copies of TASO appointments to the ISSM and ISSOs of higher headquarters.

e. Manage the cost effective commitment of organizational resources for the physical and environmental security of AIS and ensure the effective implementation of the plan.

2-5. INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

ISSOs serve as the information systems security authorities for battalion and higher level headquarters, for multi terminal/network AIS, and as directed by the ISSM. They function as coordinators of multiple subordinate level ISSOs and TASOs, provide security guidance, and review matters concerning facilities, equipment, and data security for AIS in their organizations. ISSOs will:

a. Meet all appointment requirements.

b. Read and understand this regulation, develop and update the unit Information Systems Security SOPs.

c. Accomplish the responsibilities specified in AR 380-19.

d. Be responsible to the ISM for their duties, as defined in this and other applicable regulations.

e. Exercise staff supervision over subordinate ISSOs and TASOs (para 5-4f.).

f. Assist in the accreditation of AIS for which they are assigned responsibility (para 5-3d. & e.).

g. Conduct and maintain accurate records of annual information systems security inspections, and reviews (para 5-4e, 5-4g & 5-6).

h. Ensure that the availability of AIS assets within their organizations is effectively managed and controlled.

i. Maintain an ISSO Security Reference Book containing:

(1) AR 380-19.

(2) Unit automation security SOP.

(3) Their ISSO appointment orders.

(4) Official correspondence concerning AIS security issues.

j. Maintain an AIS Security File on each system for which they are responsible that contains:

(1) A copy of the current accreditation letter.

(2) A copy of the current TASO's appointment order.

(3) Annual security inspection reports.

2-6. TERMINAL AREA SECURITY OFFICER (TASO)

TASOs serve as automation security authorities over one or more AIS, located in areas under their control. They coordinate AIS use and enforce the STARC ASP at the user level. TASOs will:

a. Read, understand, and enforce the provisions of this regulation and their unit's automation security SOP.

b. Accomplish all responsibilities as specified in para 1-6(5), AR 380-19.

c. Conduct and document required security briefings (para 4-3).

d. Control and issue passwords for single terminal stand alone AIS, and ensure that all users sign an AIS Conditions of Use Acknowledgment (Appendix C), before being granted access to any system (para 6-2c).

e. Control utilization of AIS telecommunications (para 8-1b).

f. Initiate accreditations for AIS, forward them to their unit ISSO for further action (para 5-3), and update the documents of approved accreditations as required.

g. Identify threats to the AIS for which they are responsible, and coordinate with their ISSOs in taking appropriate measures to reduce or eliminate them (para 3-3e.).

h. Conduct and document serial number inventories of issued hardware and software (para 7-1d.).

i. Ensure that a CS Processing Requirements Acknowledgment (Appendix D) is signed by all authorized users of CS3 accredited AIS before they are granted access (para 4-3c.).

j. Maintain backup copies of all software applications installed on the AIS for which they are responsible (para 6-7a.).

k. Maintain a TASO Security Reference Book containing:

(1) AR 380-19.

(2) Unit automation security SOP.

(3) Their TASO appointment orders.

(4) Official correspondence concerning AIS security issues.

l. Maintain an AIS Security File for each system containing:

(1) Current accreditation letter.

(2) Accreditation documents (para 5-2a.).

(3) Software authorization letter.

(4) Conditions of Use Acknowledgments for all users.

(5) CS3 processing requirements acknowledgments (para 2-8b.).

(6) AIS security inspection reports.

2-7. AUTOMATED INFORMATION SYSTEM USERS

AIS users are all personnel, including ISSOs and TASOs, who are authorized to utilize AIS. Users will:

a. Read and understand the unit AIS security SOP, read and sign the AIS Conditions of Use Acknowledgment (Appendix C), prior to being granted access to any AIS.

b. Sign a CS Processing Requirements Acknowledgment (Appendix D) before being granted access to critically sensitive files or AIS.

c. Receive security briefings (para 4-3).

d. Have a security clearance equivalent to that of the most highly classified AIS to which they are granted access (para 4-1b.).

CHAPTER 3
THREAT/RISK MANAGEMENT PROGRAM

3-1. GENERAL.

The goals, objectives, and methodology of the Threat/risk management program are based upon AR 380-19, Chapter 5.

3-2. OBJECTIVES.

a. The objective of threat/risk management is to safeguard AIS and information against deliberate or inadvertent:

(1) Unauthorized disclosure of information.

(2) Denial of service or use.

(3) Unauthorized manipulation of information.

(4) Unauthorized use.

b. Risk Management consists of methodical procedures, by which the risk to which AIS are subject may be measured, identified, and controlled to minimize loss. The four sequential phases are:

(1) Risk assessment & analysis.

(2) Management decision.

(3) Control implementation.

(4) Effectiveness review.

3-3. RISK ASSESSMENT & ANALYSIS.

a. Risk is derived from the identification of a threat, the likelihood of its occurring, and the degree of vulnerability to which the AIS or its data is subjected.

b. A threat is any agent or event which may exploit a vulnerability and reduce or neutralize the effectiveness of a system, thereby limiting or negating mission accomplishment.

c. Likelihood of occurrence is determined by researching the number of times that a threat has, or is likely to occur, and taking into account any corrective measures that may have been implemented.

d. Degree of vulnerability is the combination of the number of threats and the likelihood of their occurrence, to which an AIS or its information are subjected.

e. TASOs are responsible for the identification of threats to the AIS for which they are responsible, and for coordinating with their ISSOs in taking appropriate measures to reduce or eliminate them (para 2-7g. & 5-3c.).

f. ISSOs identify and evaluate vulnerabilities, and determine the degree of risk to which an AIS is subjected (para 5 3d.).

3-4. MANAGEMENT DECISION

a. The process of reviewing identified risks and determining appropriate controls is a function of ISSOs, unit commanders, and the ISSM. It determines which risks, in relation to organizational mission, goals, and objectives, are unacceptable and require the commitment of resources to eliminate them IAW established regulations and/or procedures.

b. ISSOs are responsible for developing and recommending risk controls for implementation by their commanders (para 2 6c.).

c. Commanders are responsible for the cost effective commitment of resources to implement recommended controls (para 2-5e.)

d. The ISSM is responsible for insuring that unit controls and security procedures are integrated and effective (para 2-3f).

3-5. CONTROL IMPLEMENTATION

a. Risk controls and security procedures must by coordinated and approved by accreditation authorities and unit commanders prior to implementation.

b. Implementation of risk controls must result in a series of integrated and mutually supporting countermeasures to threats, and not result in the creation of new vulnerabilities.

3-6. EFFECTIVENESS REVIEW

Review of the effectiveness of implemented controls is a continual process. TASOs and ISSOs must be constantly aware of the threats to the AIS for which they are responsible, and ensure that AIS vulnerabilities are reduced to an acceptable level. Controls will be reviewed and upgraded as required wherever:

a. Accreditations are reviewed or renewed.

b. Unit organization, mission, or goals change in such a manner as to impact upon AIS operations.

c. A new risk is identified.

d. A unit is denied the use of its AIS, access to its data, or suffers a loss of its automated information assets.

e. Unauthorized access to sensitive defense information is suspected or confirmed.

CHAPTER 4
ACCREDITATION

4-1. GENERAL.

a. The preparation, processing, and approval of accreditations is accomplished IAW appropriate chapter of AR 380-19.

b. AIS utilized by the ARNG may by accredited in one of following levels: (Reference para 1-5c AR 380-19)

(1) Classified Sensitive 1 (CS1) - SCI.

(2) Classified Sensitive 2 (CS2) - TOP SECRET.

(3) Classified Sensitive 3 (CS3) - SECRET/CONFIDENTAL.

(4) Unclassified-Sensitive 1 - Intelligence/crypto exempt data.

(5) Unclassified-Sensitive 2 - Unclassified information protected to ensure availability or integrity.

c. The requirement for accreditation is applicable to all automated mainframe, mini, micro or personal computers utilized to support the mission requirements of the ARNG, as well as any privately owned AIS which may be authorized for such use.

d. The requirements for accreditation does not pertain to memory typewriters which do not possess the capability to store information or data internally. However, the external storage media utilized by these AIS is to be safeguarded.

4-2. REQUIRED DOCUMENTATION

a Required documentation for AIS accreditation is:

(1) AIS Facility Security Profile (Appendix F).

(2) AIS installation/location diagram (para 4-2b.).

(3) Copy of TASO appointment (Appendix B).

(4) Copy of AIS hand receipt.

(5) Continuity of Operations Plan (para 10-3) (multi terminal and network systems only).

(6) Crypto facility approval certificate (WWMCCS & AUTODIN terminals only).

b. The AIS installation/location diagram will meet the following requirements:

(1) Clear, detailed and readable.

(2) Indicate location of all system components.

(3) Indicate direction of view for the CRT screen.

(4) AIS hand receipt number in the lower right corner.

(5) If the AIS has multiple terminals or is a network host, all terminal locations must be indicated, and additional diagrams provided, as required, for terminals located in other locations.

c. AIS that are part of a network, and possess the capability to operate independently of the host, must by fully accredited for operation in the stand alone mode. Such AIS must be referenced in the accreditation requirements for the host's level of sensitivity. This requirement does not apply to remote (dumb) terminals which possess no memory or processing capability other than that provided by the host AIS.

d. Battlefield automated systems (BAS) and laptops, which are not intended for use in fixed locations, are not required to submit an installation/location diagram for accreditation. BAS will submit a copy of their tactical SOP (para 11-2) in lieu of the diagram. Laptops are required to submit a copy of the Laptop Personal Computer Utilization SOP (Appendix G) lieu of the diagram. A copy of the SOP is to be kept with these systems at all times.

e. Those AIS for which Nonsensitive accreditation is requested must submit a written analysis supporting this security rating.

4-3. ACCREDITATION PROCESS

a. An interim Unclassified-sensitive 1 will be in effect for the first 30 days following the installation of a new AIS. Within this period, the responsible TASO must prepare and submit an application, through ISSO channels, for accreditation. A letter of accreditation (Appendix H) must be received by the TASO, if the AIS is to be utilized beyond the interim accreditation period.

b. TASOs are responsible for initiating the accreditation process, preparing required documentation, and forwarding it to their unit ISSO for further action (para 2-7f.).

c. TASOs, when filling out the FSP, report upon location, environment, security, and operating procedures (para 3-3e.).

d. ISSOs will review accreditation documents for completion and accuracy. In their column of the FSP, they will indicate whether vulnerabilities exist as a result of the status reported by the TASO. ISSOs evaluate the vulnerabilities, determine the degree of risk, and either forward accreditations for approval or return them to the TASO for corrective action (para 2-6f. & 3-3f.).

e. Major Command ISSOs review the accreditation documents, forwarded to them by subordinate command ISSOs. They perform the tasks listed in item (d.)

above only for FSPs submitted by TASOs that report directly to them. Accreditations reflecting an acceptable degree of risk are forwarded to the ISSM (para 2-6f.).

f. The ISSM ensures that accreditations are complete and indicate an acceptable degree of risk. Those which are incomplete or indicate unacceptable risk will by returned for appropriate corrective action. A formal letter of accreditation (Appendix H) will be issued by appropriate authority for approved accreditations.

g. An accreditation letter will be forward, by the ISSM, through ISSO channels, to the TASO responsible for the newly accredited AIS (para 2-7l.). ISSOs will make copies of accreditation letters for their records as required (para 2-6j.). The ISSM will retain a file copy of the letter and the original accreditation documents (para 5-6).

h. The TASO, upon receipt of the Accreditation Letter, is thereby authorized to permit the processing of information on the AIS, IAW the accredited security level, until the accreditation either expires or is revoked.

i. Expiration periods for Accreditation letters is for 3 years unless any of the following occur:

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

(2) A change in sensitivity designation or mode of operation.

(3) A significant change in operating system or executive software.

(4) A breach in security or violation of system integrity.

(5) A significant change in the physical structure of the facility.

4-4. REACCREDITATIONS, REVIEWS, & INSPECTIONS

a. AIS will be reaccredited within one month when any of the following occur:

(1) An increase in the security label of data processed.

(2) A breach of security.

(3) Significant changes to the facility.

(4) Relocation or reassignment to another facility or unit.

(5) Significant changes to the AIS hardware.

(6) Accreditation is revoked.

(7) Current accreditation expires.

b. A reaccreditation consists of the same documentation and processing requirements as an accreditation (para 4-3).

c. Laptops and BAS are not reaccredited due to reallocation with, or changes to, a facility.

d. ISSOs will schedule reaccreditation activities so as to provide for issuance of a new accreditation letter prior to the expiration of the current letter. AIS need not be reaccredited due to ISSO or TASO assignment changes.

e. ISSOs are to conduct periodical Accreditation Reviews (Appendix I), for all AIS under their jurisdiction, upon the discretion of the ISSM or ISSO. Should deficiencies be found in the course of the review, the accreditation may by suspended or revoked (para 2 6g. & 4-5).

f. As part of the Command Inspection Program each Major Command will inspect its ISSO's, utilizing the ISSO Security Inspection Checklist (Appendix K). The ISSM will inspect the Major Command ISSOs.

g. The results of accreditation reviews and inspections are to by maintained in the inspecting ISSO's files for a period of three (3) years (para 2-6g. & 4-6).

h. The results of the annual ISSO inspections conducted by the ISSM will be communicated to the appropriate headquaters.

4-5. SUSPENSION & REVOCATION OF ACCREDITATIONS

a. Suspension of accreditation may be directed by the ISSM, or an ISSO assigned responsibility for the AIS, at any time security deficiencies are identified which may result, or have resulted, in the unauthorized disclosure of sensitive defense information, waste, loss, unauthorized use, or misappropriation of AIS assets (para 5-4e.).

b. If accreditation is suspended by direction of the ISSM, an accreditation review must by conducted (para 5-4) by the appropriate TASO and ISSOs, forwarded to, and approved by the ISSM before the suspension is lifted.

c. If accreditation is suspended by direction of an ISSO, the Accreditation Review warranting the action will by forwarded to the ISSM within five working days.

Requirements for lifting of the suspension will be as directed by the ISSM.

d. Revocation of accreditation may only be directed by the ISSM. This may occur any time serious, or repeated, security deficiencies are identified (para 4-4e.).

e. If an AIS accreditation is revoked, a reaccreditation must be conducted and approved by the ISSM, before a new accreditation letter is issued.

f. During suspension and revocation periods, utilization of the AIS is not authorized. The responsible TASO will suspend all access to the AIS. Failure to comply with this requirement may result in the withdrawal of the AIS form the utilizing organization.

4-6. ACCREDITATION INVENTORIES

A current inventory of AIS documents will be maintained by the ISSM, ISSOs, and TASOs as indicated below:

DOCUMENT	ISSM	ISSO	TASO
Current Accreditation Documments	Original	Copy	
Current Accreditation Letter	Copy	Copy	Original
Conditions of Use Acknowledgements	Original		
CS Precessing Reg. Acknowledgements	Original		
Accreditation Reviews	Original	Copy	
Accreditation Suspensions	Copy	Copy	Original
Accreditation Revocations	Copy	Copy	Original

4-7. DOCUMENT SECURITY

Accreditation documents will be handled, marked, and stored in a manner equivalent to the level of sensitivity for which the AIS is accredited. FOR OFFICIAL USE ONLY is the minimum sensitivity level for any files or records maintained by the ISSM, ISSOs, or TASOs. Access to such records and documentation is to be managed on a strict "need-to-know" basis.

CHAPTER 5
FILE AND SOFTWARE SECURITY

5-1. ACCESS CONTROL/SECURITY SOFTWARE

a. The ISSM will designate access control/security-software, for installation on accredited AIS, to prevent unauthorized operation, and to restrict access to internal files and applications.

b. AIS accredited for CS operations must be safeguarded be access control/security software.

c. AIS with unauthorized access control/security software installed will have their accreditations suspended until such time as it is removed.

d. To be considered for authorization, an access control/security software must possess the following capabilities:

(1) Master password control over installation and removal.

(2) Master password control over lower level passwords.

(3) Password control over user access.

(4) Password indexing by user ID code.

(5) Optional password control over menu selections.

(6) Multiple menu generating capability.

(7) Time activated log-off upon lack of keyboard activity.

(8) Protection from commands entered form alternate drives.

(9) User access history and report capability.

(10) Random password generation capability.

e. The ISSM will control access to AIS operating systems and the ability to install and remove software (para 2-3h. & 5-7e.). Security software will not be disabled or removed from any AIS without the authorization of the ISSM.

f. Those AIS which do not have access control/security software installed must have an authorized user's roster posted in their vicinity, and the TASO will be responsible for ensuring that unauthorized users do not access the system (para 6 2a.).

5-2. PASSWORD CONTROL

a. The ISSM is the principle manager of access control/security software (para 2-3h.).

b. ISSOs generate, control, and provide passwords to TASOs for issue to users of multi-terminal/network AIS, and will supervise the performance of these tasks by TASOs for single terminal stand alone AIS (para 2-6c. & e. and 5-2c.).

c. TASOs will generate passwords only for single terminal stand alone AIS. Passwords for access to multi-terminal network AIS must by obtained from the ISSO. TASOs will issue all passwords by personal contact, and only after the user has received and signed all appropriate security briefings (para 2-7d. &i.). TASOs will ensure that passwords are removed, when users no longer require access.

d. TASOs will maintain AIS Conditions of Use Agreements for all current users authorized access to AIS (para 2-71. (4)).

e. Users will be provided password access to only those AIS files, and applications necessary to perform their assigned duties. At the time of password issuance TASOs will brief users on:

(1) Exclusiveness of password.

(2) Measures to safeguard passwords.

(3) The prohibition against revelation of the password.

(4) Requirement to immediately report password compromise.

f. Passwords are not to be transferred between users. When a user no longer requires a password, the password will be retired.

g. Passwords for AIS accredited for CS information must be randomly generated by security software and be eight characters long.

h. All passwords installed on AIS accredited CS2 or CS3 will be changed semiannually. All other passwords will be changed annually.

i. Passwords will consist of an alphanumeric string of not less than five (5) characters. A three (3) character ID code will be used to associate the password to the authorized user.

j. All passwords are to be memorized. Files or records of user passwords will not be maintained.

k. ISSOs will investigate all actual or suspected compromises of AIS passwords, and will immediately notify the SSM and unit commander, if unauthorized access was gained to an AIS (para 2 -6c.).

5-3. MAGNETIC MEDIA LABELING AND PROTECTION

a. Proper care, handling, marking, and storage of magnetic media is the responsibility of the user. All magnetic media is to be protected at the highest level of sensitivity of information that is stored or recorded on it (AR 380-5).

b. All removable diskettes, tapes, and disks are to be externally labeled with the following:

(1) A semipermanent label, identifying the highest sensitivity level of the information stored or recorded, is to be placed on the front and back of the media, and on the front and back any protective jacket or container in which the media may be stored.

(2) One semipermanent label containing the unit ID and file name, placed on the front of the media.

c. AIS equipped with internal disk drives, or other non volatile memory, will display, in plain view, semipermanent labels indicating the accredited sensitivity level of the system. Labels will be affixed to all system CRTs, and adjacent to an external drive ports.

d. User files are to be maintained on removable media, and valuable information should be write protected, to safeguard against accidental formatting or over writing.

e. Removable media is to be stored IAW para 9-2.

f. The read/write heads of disk drives are to be retracted (shipped) at the end of each day before the AIS is shut off, and any time the AIS (desktop or portable) is to be moved.

g. Protective inserts are to be placed into disk drives when they are not in use, to provide evidence that the diskettes have been removed and that the drives are secure.

h. Users are responsible for maintaining sufficient and appropriate backup copies of files, and applications critical to their processing requirements (para 10-1a.).

i. TASOs are to conduct periodic reviews of the available data storage space on fixed disk drives. In the event that more than 3/4 of available memory is in use, unnecessary and seldom used files should either be deleted or copied to removable storage media.

5-4. PROCESSING OF CRITICALLY SENSITIVE FILES

a. Prior to the conduct of classified processing sessions, users will ensure AIS are prepared IAW AR 380-19, and that all provisions of the CS Processing Requirements Acknowledgment are complied with (Appendix D).

b. TASOs for AIS accredited as critically sensitive must have signed originals of the CS Processing Requirements Acknowledgment (Appendix D) on file for all currently authorized users (para 2-71.).

c. TASOs will establish a procedure for a daily security check of CS3 work stations, utilizing DD Form 70 (Area Security Checklist) to ensure that all classified media and materials have been secured.

d. Personnel who discover the compromise of critically sensitive data will report the disclosure IAW AR 380-5.

5-5. TEMPEST REQUIREMENTS

All users of critically sensitive files and data will receive a TEMPEST briefing from their TASO, explaining the provisions of AR 530-4, prior to being granted access to AIS accredited for CS3 processing (para 4-3a.). TEMPEST requirements will be listed on the CS Processing Requirements Acknowledgment (Appendix D), and will be practiced during all CS processing sessions.

5-6. PRIVACY ACT REQUIREMENTS

a. The Privacy Act of 1974 prohibits unauthorized access to records containing personal data. All AIS users are to protect personal data from unauthorized disclosure. Disciplinary action, to include criminal penalties, may by imposed on users who make willful, unauthorized disclosures or obtain access to records under false pretenses. Similarly, all users must by alert to, and protect against, unauthorized alternations of personal data (AR 340-21)

b. All personal records are Highly Sensitive and will by handled, labeled, processed, and stored For Official Use Only.

c. Authorization and identification must be established prior to releasing personal data to any individual.

d. Destruction of magnetic media containing privacy act data is to accomplished by either shredding, burning, or melting.

5-7. COMMERCIAL SOFTWARE

a. The term "Commercial Software" applies to any program or application that requires user licensing, to include "SHAREWARE".

b. ISSOs and TASOs will insure that commercial software is installed only on AIS for which it is issued, and that unauthorized software is not installed on any AIS for which they are responsible. TASOs will maintain copies on the written authorizations for all software installed on their systems.

c. Original media will only be utilized for backup

purposes. All installation, testing, and processing will be accomplished utilizing copies made from the originals (para 2-7j.).

d. Only software approved by the DOIM may be utilized on federal equipment. Any AIS found to have unauthorized software installed will have such software deleted, and be subject to suspension or revocation of its accreditation (para 4-5a. & d.)

e. ISSOs and TASOs will not permit installation, copying, distribution, or any other activity that may violate the copyright privileges of commercial software manufacturers.

f. Access to AIS operating systems, and the ability to install software, will be password controlled for access only by personnel authorized by the ISSM (para 5-1e.).

5-8. GOVERNMENT/USER DEVELOPED APPLICATIONS

a. Applications, programs and software, developed by users, on accredited AIS, for the purpose of processing government records and information, are intended for the exclusive use of the ARNG, are the property of the organization supported, and are subject to the provisions of para 5-7 above.

b. Users who develop applications, programs, and software for the purpose of processing government records and information, are to maintain detailed documentation of their work. As a minimum they will maintain records of the program description, sample input and output formats, method of operation, source code and test data.

c. Following final debugging, user developed applications and supporting documentation are to be forwarded to the DOIM for review.

d. User developed applications, and software obtained from other military sources, will not be distributed or installed to support mission requirements, until it has been reviewed and approved by the DOIM.

5-9. PRIVATELY OWNED SYSTEMS

a. Use of privately owned AIS (i.e. not owned or leased by the Army or the ARNG) to support mission requirements is strongly discouraged. Commanders and AIS security personnel will prohibit the use of privately owned AIS within their commands, unless they are authorized by TAG (para 2-1e.) and properly accredited IAW Chapter 4.

b. In the event a privately owned AIS is accredited for use, the following restrictions will be enforced:

(1) Support of mission essential tasks is prohibited.

(2) Only processing of nonsensitive data is authorized.

(3) May be used only in the stand alone mode.

(4) May not have a communications capability.

(5) Must not access government systems in any manner.

c. Information processed on privately owned AIS becomes the property of the supported organization.

d. Privately owned AIS will be utilized only at the facilities for which they are accredited, regardless of their portability, owners may not remove them from accredited facilities without prior authorization from the ISSM.

e. Owners of personal AIS, accredited for use at government facilities, must recognize that the government assumes no responsibility for the AIS, and that all such utilization is at the owners own risk.

f. Accredited privately owned AIS are subject to all provisions of this and other applicable regulations (para 1-2).

5-10. WORKING AT HOME

Privately owned AIS will not be accredited for use at any location other than government owned facilities. Processing of Critically Sensitive Unclassified-Sensitive data, on unaccredited privately owned AIS located in private residences or public facilities is prohibited.

CHAPTER 6
HARDWARE SECURITY

6-1. ACCOUNTABILITY AND UTILIZATION

a. The DOIM will exercise centralized control of the hardware assets necessary to implement the ARNG Information Systems Plan. AIS governed by this regulation, will be distributed, utilized and maintained as directed by the DOIM (para 2-2i.).

b. If AIS equipment is not utilized IAW this and other applicable regulation, it may be withdrawn by the DOIM.

c. Nontactical AIS are issued solely for garrison use at unit home stations. These systems ARE NOT to be

used for field of combat service support requirements, and ARE NOT to be taken to Annual Training sites, without the written approval of the DOIM.

d. TASOs will conduct serial number inventories of their AIS on a quarterly basis (para 2-7h.).

e. Expenditures for automation equipment are subject to Congressional funding restrictions. To ensure compliance with these restrictions, no organization or activity is to acquire or purchase AIS equipment, without the prior notification and approval of the DOIM.

f. Organizations and activities, which receive AIS equipment from sources other than the office of the DOIM, will provide the DOIM with a detailed inventory, which specifies the manufacturer, model, and serial number, of all equipment received.

6-2. ACCESS CONTROL.

To safeguard AIS assets against compromise, waste, loss, unauthorized use, and misappropriation, the physical security of the equipment will be maintained IAW AR 190-51. To accomplish this objective the following requirements are established. AIS will:

a. Be restricted for use by only trained and authorized users.

b. Be freely accessible only during scheduled duty hours, and by arrangement with the TASO during non duty hours. AIS shared by multiple organizations/ activities will have a user's utilization schedule posted in the vicinity of the AIS, which will reflect the utilization periods for each organization/activity.

c. Be checked upon periodically by the TASO.

d. Be located in an area that is secured during non duty hours, or other periods when no one is present.

e. Be located in common work areas, which provide for access by all authorized users.

f. Be serviced only by DOIM service personnel, or by contract personnel authorized by the ISSM (para 4-1d.).

CHAPTER 7
COMMUNICATION SECURITY

7-1. ACCESS CONTROL

a. Telecommunications assets will be protected by password.

b. Utilization of telecommunications assets will be monitored by the TASO, and other auditing methods as required by COMSEC policies.

c. Telecommunications assets are FOR OFFICIAL USE ONLY.

d. Activities which utilize telecommunications assets will designate in writing those personnel authorized to release messages (para 2-7l.(11)).

7-2. TEMPEST REQUIREMENTS

a. Any transmission of critically sensitive information must meet established TEMPEST requirements IAW AR 380-19 1 local COMSEC procedures, and para 5-4 & 5-5.

b. During any processing period, during which critically sensitive information is being processed, any telecommunications lines not being utilized must by physically disconnected. Logical disconnects do not meet TEMPEST disconnect requirements.

7-3. ELECTRONIC MAIL SERVICES

a. Communications will be established only with electronic mail services approved by the DOIM. Toll charges for remote connection to any electronic messaging or data inquiry system are subject to the restrictions applicable regulations.

b. Electronic mail services are not authorized for transmission of critically sensitive information.

c. Information transmitted on electronic mail services will be fully prepared for transmission, before accessing the electronic mail system. Documents are not to be composed while "on line".

d. Information retrieved from electronic mailboxes will be copied to a disk, and printed after signing off from the service.

e. Down loading of Public Domain Software, Shareware, or any other programs, from electronic bulletin boards or communications services, to AIS owned or leased by the government, is prohibited.

CHAPTER 8
PHYSICAL/ENVIRONMENTAL SECURITY

8-1. ACCESS CONTROL

a. Access to AIS hardware and equipment will be

controlled by appropriate access control procedure, as established in para 6-2 of this regulation.

b. Magnetic media is to be protected at the highest level of sensitivity of information that is stored on it IAW AR 380-5.

8-2. STORAGE OF MEDIA AND SUPPLIES

a. AIS media and supplies are to be stored in a secure manner, as warranted by their value and level of sensitivity (para 8-1b.).

b. Accountability of supply, distribution, and use will be maintained by the TASO, to determine unit requirements, expenditures, storage levels, and to detect loss and misappropriation.

c. Due to the fragile nature of magnetic storage media, storage area must meet the following requirements:

(1) Located away from the vicinity of heat sources.

(2) Located away from magnets, or items containing magnets.

(3) Located away from excessive dust, smoke, or moisture.

d. Storage areas for AIS backup files must be located in area which would not be threatened by the same emergency or disaster that would affect the AIS itself (para 9-3a.).

8-3. ENVIRONMENTAL HAZARDS

When determining the location for the installation of a AIS, consideration must be given to environmental hazards. Those that are part of the nature of the facility must be avoided, and those that develop as a result of poor security practices must be prevented.

a. Hazards that may be part of the facilities nature are:

(1) Excessive smoke and dust.

(2) Static electricity.

(3) Excessive warmth or heat for extended periods.

(4) Area subject to flooding or water damage.

(5) Equipment which generates electromagnetic fields.

(6) Open windows, through which debris may be taken in.

b. Hazards resulting from poor security practices are:

(1) Tobacco smoke taken into the AIS by the cooling fan.

(2) System's cooling fan becoming obstructed.

(3) Liquids spilled on or into the AIS.

(4) Food particles obstructing keyboard functions.

(5) Damage due to falls or rough handling.

(6) Failure to use surge protectors.

(7) Operation of the AIS during electrical storms.

(8) Non-AIS equipment plugged into surge protectors.

c. If class "C" fire suppression equipment is not installed in the room where the AIS is located, a portable class "C" fire extinguisher must be located within fifty (50) feet of the AIS.

d. Smoking, eating, and drinking is not to be permitted in the vicinity of an AIS, appropriate signs will be posted.

CHAPTER 9
CONTINGENCY PLANNING

9-1. DATA FILE BACKUP

a. Users are responsible for maintaining sufficient and appropriate backup copies of critical files (para 5-3h.).

b. An active work file, stored either on removable media, or on the fixed disk drive, which serves as the primary source of information for data processing does not constitute a backup.

c. Backup files should be maintained on three generations:

(1) Son - the most recent copy of the active data file.

(2) Father - the copy of the active data file that was made during the backup cycle preceding that of the son.

(3) Grandfather - the copy of the active data file that was made during the backup cycle preceding that of the father.

d. Once a backup has been established for each generation, the cycle is continued by using the grandfather to

create a new son.

e. The time period between the creation of each new generation is determined by the user, based upon the sensitivity of the data.

f. Following the creation of each backup generation, the user should conduct a "Check Disk" of the storage media to insure that the media is not defective.

9-2. SOFTWARE BACKUP

Backup of AIS software applications is the responsibility of the TASO (Para 2-7j., 5-7a. & 8-2d.).

9-3. CONTINUITY OF OPERATIONS PLAN (COOP)

a. TASOs of multi-terminal/network systems will prepare a COOP for their AIS. A copy of the COOP, and backup copies of critical files and software, are to be stored in a location which would not be threatened by an emergency or disaster that would damage or destroy the AIS (para 8-2d.).

b. The COOP will address the following:

(1) Who maintains the files for each functional area.

(2) Established criteria for activation.

(3) Identification of the backup AIS, and point of contact.

(4) Backup AIS utilization plan (time sharing/scheduling).

(5) Signatures of the commanders of effected units.

(6) Evacuation plan for sensitive files.

CHAPTER 10
BATTLEFIELD AUTOMATION SYSTEMS (BAS)

10-1. GENERAL

Battlefield Automation Systems (BAS) are portable AIS designed for use in field or tactical environments. The compromise of a BAS has the potential to place vast amounts of information into the hands of hostile forces. Commanders and automation security personnel must therefore strive to ensure that automation security is attained and maintained in the field. It is DA policy to field BAS with built in security features. The principle tasks of AIS security personnel are to ensure proper utilization of the security features, establish AIS security procedures for the field environment, and integrate the BAS into the tactile posture of the unit.

10-2. PHYSICAL SECURITY

To meet the demands of hostile, mobile, and extremely stressful environments, ISSOs must develop physical security SOPs for their BAS, which address the following threat areas:

a. Transportation security - Protection against damage, misplacement of component parts, and access control appropriate to the sensitivity level of the system.

b. Destruction procedures - Criteria, priority, and means of destruction for the BAS and its storage media if threatened with capture.

c. Camouflage - Measures to be taken to conceal the BAS site, and its electronic and heat signatures.

d. MOPP - Operation and decontamination procedures for the BAS equipment and storage media.
e. Electromagnetic Pulse (EMP) - Procedures to protect the BAS from EMP resulting from nuclear detonations.

f. Environmental conditions - Operating procedures in inclement weather and other hazardous field conditions.

g. Communications security - Integration of the BAS into the command's COMSEC and TEMPEST SOPs.

h. Garrison security - Utilization, storage, access control, and equipment servicing requirements for the BAS when in garrison.

10-3. FILE AND SOFTWARE SECURITY.

a. AIS security personnel must ensure that BAS operators can:

(1) Operate the security features without difficulty.

(2) Recognize BAS security deficiencies and alerts.

(3) Respond to security alerts.

(4) Make minor adjustments to the security features.

(5) Purge the BAS when necessary.

b. Nonperishable, highly classified data must be stored in special, segregated tables and directories to facilitate purging or destruction in the event of capture.

c. The provisions of chapter 6 of this regulation are applicable to BAS and are to be complied with whenever practical.

10-4. HARDWARE SECURITY

BAS contain integral security features, with which operators are to be fully trained. Chapters 6 and 8 of this regulation are applicable to BAS and are to be complied with whenever practical.

10-5. PERSONNEL SECURITY

BAS are particularly vulnerable, due to the number of operators that may be authorized access in a tactical situation.

10-6. COMMUNICATIONS SECURITY

a. Transmission security and local COMSEC requirements must be practiced on a continual basis. BAS operators are to be trained to operate in a COMSEC environment, to identify COMSEC violations, and to take corrective actions.

b. Emission security and TEMPET requirements are to be practiced continually. BAS designed to be TEMPEST certified are to be handled to ensure continuous maintenance of TEMPEST certification criteria. Operators of such systems are to be trained to ensure the validity of TEMPEST certifications.

c. The provisions of chapter 7 of this regulation are applicable to BAS and are to complied with whenever practical.

10-7. ACCREDITATION

BAS must be accredited IAW Chapter 4 of this regulation.

FOR THE GOVERNOR:

JOSEPH J. SKAFF
Major General, WVARNG
The Adjutant General

Encls
A thru K

APPENDIX A

ISSO RECOMMENDATION

MEMORANDUM FOR See Distribution

SUBJECT: Recommendation for Appointment of Information Systems Security Officer (ISSO)

1. (NAME), (SSN), and (UNIT), is recommended for appointment as Information Systems Security Officer (ISSO). SECURITY CLEARANCE: (SECRET), PHONE #: XXX-XXX-XXXX.

2. AUTHORITY: AR 380-19

3. PURPOSE: Individual will report to the ISSM, senior ISSOs, and the commander, all practices dangerous to overall AIS security and instances of AIS security violations. He will also enforce the provisions of the authority referenced in item 2, guidance published by the state ISSM, and the unit's Information Security SOP.

4. Period: Until officially relieved or released from appointment or assignment.

5. Instructions: Individual will read and understand his/her duties and responsibilities as defined in AR 380-19 and the units Information Security SOP. Upon appointment, will conduct an initial review of all current accreditations for AIS over which responsibility has been assigned.

(SAMPLE RECOMMENDATION FOR ISSO APPOINTMENT)

XXXXXX
XXX, XX
XXXXXX

DISTRIBUTION:
1-Individual Concerned
1-ISSO, HQS
1-HQ STARC(-), ATTN: WVAR-DOIM

APPENDIX B

TASO APPOINTMENMT

MEMORANDUM FOR See Distribution

SUBJECT: Appointment of Terminal Area Security Officer (TASO)

1. (NAME), (SSN), and (UNIT), is appointed Terminal Area Security Officer (TASO). SECURITY CLEARANCE: (SECRET), PHONE #: XXX-XXX-XXXX.

2. SYSTEM: The Automated Information System(s) for which the above named individual is assigned responsibility is/are as identified by AIS ID number(s).

3. AUTHORITY:

4. PURPOSE: Individual will report to the unit ISSO and the commander, all practices dangerous to overall AIS security and all instances of AIS security violations. Will enforce the provisions of the authority referenced in item 3, guidance published by the state ISSM and unit ISSOs, and the unit's Information Security SOP.

5. Period: Until officially relieved or released from appointment or assignment.

6. Instructions: Individual will read and understand his/her duties and responsibilities as defined in AR 380-19, and the unit's Information Security SOP. Upon appointment, will conduct an initial review of all current accreditations for AIS over which responsibility has been assigned.

(SAMPLE FORMAT FOR TASO APPOINTMENT)

XXXXXX
XXX, XX
XXXXXX

DISTRIBUTION:
1-Individual Concerned
1-ISSO, HQS
1-HQ STARC(-), ATTN: WVAR-DOIM

APPENDIX C
ACKNOWLEDGEMENTS

I hereby acknowledge that I have been briefed as to my responsibilities and duties as a user of AIS equipment, and assets accredited for use by the ARNG. By signing this acknowledgment I affirm that:

1. I have read, understand, and will comply with the provisions of the unit automation security SOP and other applicable regulations.

2. I have been given an initial security briefing by the TASO.

3. I will access only those files, directories, and applications programs necessary to perform my assigned duties.

4. I will safeguard any assigned passwords from disclosure, and be accountable for any and all utilization of my passwords.

5. I will report to the TASO any disclosure of, or attempted unauthorized access to, sensitive defense information, and any AIS failure which could result in the unauthorized disclosure of such information.

6. I will report to the TASO any changes in my duties or responsibilities which impact upon my requirement for access to the AIS to which I have been granted access.

7. I will properly secure all sensitive information and media IAW the unit automation security SOP and other applicable regulations.

8. I will protect all AIS equipment and media against the detrimental effects of heat, liquids, smoke, magnetism, and other hazards.

9. I will properly label all storage media.

10. I will properly document any applications programs I create.

11. I will maintain appropriate backups of my critical files and applications programs.

12. I will not install software without authorization from the office of the DOIM.

13. I will not copy, destroy or alter files, records, or applications nor will I install them on another AIS, unless such utilization is IAW applicable regulations and assigned duties.

14. I will not violate the copyright privileges of any provider of software utilized by the WV ARNG.

_____ _____ _____

(Signature of User) (Date) CPU SERIAL #

APPENDIX D
CRITICALLY SENSITIVE PROCESSING
REQUIREMENTS ACKNOWLEDGEMENT

I hereby acknowledge that I have been briefed as to my responsibilities and duties as processor of Critically Sensitive (CS) information on the AIS equipment and assets identified below. By signing this statement I affirm that:

1. I have read, understand, and will comply with the provisions of applicable Information Systems Security regulations.

2. I will process critically sensitive files only on AIS accredited for a level of sensitivity equivalent to the sensitivity of the information I am processing.

3. I have received a TEMPEST briefing from my TASO, explaining the provisions of AR 530-4, prior to being granted access to critically sensitive files.

4. Prior to the conduct of processing on any critically sensitive files or data, I will:

   (a) Ensure the AIS, on which the processing will be conducted, is accredited for the level of sensitivity of the information to be processed.

   (b) Turn the power to the AIS and any peripheral devices off, and then back on.

   (c) Disconnect any/all modems or other communications lines.

   (d) Disconnect any/all peripheral devices (external hard disks, printers, plotters, remote workstations/terminals, etc.) not required for the conduct of the processing.

   (e) Display a placard indicating the classification level of the processing being conducted.

   (f) Secure the area to prevent access by unauthorized personnel.

   (g) Ensure that the display screen is positioned to prevent viewing by unauthorized personnel, either within or outside the processing area.

5. During the conduct of processing on any critically sensitive files or data, I will:

   (a) Prevent viewing of the display screen by unauthorized personnel.

(b) Ensure that no critically sensitive data is transferred to, stored on, or otherwise placed onto the AIS's fixed (internal) disk drive, or any other fixed memory location.

(c) Not leave the information or the AIS unattended for any reason, without first terminating the processing session as described in item 6 below.

6. Upon termination of the processing session, I will:

(a) Remove all critically sensitive media from the AIS.

(b) Ensure all critically sensitive media is properly labeled, to indicate its level of sensitivity.

(c) Clear the random access memory (RAM) of the AIS, and the memory buffers of peripheral devices utilized during the processing session, by utilizing a clearing program provided by the SSM.

(d) Turn off the power to the AIS and any peripheral devices.

(e) Reconnect any peripheral devices that were disconnected prior to the processing session.

(f) Reconnect any modems or communications lines that were disconnected prior to the processing session.

(g) Store the critically sensitive media as required for its level of sensitivity.

_____ _____ _____

(Signature of User) (Date) CPU SERIAL #

_____

(Signature of TASO)

APPENDIX F
ARNG AIS FACILITY SECURITY PROFILE

1. Facility Identification: _____

   a. Address: _____
   (street, city, zip)

   b. Organization/Activity/Unit: _____

   c. Building, Floor & Room #: _____

   d. **Attach Facility Diagram (n/a Laptops & BAS)**
   OR
   Attach System Security SOP (Laptops & BAS only)

2. AIS **CPU Serial #**: _____

3. AIS Equipment Description: (Attach copy of hand receipt)

4. Connected or Proposed Telecommunications Capabilities:

   a. Does/will the system utilize:
   (1) dial-up telephone [ ]
   (2) auto-dial modem [ ]
   (3) auto-answer modem [ ]
   (4) direct wire [ ]
   (5) No communications [ ]

   b. If AIS is the host for a network, list the location and type of device(s) connected, and attach diagrams of all remote terminal locations:

5. Categories of Information/Data processed by this AIS:

   a. CS2 (Top Secret) _____ %
   b. CS3 (Secret/Confidential) _____ %
   c. Highly Sensitive (FOUO) _____ %
   d. Sensitive (Proprietary/Contractual) _____ %
   e. Nonsensitive: _____ %
   TOTAL = 100 %

6. Personnel Security and Surety Program (PSSP).

   a. Level of clearance required to operate the AIS:
   Unclassified/FOUO _____
   Secret/Confidential _____
   Top Secret _____

b. Number of personnel authorized to operate system: _____

c. Number of Security clearances, by type, of authorized users:

(1) Secret or above: _____
(2) Confidential: _____
(3) No Clearance: _____

d. Status of personnel without valid security clearances:

(1) Number of personnel with completed NAC, ENTNAC, or NACI investigations but no clearance issued: _____

(2) Number of personnel with pending NAC, ENTNAC, or NACI investigations but no clearance issued: _____

(3) Number of personnel without any investigations initiated or pending: _____

7. TASO's Certification for computer CPU SERIAL #: _____

a. Date of TASO Inspection: _____

b. TASO's signature: _____

c. ATTACH COPY OF TASO APPOINTMENT LETTER (Appendix B).

8. ISSO's recommendation:

a. I have reviewed this document and recommend a level of:

(1) Non Sensitive [ ] (3) Highly Sensitive [ ]
(2) Sensitive [ ] (4) Critically Sensitive [ ]

b. Date of ISSO recommendation: _____

c. ISSO's signature: _____
(Type name & rank) _____

9. Major Command ISSO's review:

I have reviewed this document and concur with recommendation for the indicated accreditation level.

a. Date reviewed: _____

b. ISSO's signature: _____
(Type name & rank) _____

10. State System Security Manager's (SSM) Approval:

a. Action: APPROVED DISAPPROVED SITE VISIT REQUIRED

b. Level: US-2 S HS FORWARD FOR CS APPROVAL

c. Date reviewed: _____

d. SSM's Signature: _____

11. Fundamental Criteria:

a. Will this AIS process classified defense data at any time? (CONFIDENTIAL or above):

YES [ ]
NO [ ]

b. Will this AIS process defense data that is FOR OFFICIAL USE ONLY or meets the requirements of PRIVACY ACT information?

YES [ ]
NO [ ]

c. Mission Criticality: (Consider the consequences to the mission if data is lost).

Peacetime: [ ] High
[ ] Low

Wartime: [ ] High
[ ] Low
[ ] None (not a mobilization asset)

d. Sensitivity Level of Data:

[ ] Critically Sensitive
(Confidential and above)
[ ] Highly Sensitive (FOUO & Privacy Act)
[ ] Sensitive
[ ] Nonsensitive

e. Theft/Vandalism Threat:

[ ] High
[ ] Moderate
[ ] Low

f. Local Intelligence Threat:

[ ] High
[ ] Moderate
[ ] Low

-STOP- NO further processing is required if questions a. and b. above are both answered "NO" and questions c. thru f. are answered "none & none, nonsensitive, low, and none".

12. Risk Assessment (Access Controls):

-ISSO- (Vulnerability?)	-TASO- (Status?)	
____ YES ____ NO	____ YES ____ NO	a. Is user authorization and identification authenticated in some manner, and are signed and current AIS Conditions of Use Acknowledgment on file for all authorized users?
____ YES ____ NO	____ YES ____ NO	b. Could an unauthorized user destroy or compromise valuable data by playing with the unattended AIS?
____ YES ____ NO	____ YES ____ NO	c. Do you log off the AIS, or secure it, when it is not in use and during periods when it is unattended (out of your physical control)?

13. Risk Assessment (Magnetic Media Protection):

____ YES ____ NO	____ YES ____ NO	a. Are all of your magnetic media labeled to indicate file name(s), user, and owning organization?
____ YES ____ NO	____ YES ____ NO	b. Are semipermanent gum type labels of all media and their protective containers, which reflect the sensitivity level of information on them?
____ YES ____ NO ____ N/A	____ YES ____ NO ____ N/A	c. If your AIS is configured with an internal disk drive, is it labeled to indicate the highest level of information that may be processed or stored on it?
____ YES ____ NO ____ N/A	____ YES ____ NO ____ N/A	d. If your AIS is configured with an internal disk drive, have precautions been taken to protect it from accidental or malicious formatting?
____ YES	____ YES	e. Do you have a lockable container or cabinet in which

____ NO	____ NO	to store sensitive magnetic media when it is not in use?

14. Risk Assessment (File Protection):

____ YES ____ NO	____ YES ____ NO	a. Do you use write protection to prevent the accidental destruction of your files contained on removable media (i.e. diskettes)?
____ YES ____ NO ____ N/A	____ YES ____ NO ____ N/A	b. If you have multiple users accessing sensitive files on hard disks, and all users do not have a need-to-know, are either hardware or software based security mechanisms used to provide file access control?

15. Risk Assessment (Software Security):

____ YES ____ NO ____ N/A	____ YES ____ NO ____ N/A	a. Does your local user developed software include as a minimum, a program description, sample I/O formats, the security/privacy requirements and source code?
____ YES ____ NO	____ YES ____ NO	b. Are you protecting vendor and proprietary software by properly accounting for the original media, protecting them from damage or loss, and are you aware that user made copies are either limited or prohibited by law?

16. Risk Assessment (Physical and Environmental Security):

____ YES ____ NO	____ YES ____ NO	a. Is the AIS room or building locked during non-duty hours, and is the AIS secure when you are not present during the day?
____ YES ____ NO	____ YES ____ NO	b. Is a serial number inventory maintained of the AIS equipment and is it periodically validated?
____ YES	____ YES	c. Is a placard posted which prohibits the environmental

____ NO	____ NO		hazards of eating, drinking, and smoking around the AIS?
____ YES	____ YES	d.	If static electricity poses a potential problem in the AIS area, have measures taken to control its effects on the system (i.e. anti-static mats, electrical grounds)?
____ NO	____ NO		
____ N/A	____ N/A		
____ YES	____ YES	e.	Are portable class "C" fire extinguishers available in, or within 50 feet of, the AIS room? (N/A only to laptops)
____ NO	____ NO		
____ N/A	____ N/A		

17. Risk Assessment (Document Security):

____ YES	____ YES	a.	Do you know who the Privacy Act Official is that serves as the state advisor on Privacy matters?
____ NO	____ NO		
____ YES	____ YES	b.	Are all output and storage media containing Privacy Act data labeled "FOR OFFICIAL USE ONLY"?
____ NO	____ NO		
____ YES	____ YES	c.	Is authorization and positive identification established prior to releasing personal information?
____ NO	____ NO		
____ YES	____ YES	d.	Is Privacy Act data disposed of by either melting, shredding, or burning?
____ NO	____ NO		
____ YES	____ YES	e.	Do you maintain backup copies of operating system software and critical data files outside of the AIS room?
____ NO	____ NO		
____ YES	____ YES	f.	Is it understood by all personnel that if there is a suspected security violation involving the AIS, that initial notification is to be sent through the ISSO to the SSM within five working days?
____ NO	____ NO		

18. Risk Assessment (Classified Processing Procedures):

	____ YES	a. Is the AIS to be utilized for

____ NO

processing of Critically Sensitive (CONFIDENTIAL, SECRET, TOP SECRET) information or data?

-STOP- NO further processing is required if item # 18a. above is answered "NO".

____ YES ____ YES b. Do you have a GSA approved security container available
____ NO ____ NO in your working area in which to store removable classified media?

____ YES ____ YES c. Do you have storage area, approved in accordance with
____ NO ____ NO Appendix F AR 380-5, to store nonremovable media containing classified information?

*(Attach appropriate documentation)

____ YES ____ YES d. Do you understand that media which contains classified
____ NO ____ NO COMSEC material marked CRYPTO is not to be declassified?

____ YES ____ YES e. Are you using one of the approved methods of
____ NO ____ NO destruction for your classified magnetic media, such as cutting, incineration, or melting at temperature above 6000 F?

____ YES ____ YES f. Are the eight (8) procedures listed below practiced by ALL
____ NO ____ NO users during ALL classified processing sessions?

TASO INITIALS

1. Ensure the AIS is accredited for the level of classified information to be processed? _____
2. Turn the power to the AIS off, then back on prior to beginning the session. _____
3. Physical disconnect all modems and/or communications lines. _____
4. Disconnect any peripheral devices not required for the processing session. _____

5. Display a placard indicating that classified processing is being conducted. _____

6. Secure the processing area to prevent access by unauthorized personnel. _____

7. Ensure that the display screen cannot be viewed by unauthorized personnel. _____

8. After the session, media is removed, and the AIS is cleared the powered down in accordance with local procedures. _____

____ YES	____ YES	g. Are signed and current Critically Sensitive Processing Requirements Acknowledgments on file for all authorized users of the system?
____ NO	____ NO	

APPENDIX G
LAPTOP PERSONNEL COMPUTER UTILIZATION SOP

Due to the highly portable nature of laptop personnel computers, the ability to take them into various environments, and the likelihood that they may be utilized by various users, the following procedures will be practiced when utilizing them:

A. Data sensitivity restrictions:

(1) Classified and sensitive information is not to be processed at any location other than government or approved government contractor facilities.

(2) Classified and Sensitive information is not to be stored on the internal fixed disk drives. Such information is to be stored on removable diskettes and secured in a manner appropriate to its level of sensitivity.

(3) Classified media may not be carried on commercial aircraft without written courier orders IAW AR 380-5, paragraphs 8-300 thru 8-302.

(4) Neither the computer, or its magnetic media are to be passed through any device which would radiate or x-ray them.

B. The computer is not to be operated at any time, or location, which would permit the information being processed to be viewed by unauthorized personnel.

C. Physical Security Requirements:

(1) Laptops are not to be left unattended in public or common use area.

(2) If the computer must be left unattended it is to be secured in a container or room controlled by lock and key.

(3) If secured in a hotel room, or other transient quarters, the computer is to be stored out of sight (i.e. in a locker or drawer).

D. Transport Requirements:

(1) Laptops will be placed into the "SHIP" mode prior to any movement or relocation.

(2) When transported in automobiles, computer are to be either placed on the floor of the vehicle, or, if placed on a seat, secured to prevent movement or falling in the event of mishap or accidents.

(3) If shipped in hold baggage, computers are to be packed in secured luggage or containers, in addition to their carrying bag, and padded sufficiently to protect against rough handling.

(4) Computers are not to be transported by any means which would cause them to be exposed to inclement weather conditions.

(5) Laptops are not to be operated in pressurized aircraft cabins while in flight, due to the potential for data loss from static discharge induced by the rarefied atmosphere.

E. If a laptop was released to a user on a temporary hand receipt, for utilization during a specified period, it is the responsibility of the user to transfer any and all user information to removable media prior to its return.

F. Laptops, which are maintained for the purpose of temporary issue to various users, will be purged of all user data files, upon their return.

G. A copy of the accreditation documents and this SOP are to be kept with the computer at all times.

APPENDIX H
LETTER OF ACCREDITATION

MEMORANDUM THRU: Expires: (DATE)

Sr. ISSO, HQS

ISSO

FOR: TASO

SUBJECT: Letter of Accreditation, System ID #

1. Reference:

a. Paragraph , AR 380-19, Information Systems Security

2. I have carefully considered the actual and potential threats to and vulnerability of the ZENITH CPU, SN# 1234567890 utilized at .

3. Weighing the threats and vulnerabilities against the system's operational requirements and the security measures which have been implemented an/or planned, I have determined that the level of accreditation requested is in the best interest of the Army National Guard and its mission.

4. Accordingly, under the authority granted by the above referenced regulations, delegated by the Chief, NGB IAW AR 380-19, I accredit this system as ID # , for the processing of Highly Sensitive data.

5. Point of Conduct for this action is the DOIM Information Systems Security Officer (304-341-6454).

FOR THE ADJUTANT GENERAL:

(SAMPLE ACCREDITATION LETTER)

XXXXXX
XXX, XX, XXXX
XXXXXXX

3 Encls:
1. Accreditation Documentation
2. TASO Appointment Letter
3. AIS Hand Receipt

APPENDIX I
ACCREDIDATION REVIEW CHECKLIST

DATE OF REVIEW_____ SYSTEM ID #:_____

REVIEWING OFFICER

NAME AND GRADE:_____

ORGANIZATION: _____

PHONE NUMBER: _____

REASON FOR REVIEW: ISSO ANNUAL INSPECTION [ ]

SSM INSPECTION [ ]

OTHER: _____

A. TASO's AIS SECURITY FILE

1. Is an individual Security File established for the AIS?	YES	NO	
2. Is an accreditation letter on file for the AIS?	YES	NO	
3. Is the accreditation letter current? (CS valid for one year, all years valid for two years)	YES	NO	
4. Is the AIS Facility Security Profile on file, current and accurate?	YES	NO	
5. Is the Continuity of Operations Plan on file? (applicable only to network hosts)	YES	NO	N/A
6. Is a copy of the AIS hand receipt on file, are all items on hand, and serial numbers correct?	YES	NO	
7. Is an accurate AIS installation/location diagram on file. (n/a to portables or BAS)	YES	NO	N/A
8. If the system is the host for a network of remote terminal, are installation/location diagrams on hand indicating their current locations?	YES	NO	N/A
9. Are copies of previous security inspections and accreditation reviews on file?	YES	NO	N/A
10. Have all previous security inspection or	YES	NO	N/A

accreditation review deficiencies been corrected?

11. Are current AIS Conditions of Use Acknowledgments on file for all authorized users? (valid for one year) YES NO

12. Are currently Critically Sensitive Processing Requirements Acknowledgments on file for all authorized users? (valid for one year, CS3 accredited AIS only) YES NO N/A

13. If the AIS is equipped with a telecommunications capability, is a written order appointing authorized users on file? YES NO N/A

B. TASO's SECURITY REFERENCES

1. Are the TASO's appointment orders on file? YES NO

2. Are the following reference materials available:

(1) AR Reg 380-19 YES NO

(2) WVMR 380-19 YES NO

3. Is a file being maintained for official correspondence concerning AIS security? YES NO

C. IMPLEMENTATION OF AIS SECURITY PROCEDURES

1. Does the TASO employ effective means of restricting unauthorized access to the AIS? YES NO

2. Is the system appropriately accredited for the level of sensitivity of information processed? YES NO

3. Is the system properly labeled to indicate its current level of accreditation? YES NO

4. Is all magnetic storage media appropriately labeled for identification and sensitivity? YES NO

5. Is sensitive information properly secured when not in use or when left unattended? YES NO

6. Is class "C" fire suppression equipment available within 50 feet of the AIS? (n/a to Laptops) YES NO N/A

7. Is all software installed on the system authorized by the DOIM, and posted on the system's software authorization letter? YES NO

8. Are copies of the Utilization SOP and accreditation documents kept with the system? (portables & BAS only)	YES	NO	N/A
9. Is the AIS installed and operated in a hazard free area and manner, and is appropriate signage posted prohibiting smoking, eating, and drinking?	YES	NO	
10. Are backups of all commercial software and critical user files being maintained?	YES	NO	
11. Are CS and TEMPEST security procedures enforced during all classified processing sessions? (CS accredited AIS only)	YES	NO	N/A
12. Are classified files and data properly secured IAW applicable regulations? (CS accredited AIS only)	YES	NO	N/A

D. COMMENT ON ALL "NO" AND "N/A" ANSWERS (index by letter & number):

(Attach additional pages as required)

_____ _____

(Signature of inspector) (date)

APPENDIX J
ACCREDITATION SUSPENSION LETTER

MEMORANDUM THRU: Expires: (DATE)

ISSO

FOR: TASO

SUBJECT: Suspension of Accreditation, System ID #

1. Reference: AR 380-19

2. I have carefully considered the actual and potential threats to and vulnerability of the Automated Information System located at for the processing of Highly Sensitive data.

3. Weighing the threats and vulnerabilities against the system's operational requirements and the results of the Accreditation Review recently conducted on the system (attached), I have determined that it is in the best interest of the WV ARNG to temporarily suspend the accreditation of the ZENITH CPU, SN# 1234567890, ID # until the identified deficiencies are corrected.

4. Accordingly, under the authority granted me by the regulations referenced above, I am recommending that the SSM direct the cancellation of all password access to the system until such time as the suspension is lifted.

5. Point of Conduct for this action is XXXXX XXXX XXXXX.

(SAMPLE ACCREDITATION SUSPENSION LETTER)

XXXXXXXX
XXX, XX, XXXX
XXXXXX

Encl:
Accreditation Review Checklist

CF:
1-HQ STARC(-), ATTN: WVAR-DOIM

APPENDIX K
ISSO SECURITY INSPECTION

DATE OF INSPECTION: _____

ISSO's NAME, GRADE & UNIT: _____

INSPECTOR'S NAME, GRADE & UNIT: _____

INSPECTOR'S PHONE NUMBER: _____

REASON FOR INSPECTION: SSM SECURITY INSPECTION [ ]

COMMAND INSPECTION [ ]

OTHER: _____

1. Is an AIS Security File maintained on each system for which the ISSO is responsible?	YES	NO	
2. Is an accreditation letter on file for each of the AIS for which the ISSO is responsible?	YES	NO	
3. Are all of the accreditation letters current?	YES	NO	
4. Is a copy of the State order appointing the ISSO to his/her position on file?	YES	NO	
5. Are appointment letters on file, appointing a TASO for every AIS for which the ISSO is responsible?	YES	NO	
6. If the ISSO is a Senior ISSO, are ISSO Security Inspection Reports on file indicating that all subordinate ADPSSOs have been inspected within the last year?	YES	NO	N/A
7. Has the ISSO conducted Accreditation Reviews for those AIS that have not been either accredited or reaccredited in the last twelve months?	YES	NO	
8. Are copies of Accreditation Reviews kept on file for three years as required?	YES	NO	
9. Have all previous ISSO Security Inspection and Accreditation Review deficiencies been corrected?	YES	NO	N/A
10. Is a file maintained for official correspondence concerning automation security?	YES	NO	
11. Does the ISSO have a copy of AR 380-19?	YES	NO	
12. Does the ISSO have a copy of WVMR 380-19	YES	NO	

13. Has the ISSO developed and implemented an automation security SOP? YES NO

14. Are AIS assets equably distributed throughout the command? YES NO

15. Are utilization schedules posted, for those AIS that are shared by multiple units/activities? YES NO N/A

16. Are shared AIS installed in conveniently assessable common use area? YES NO N/A

17. Conduct accreditation reviews for a minimum of 25% of the AIS for which the ISSO is responsible. Attach the completed reviews to this document, and enter the system ID #'s on the line below:

_____.

18. Explain all "NO" answers, index by question number.

(Attach additional pages as required)

_____ _____
(Signature of inspector) (Date)