

Kansas National Guard
Regulation 25-1

State of Kansas, Military Division
The Adjutant General's Department
Topeka, Kansas 1 June 1996

Information Management

INFORMATION RESOURCES MANAGEMENT PROGRAM

Summary. This regulation prescribes procedures for acquiring, managing, operating, maintaining, securing and obtaining training for automation, communications and visual information systems within the Kansas Army National Guard.

Applicability. This regulation applies to the department, as a State agency and a military headquarters, the Kansas Army National Guard (KSARNG).

Internal Control Systems. This regulation contains management control provisions but does not contain checklists for reviews.

Supplementation. This regulation may be supplemented by HQ 35th Division and HQ, 69th Troop Command. Supplement must be coordinated with the Directorate of Information Management (DOIM).

Suggested Improvements. The proponent of this regulation is the Directorate of Information Management. Users are invited to send comments and suggested improvements directly to the Adjutant General's Department, ATTN: AGKS-DOIM, 2800 Topeka Ave, Topeka KS 66611-1287.



1 June 1996

1. General

1.1 Purpose

This regulation provides guidance for managing, acquiring, operating, maintaining and securing information resources management assets for the Kansas Army National Guard.

1.2 References

- a. AR 5-3, Installation Management and Organization
- b. AR 25-1, The Army Information Resources Management Program.
- c. AR 25-30, The Army Integrated Publishing and Printing Program.
- d. AR 380-19, Information Systems Security.
- e. AR 380-67, The Department of the Army Personnel Security Program.
- f. AR 380-5, The Department of the Army Information Security Program.
- g. AR 27-60, Intellectual Property.
- h. AR 380-19-1(C), Control of Compromising Emanations.
- i. AR 335-15, Management Information Control System.
- j. KS-SOP 105-23, Telecommunications
- k. KS-SOP 380-19, Information Systems Security

1.3 General

Microprocessor technology has provided the military office with automated data processing equipment (ADPE), via personal computers, facsimile (FAX) communication equipment and sophisticated visual processing equipment. This technology has significantly enhanced the user's ability to produce numerous quality products. For purposes of this regulation, the term microcomputer includes electronic data processing devices using microprocessor technology which are designed for office environments. These devices are usually single-user desktop systems, but also include small multi-user systems, laptop and portable devices. Facsimile and visual processing equipment include commercially available systems intended for the office environment. This regulation does not address specific detail regarding information systems that are designed for tactical operations.

1.4 Objectives

The objective of this regulation is to provide uniform procedures to:

- a. Provide a program to effectively manage and use automation assets.
- b. Promote the use of compatible hardware systems.
- c. Promote the use of off-the-shelf standard software programs approved/supported by the DOIM.
- d. Promote the development of standard applications used throughout the Adjutant General's Department.
- e. Ensure that users are provided with required automation equipment, training and support.
- f. Ensure the Adjutant General's Department is in compliance with current DOD, U.S. Army and National Guard Bureau (NGB) Regulations and Directives.

2. Responsibilities

The Kansas Army National Guard DOIM is established to manage multi-discipline information service support activities for efficiency and effectiveness. The DOIM is responsible for the management of telecommunications facilities to include voice, video, and computer communications lines, local area networks, PBX systems, interfaces to other networks and facsimile systems; for data/information processing facilities and associated computers, software, peripherals, and associated services and support; for visual information services; and for records management activities including publications and forms, printing/duplication and information distribution.

a. To ensure the efficient management and utilization of microcomputer assets, the following responsibilities are assigned to the Director of Information Management:

(1) Coordinate/Approve all KSARNG automation requirements IAW AR 25-1, Chapter 3, the Army Information Management Plan (IMP), and KSARNG Information Requirement Statement (IRS).

(2) Provide for the training of personnel on computer software approved by the DOIM.

(3) Assist users in formulating applications for micro-computers and solving technical operational problems.

(4) Serve as the Adjutant General's technical advisor for automation requirements and activities.

(5) Research and develop automation standards to ensure compatibility with the NGB and DOD.

Contents

Paragraph	Page
1. General.....	1
1.1 Purpose.....	1
1.2 References.....	1
1.3 General.....	1
1.4 Objectives.....	2
2. Responsibilities.....	2
2.1 Acquisition.....	4
3. Standardization.....	6
4. Training.....	6
4.1 Equipment Installation.....	7
4.2 Accountability.....	8
4.3 Maintenance.....	8
4.4 Supplies.....	8
4.5 Operations.....	8
5. Security (See KSSOP 380-19).....	9
6. Accreditation.....	10
6.1 Non DOD Computers.....	10
7. Automation Support.....	10

APPENDIXES

A- Control of Hardware and Software.....	1
B- Microcomputer Temporary Loan Program.....	1
C- Development of Computer Software.....	1
D- Appointment of ISSO and TASO.....	1
E-Information Management Advisory Council (IMAC).....	1
F- Use of Computers outside Office Envrironments.....	1
G- Maintenance.....	1
TAB 1- Maintenance Allocation Chart.....	1
H- Computer Training.....	1
I- Personal Computers.....	1
J- FAX Operations.....	1
K- Visual Information.....	1
19.1.1 General.....	1
19.1.2 Functional Requirements.....	4
19.1.3 Equipment Requirements.....	6
19.1.4 Long Term Requirements.....	7
19.1.5 Equipment Terms.....	8
L- Reaccreditation Requirements.....	1
M- NGNET and Bulletin Board.....	1
N- Tempest Control Officer.....	1
O- Disposition of Equipment.....	1
P- Communications.....	1
Q- Admin Services.....	1
R- Blank Forms.....	1



1 June 1996

(6) Coordinate and develop long-range automation, visual information and telecommunications plans for the Adjutant General's Department.

(7) Assist functional users in developing information management-related budget requirements.

(8) Provide for the maintenance of computer systems hardware.

(9) Serve as the KSARNG Information System Security Manager (ISSM) which advises and assists functional users with microcomputer security and accreditation requirements IAW AR 380-19 and KSSOP 380-19.

(10) Serve as member of the Information Management Advisory Council (IMAC) for the Adjutant General's Department. The DOIM also represents the units under the command and control of the STARC.

b. Major Subordinate Commands (MSC) will appoint on orders an Information Management Officer (IMO) to serve as the automation point of contact (POC). The IMO, who may also function as the ISSO or Terminal Area Security Officer (TASO), will:

(1) Serve as the interface between the functional user and the chain of command and the IMAC for all automation programs and security activities.

(2) Contact the DOIM in order to obtain assistance or instructions for resolution of any problems encountered with installed microcomputer systems (e.g. hardware, software, communications, etc.).

(3) Ensure that office environment is appropriate for the automation equipment. (i.e. sufficient outlets, proper current etc)

(4) Coordinate and manage unit/activity functional area software applications. (i.e. ULLS-S4, ATRRS etc)

(5) Provide the DOIM with copies of new or updated locally prepared software application programs for the KSARNG application directory.

(6) Submit requests for training, equipment, software and programming support for microcomputer systems through appropriate channels to their IMAC Rep.

c. Units and Battalions will appoint ISSO's and TASO's in accordance with KSSOP 380-19. In addition to the duties in KSSOP 380-19 the ISSO's and TASO's will also:

(1) Serve as the interface between the functional user at CO level and the BDE or MSC ISSO as the Command Information Management Officer (IMO) for all automation programs and security matters.

(2) Contact the next higher IMO in order to obtain any assistance or instructions for resolving problems with installed microcomputer systems (i.e., hardware, software, communications, etc.).

(3) Ensure that office preparation actions are initiated prior to or in conjunction with the delivery of automation equipment. (Proper electrical service etc)

(4) Provide the next higher IMO with copies of new or updated locally prepared software application programs for the KSARNG application directory.

(5) Submit requests for training, equipment, software and programming support for microcomputer through appropriate channels to the IMAC.

(6) Assist ISSO to initiate a security accreditation request for all new systems, and systems which have been moved to new locations, and forward through command channels to the DOIM.

2.1 Acquisition

a. The acquisition, management, and use of microcomputers is subject to existing Federal Acquisition Regulations (FAR's), DA Automation Regulations, US Army Microcomputer Contracts, the Reserve Component Automation System (RCAS) Program and policy contained in this regulation. The KSARNG microcomputer policy is based on centralized acquisition and decentralized management. See Appendix A.

b. Under NGB policy, automation requirements are implemented to satisfy mission requirements within congressional guidelines outlined in the RCAS program. Mission requirements that cannot be economically supported by current automation capabilities may be supported by new acquisition after approval by NGB. All newly acquired automation hardware will be compatible with both current and planned microcomputer systems to the greatest extent possible.

c. Unique unit/activity programming to support the use of off-the-shelf software is the responsibility of the user. Custom designed software will not be routinely developed by DOIM, nor will the DOIM provide maintenance support for user-developed software. Users are required to submit locally developed programs to the DOIM for review. Software which has general application to the KSARNG and which has received DOIM approval, will be incorporated as standard KSARNG software programs. All approved programs will be supported by the DOIM. See Appendix C.

1 June 1996

d. Access to other KSARNG automated systems.

(1) A microcomputer with dial-up communications capabilities functions as a computer terminal when accessing another computer system. (Terminal Emulation)

(2) System access shall be restricted by the Host Computer as to functions and activity. Only approved programs will be used to accomplish these functions. (BLAST, Enable, PROCOMM)

(3) The ISSO for each host computer system is the authority for determining user access to a host computer system.

e. Classified Operations.

(1) CLASSIFIED INFORMATION. Classified information may be processed only on systems approved/accredited for Classified Sensitive 3 (CS3) (SECRET/CONFIDENTIAL) operations. All CS3 systems must have a security accreditation for that level prior to operations. Accreditation by the KSARNG Systems Security Manager is required prior to initiating classified operations. Classified information may not be stored on non-removable disk drive systems. Reference AR 380-19, Chapter 2 concerning Computer Security and the Personnel Training and Awareness Program requirements for individuals who work with automation systems.

(2) PRIVACY ACT DATA. All users must safeguard systems which contain personnel data covered by the Privacy Act of 1974, Public Law 93-597, Title 5, protection of Privacy Act Data, IAW 340-21.

f. Software Piracy.

(1) Software Licensing Agreement. Users will read and comply with all software licensing agreements. This includes prohibitions against copying material (disks and manuals) legally protected by copyrights and using software on more than one PC. If multiple copies of a program are needed they must be individually purchased. It is in violation of U.S. Copyright Laws (see AR 27-60) to copy or reproduce computer programs unless they are in the public domain. Each program may have additional limitations and restrictions based on license agreement.

(2) Copying. Some software licenses allow a user to backup a program in case the master program diskette is damaged. Making copies to share with other computer users, or copying a program for use at home is PROHIBITED, unless allowed by specific software license agreement.

g. Personal use of government owned computers. The use of government owned computers for private/personal endeavors is

PROHIBITED. Such endeavors include personal use, use by clubs or other organizations, for corporate business, playing computer games or any other activity which does not specifically support the mission. Violations of this policy will be reported immediately to the TASO, ISSO and through command channels to the Information System Security Manager (ISSM), KSARNG, who is the DOIM.

3. Standardization

Microcomputer technology acquired by the KSARNG enhances the ability of the user/decision maker to share and exchange information. Achieving this objective is possible only by adherence to the following principles of standardization:

a. Software Applications. Software applications must use and manipulate data in a manner that is appropriate and consistent with the requirements of the functional area. Software applications will be developed with the involvement of functional channels at all levels of command.

b. Hardware/Software. The use of standardized microcomputer hardware and software ensures that computer systems are compatible throughout the KSARNG. The DOIM is responsible for the selection of hardware and software compatible for both existing and projected computer systems.

c. Reference Library. Reference library materials for standard hardware and software may be obtained from the DOIM, AGKS-DOIM. Requests will be submitted through normal command channels.

4. Training

a. Formal computer software training is available for all users. Units/Activities will submit written requests through command channels for coordination and approval for training. See Appendix I.

b. The DOIM is responsible for submitting an annual training budget to the NGB, Information Management Agency. This dollar budget is based upon the total number of training requests required by Adjutant General's Department, units and activities during the fiscal year.

c. Users are provided documentation when initial hardware and software is issued (e.g., user's guides, reference manuals, owner's manuals). It is the responsibility of the user to read and understand the instructions prior to using the computer. Users will maintain and secure the manuals and disks as "proof" of legal software.

d. Instructional software is available from AGKS-DOIM for selected standard applications. Submit requests through normal command channels.

4.1 Equipment Installation

a. Location of Automation Equipment. Computer equipment must be located in an acceptable environment. The environment is normally described in the manufacturer's warranty literature. The following guidelines also apply:

(1) Each unit/activity and ISSO/TASO will ensure that newly acquired equipment is located in the prescribed environment and is physically secure.

(2) Automation equipment can be operated on an office table or desk. Furniture designed specifically for computers and peripheral devices is available through supply channels on a limited basis.

(3) The area in which a microcomputer is located should be dust and smoke free. No food or drinks are permitted near the computer.

(4) Static electricity is a major concern in dry locations and carpeted areas. It can destroy the internal components of a microcomputer. Static electricity can also damage or erase a floppy diskette. If static electricity is a problem, units should consider acquiring anti-static mats or a humidifier.

(5) Do not locate automation equipment by windows or doorways. Keeping equipment out of sight from unauthorized observers reduces the possibility of theft. Protect all automated systems from direct sunlight and excessive heat/cold sources. Do not block computer equipment air vents. Provide adequate ventilation for all automated equipment.

(6) The location of the Central Processing Unit (CPU) is important. Do not locate adjacent to the printer in such a way that the CPU will ingest paper dust emitting from the printer.

(7) For use of microcomputers outside the normal office environment, refer to Appendix G.

b. Power Supply. Microcomputers must be protected from damage by power surges. Only a surge protector and the printer should be plugged directly into a standard wall outlet. All other equipment, i.e., the microcomputer, modem, and external drives will be plugged into a protected power supply. Unplugging all computer equipment, including telephone and the modem telephone connection, on weekends and during electrical storms is a precaution against power surges and may prevent extensive damage to the equipment.

4.2 Accountability

HQ DA requires an inventory be maintained for all automated data processing equipment (ADPE) over \$100. Each major command is responsible for their respective inventories. Property Book Officers (PBO's) are responsible for proper issue, transfer, and turn in of any computer component. Individual hand receipt holders are responsible to insure accountability of all computer equipment and software.

4.3 Maintenance

a. The DOIM office will submit an annual budget document request for projected maintenance costs.

b. Units/Activities will notify their Information Management Officer (IMO) immediately if there are any problems with hardware or software. The IMO will coordinate with the DOIM as necessary. Maintenance for microcomputer systems can be authorized only by CSMS. See Appendix H.

4.4 Supplies

Microcomputer supplies will be procured by submitting the appropriate request through supply channels. Expendable supplies such as diskettes, ribbons, and paper are obtained at the supporting SSSC. Request for supplies unavailable thru the SSSC are forwarded to the DOIM. Furniture is obtained through normal supply channels.

4.5 Operations

a. Power Up/Down Procedures. Specific instructions for the power up/down sequence are contained in each microcomputer system's operating instructions. Adherence to these procedures is MANDATORY. Failure to follow these instructions can result in damage to the microcomputer and peripherals and may also void the manufacturer's warranty.

b. Diskettes. Diskettes are precision recording media and are easily damaged. The following procedures for the care and maintenance of diskettes should be followed:

(1) Keep the diskette in its storage envelope or folder when not in use.

(2) Keep diskette away from magnetic fields. Magnetic fields will erase the data stored on a diskette.

(3) Do not touch the exposed area of a diskette or try to wipe or clean. Diskettes scratch easily.

(4) Diskettes must be kept out of the sun and away from extreme heat and cold.

1 June 1996

(5) Do not write on the diskette jacket or on a diskette label with a pencil or other hard point device. ONLY A FELT TIP PEN SHOULD BE USED FOR MARKING OF DISKETTES AND JACKETS.

(6) Store diskettes vertically in a diskette file to avoid pressure to their sides.

(7) Protect diskettes from theft by securing them in a locked area.

c. Backup Data. Making backup copies of diskettes or tape if available is a good data processing practice. Backup copies of data should be made frequently and consistently because a power failure could destroy weeks/months of hard work instantly. Deleting files no longer needed on the hard disk will permit more users the opportunity to use the microcomputer. Several large application programs will quickly fill the available space on a hard disk. Original (Copyright) copies and backup diskettes should be stored in a GSA approved security container.

d. Miscellaneous. Any substances that could damage a microcomputer or its peripherals should be eliminated from the environment. Computers and peripheral devices should be covered when not in use to prevent the accumulation of dust. USERS WILL NOT EAT, DRINK, OR SMOKE IN THE VICINITY OF MICROCOMPUTER SYSTEMS. Printers will be cleaned frequently by the user.

5. Security (See KSSOP 380-19)

a. General. Computer work areas will be secured at the end of each duty day or when the facility is unoccupied. Only authorized users should be allowed access to the microcomputer.

b. Computer Access Security. Access will be restricted to personnel having a need to access the stored data. A security access menu will be provided for all microcomputer systems, i.e., GMENU. Users will return the microcomputer to that screen when unattended. The TASO has the responsibility to ensure users follow proper security procedures.

c. Security of Diskettes. Floppy disks will be secured in a locked filing cabinet or locked desk during non-duty hours. All software must be kept under close control to prevent tampering. Appropriate labels (i.e., FOUO/Privacy Act, etc.) will be attached to diskettes when applicable.

d. Diskettes Containing Classified Data. Classified information will be processed only on microcomputers accredited for secure operations or those located in a facility approved for secure operations. Master copies of application software used to process classified information, and the documentation for that software will be secured and safeguarded as prescribed by AR 380-19. Master diskettes will be secured during non-duty hours in a GSA approved security container and will be closely

controlled by the user and TASO during duty hours. An access roster of all personnel authorized to use classified systems will be maintained by the user(s) and monitored daily by the TASO.

6. Accreditation

a. Accreditation is the critical review of a designated system and/or facility prior to initiation of computer operations. The review provides the accreditation authority the information needed to determine the classification level of a particular system. The system(s) will not process information above the approved level as defined in AR 380-19. The accreditation documentation will be prepared as described in AR 380-19. Accreditation requests are forwarded through the appropriate headquarters to AGKS-DOIM for accreditation determination.

b. Reaccreditation will be completed when 1) Increase of security level, 2) Significant change in hardware or software or 3) Three years since last accreditation. The commander, ISSO and the TASO are jointly responsible to ensure the accreditation documents are current and reflect the proper accreditation level. See KSSOP 380-19.

c. Delegation of accreditation signature authority through and including Unclassified-Sensitive (UP) level is extended only to CDR, Kansas Army National Guard. This authority may not be further delegated. Classified Sensitive 3 (CS3) (SECRET/CONFIDENTIAL) accreditation authority will be retained by the Adjutant General. The DOIM will forward the accreditation requests for all other AGKS offices and directorates.

6.1 Non DOD Computers

The use of employee and unit owned microcomputers for official matters is discouraged. See Appendix J.

7. Automation Support

The application of information technologies, current and emerging, are often difficult to define. A studied approach to evaluate specific needs is usually required in order to ensure that requirements are satisfied by the most economical means available. In order to initiate a request for assistance from the DOIM, AGO 2500 (Information Systems Project Document) will be used. The use of this form is required for all requests for services and/or hardware acquisitions to include VI equipment, with the exception of requests for Visual Information (VI) services. For VI service requests, see AR 25-1.

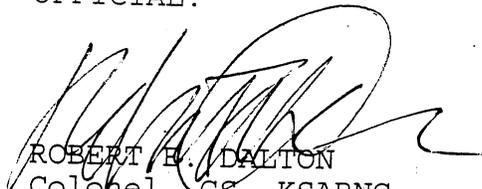
a. The AGO 2500 can be initiated at unit level. Where higher headquarters approval is required for automation projects, the form will be attached to correspondence through the appropriate chain-of-command and forwarded to the attention of the DOIM. New automation capabilities, programming services, and new equipment acquisitions are appropriately initiated on the AGO

1 June 1996

2500. For equipment repairs and maintenance support, DA Form 5504 will be used. (See Appendix H).

FOR THE ADJUTANT GENERAL:

OFFICIAL:



ROBERT E. DALTON
Colonel, GS, KSARNG
Chief of Staff

JAMES F. RUEGER
Major General KSARNG
The Adjutant General

DISTRIBUTION:

A:



Appendix A

CONTROL OF HARDWARE AND SOFTWARE

1. Purpose. To establish standard practices for the control of information systems hardware and software programs.
2. Policy. The following policies are in effect until changed or amended by the Directorate of Information Management (DOIM).
3. Hardware Acquisition and Control.
 - a. The DOIM has the overall responsibility for the evaluation of off-the-shelf information systems, i.e. hardware, peripheral equipment, and software. Requests for evaluation are submitted through channels to AGKS-DOIM. Requirements for evaluation of hardware or software products must be included in the request. If necessary, the USP&FO Purchasing and Contracting (P&C) Officer and the DOIM will communicate directly with the vendor(s) to determine feasibility. Evaluation results are forwarded through channels to the requester. When dealing with the public sector, only the P&C officer can act as an agent of the Kansas Army National Guard concerning hardware or software products.
 - b. Request to purchase information systems hardware are submitted through channels to AGKS-DOIM for approval. The procedures listed below ensure maximum utilization of information resources. The DOIM:
 - (1) Ensures equipment is authorized on the CTA and items are consistent with the Automation Architecture.
 - (2) Signs all requisitions for hardware and software.
 - (3) Obtains fielding plans and controls the assignment of hardware, software, and peripheral equipment.
 - c. Property Book Officers (PBO) will maintain, by serial number, accountability for all hardware and peripheral equipment. If serial numbers are not available, then other means of identifying the item will be created. The PBO's and the DOIM will coordinate the issue of all information systems equipment. PBO's will utilize DD Form 1348-1 to issue equipment, DA Form 2765 to turn-in equipment, and DA 3161 for Lateral Transfers.
 - d. Information systems not utilized are withdrawn and reissued to another office or command. Commanders are encouraged to report non-utilization of information systems equipment through the IMAC representative to the DOIM.
4. Software Acquisition.

a. Computer software requests will be approved by the DOIM before the purchase is authorized. Software valued over \$100 will be hand receipted and controlled by serial number. Only a single backup copy, for safekeeping purposes, is permitted subject to copyright restrictions and/or licensing agreement. If in doubt, coordinate with the DOIM.

b. The P&C Officer will coordinate the purchases of information systems hardware and software with the DOIM. Purchases by the DOIM will be accomplished only after bids are received by and approval obtained from the Purchasing and Contracting Officer. Systems, peripherals, and software that are not compatible or do not fit into the approved Architecture will not be purchased by any office or command.

5. Software Installation and Control.

a. Only government procured/approved software will be installed on any government owned computer. All approved software should be noted on Accreditation updates.

b. Public domain software will be installed only after careful review, testing for viruses, and written approval has been received from AGKS-DOIM.

c. Individual sections/offices will maintain a current inventory of all software installed on government computers under their control by CPU serial number. The TASO is responsible for performing this task as a part of the Accreditation.

d. Government owned software will not be removed from government facilities except in the performance of official duties and only after receiving supervisor approval.

e. All government purchased software will be copied for backup unless prohibited by the purchasing agreement. Original copies of software (i.e. diskettes) will be kept in a locked container or returned to AGKS-DOIM when directed.

f. Original software will be protected from loss, damage or theft by storage in a locked container such as a cabinet, safe, or desk.

6. Software Use.

a. At no time will unapproved or unauthorized software be used on any system. This includes the following software categories:

- (1) Freeware
- (2) Shareware
- (3) Privately procured software except as noted below.

1 June 1996

(4) Pirated software (illegal copies).

b. Use of government purchased software will comply with individual software licensing, copyright, and contract restrictions and requirements. This may limit a single issue to a single system. Except where backup copies are authorized, there must be no more copies of the software in use than were originally purchased. Reference AR 27-60.

c. Privately owned software will not be installed or used on government owned equipment unless extreme situations dictate its use to satisfy immediate and mission essential requirements. Coordinate through channels to the DOIM via telephone and follow up with a hard copy request for authority to utilize privately owned software in emergency cases. Otherwise, employee owned software WILL NOT be used.

7. Software Return Procedures. These procedures will be used when returning obsolete or unused software packages.

a. Software Returns. Software, with accompanying manuals, no longer needed to support mission requirements will be returned to AGKS-DOIM for redistribution or appropriate disposition.

b. Software Destruction. Old versions of software that have been upgraded may be destroyed by the user only when specifically instructed to do so by the DOIM. Normally, this software is returned to the DOIM. Inventory records will be updated to reflect the date of change and/or date of destruction.

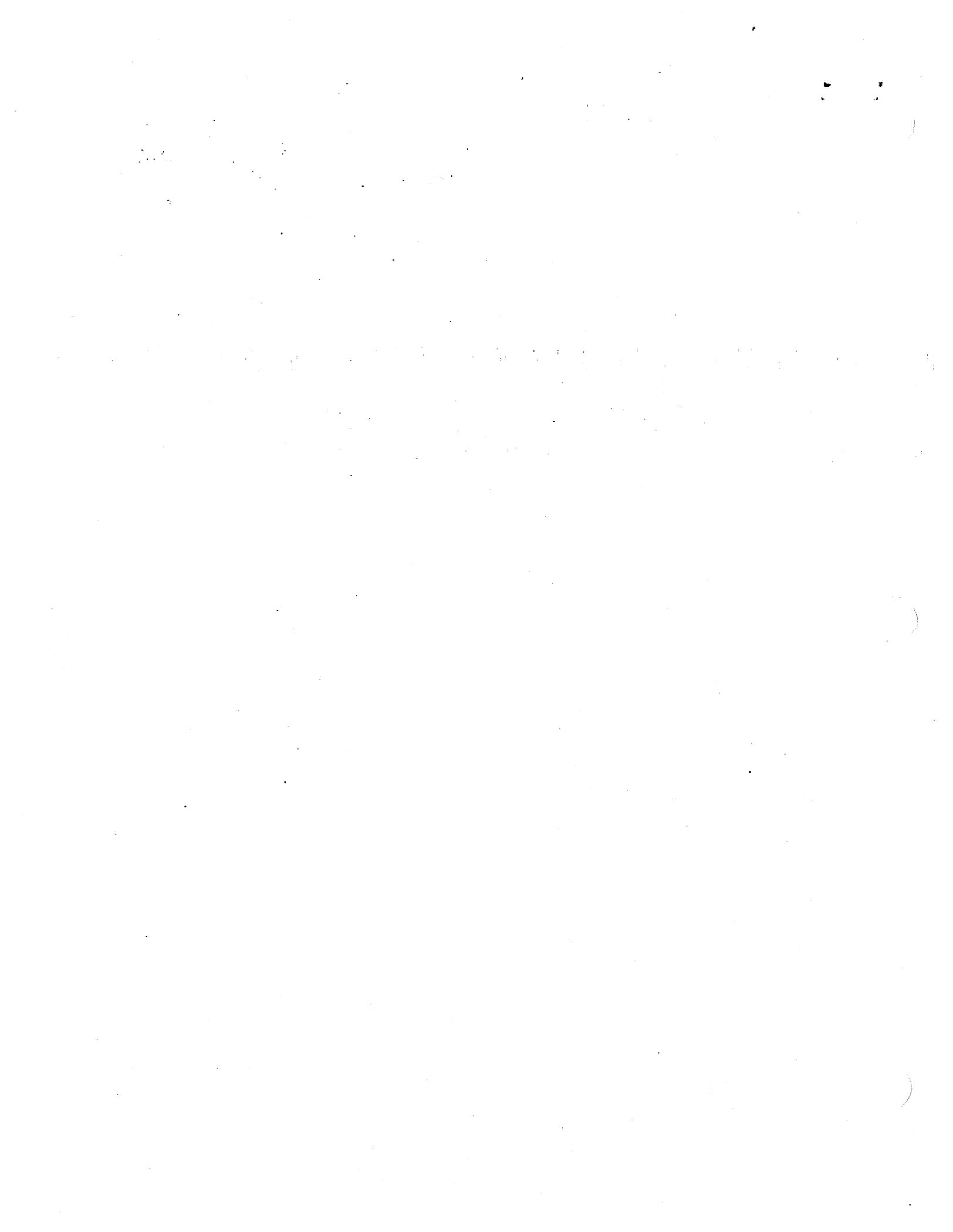
8. Software Inventory Procedures. These procedures will be used to control and account for all computer software. The TASO must maintain a list of authorized software for each machine for accreditation purposes.

a. DA Form 2062 is used to issue software. Hand receipt holders will maintain an inventory of all federally purchased software.

b. The inventory will be updated at the time new software is issued.

c. An inventory will be conducted annually and when a new ISSO is appointed.

d. The user database will be updated to reflect the last inventory date.



1 June 1996

Appendix B

MICROCOMPUTER TEMPORARY LOAN PROGRAM

1. Purpose. To provide an equitable loan program for portable and laptop microcomputers within the Adjutant General's Department.
2. Policy. A written request (AGO 2500) or memorandum must be submitted through channels to obtain a computer on a loan basis. The request is required for record and to establish priority of loan. The Loan computers will only have basic MS Office and a communication program for use.
 - a. Users must be familiar with the system hardware and software before using the system.
 - b. Systems must be used for Official Business Only.
 - c. Systems are loaned out for no more than ten consecutive days and must be returned NLT 1500 hours on the due date. Request for more than ten days must be approved by the DOIM. Systems loaned on Friday for unit visits will be returned the following Monday NLT 1000 hours.
 - d. Priority of loan is as follows:
 - (1) Directors and commanders on TDY for ten days or less.
 - (2) Office chiefs and supervisors on TDY for ten days or less.
 - (3) Individual KSARNG personnel on TDY for ten days or less.
 - (4) Microcomputers loaned to personnel not in TDY status will be recalled for TDY purposes should the need arise.
3. Public Domain. Public domain owned application programs will not be loaded into the portable systems without written approval from the DOIM.
4. Data. User data must be removed from portables loaned out before turning the system into the DOIM. If needed, the DOIM can upload or download data to another system.
5. Responsibility. Individuals are held solely responsible for issued equipment. Persons destroying the operating system or application software are subject to being charged a replacement

cost. A statement of charges may be initiated for missing cables, software or hardware items that were signed for but not returned by the recipient.

Appendix C

DEVELOPMENT OF COMPUTER SOFTWARE

1. Purpose. To provide for the development and management of computer software programs in the Kansas Army National Guard; to enable the DOIM to provide support and assistance to users of locally developed software programs. To prevent duplication of effort and proliferation of non-validated programs. This policy covers programs written in machine language not uses of off the shelf software packages.
2. Policy. Local development of software programs must be approved by the DOIM to prevent "stove piping" of applications that cannot interact with existing KSARNG data bases or with the U.S. Army Corporate Database. Development of software programs will be accomplished in accordance with the following policy:
 - a. Before creating software programs for KSARNG computers supported by the DOIM, organizations will contact the DOIM to determine if programs already exist that meet their requirements. After receiving confirmation a program does not exist, a user may then design and develop a program satisfying mission requirements.
 - b. After completion of program development, and before the program is distributed, the supervisor and/or program developer will submit in writing, through channels, to AGKS-DOIM, the following:
 - (1) One copy on diskette(s) of each of the newly created program(s) to include source code, object code (if available), and other related files as appropriate.
 - (2) A printed copy of all software documentation to include source code and a detailed description of programs execution including operational considerations and plans for future changes (if any).
 - (3) User instructions.
 - (4) Identification of the programmer and programmer's supervisor, to include name, rank, title, unit/organization, business phone number.
 - c. The DOIM will acknowledge receipt of the above information by assigning a Software Authorization Number (SAN). After reviewing and approving the program, the DOIM will grant permission to the originator to distribute the software. The DOIM will include the software in the KSARNG inventory and provide the software to other requesting organizations.

d. KSARNG organizations using software not having an approved SAN will not receive DOIM support for the use of that software. Software problems encountered from the use of non-approved software programs will not be supported by the Directorate of Information Management.

3. Documentation.

a. Microcomputer applications developed by users will be documented. User documentation provides potential users with information necessary to properly use the application. User documentation is also important for use in training other personnel, and it facilitates software sharing and validation.

b. Documentation will be prepared as applications are developed. The documentation will include, at a minimum, the following items:

(1) Application Functions: An application description will be completed and maintained in the functional area, with a copy forwarded to AGKS-DOIM through channels.

(2) System Operations: A user's guide will be prepared for each production program. The user's guide will contain:

(a) Information on how to load, set up, and run the program.

(b) An explanation of valid responses, available options, and input data required for processing and interface with other programs.

(c) Any constraints in the capability or use of the program.

(d) A description of any data files used to include file structure and data element descriptions.

(e) Error messages and required corrective measures.

Appendix D

APPOINTMENT OF ISSO AND TASO

1. Policy. Appointments of ISSO and TASO will be in accordance with KSSOP 380-19, Information Systems Security. All appointed ISSO, TASO, and NSO's will read and become familiar with this regulation and the KSSOP 380-19.
2. Definitions.
 - a. TASO: Terminal Area Security Officer: TASO's serve as information systems security authorities over one or more AIS located in areas under their control. They coordinate AIS use and enforce the STARC ISSP at the user level.
 - b. NSO: Network Security Officer: NSO's serve as information systems security authorities for identified networked AIS under their control.
 - c. ISSO: Information Systems Security Officer: ISSO's serve as the information system 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 ISSO's/TASO's and NSO's, provide security guidance, and review matters concerning facilities, equipment, and data security for AIS in their organizations.
3. General. The appointed ISSO, NSO, or TASO will have the additional responsibility to be the Automation Information Systems Point of Contact for the users they represent. As the AIS POC they will submit requests for AIS requirements, equipment, and training through the ISSO command chain to the IMAC. They are also responsible for feedback on new or existing software, equipment and problems in the AIS arena.
4. Appointment Orders. Units/Activities are responsible to ensure that appointment orders are forwarded to AGKS-DOIM. Appointment orders will include, as a minimum, the following:
 - a. Type of appointment;
 - b. Effective date of appointment;
 - c. Name, rank, SSN and organization;
 - d. Model and serial number of the computer;
 - e. Location of CPU (include armory number or name, building number, room number, activity, city, state and zip code).



Appendix E

INFORMATION MANAGEMENT ADVISORY COUNCIL (IMAC)

1. General: The IMAC is a chartered committee from the Army Council. Its purpose is to manage the information and administrative services for the Kansas Army National Guard. It is expected to develop and maintain current information architecture and an information management plan. They will resource targets and review and approve requirement analysis.
2. Membership: The following are members of the IMAC:
 - Assistant Division Commander 35th ID
 - Commander 130th FA BDE
 - Commander 69th BDE
 - Commander 69th Troop Command
 - Commander 35th Divarty
 - Commander Kansas Regional Training Institute
 - Director Plans Operation Training
 - Director Personnel
 - Director Information Management
 - Director Maintenance
 - US Property & Fiscal Officer
 - Human Resource Officer
 - State Aviation Officer
 - Foreman, CSMS
 - Chief, SPBS
3. Vision: Our vision is an innovative, state of the art, standards based, integrated information management system which accomodates planned technological advances. Though technical in nature, the system must be cost effective, efficeient, user friendly, and supportive of the needs of its users.
4. IMAC representatives act as the liaison between the user and the DOIM. The IMAC reps should field all questions and problems about hardware, software, telephones, applications, excesses, requirements and audio/visual uses. Many problems can be fixed at the lowest level and much faster when using the TASO and IMAC chain. The IMAC representatives also provide feedback to the DOIM for future needs, training requirements, trends of problems, and customer satisfaction. The IMAC committee meets monthly to discuss the automation/communication needs of the Kansas National Guard.

Appendix F

USE OF MICROCOMPUTERS OUTSIDE NORMAL OFFICE ENVIRONMENTS

1. Purpose. To establish policy on the use of microcomputers outside the normal office environment.
2. Policy. The use of 'nonruggedized'/non-developmental item (NDI) computers in a tactical environment can result in serious damage and/or total destruction of the computer. Commanders should evaluate risks inherent to fielding NDI systems in harsh field conditions.
 - a. The TACCS family of microcomputers or other designated NDI systems may be used in a field environment.
 - b. Non-tactical, government-owned microcomputers may be taken to and used in a tactical area only if the computer and its associated subsystem components are located, used and secured in a structure that provides protection from extreme weather elements. The following guidelines apply:
 - (1) High heat -- which is more detrimental to a computer than cold temperatures -- should be avoided. Wet weather environments should be avoided altogether. NDI systems do not have all-weather electrical connections.
 - (2) Computers should be shipped or transported in original shipping containers or in a similar protective transport container.
 - (3) Computers should only be operated from properly grounded and monitored generator power. The use of a surge suppressor, power strip is mandatory between the computer and the power source.
 - (4) The TASO (Terminal Area Security Officer) will ensure that security procedures outlined in KSSOP 380-19 are followed.
 - (5) The Commander and the TASO will ensure that the computer hard disks are backed up before transporting to the field. This will ensure that if system failure occurs the unit will be able to restore operations when the system is repaired.
 - (6) All other precautions for system operations must be followed in accordance with this regulation.
3. Liability For Computer Equipment. The Unit Supply Sergeant and the Unit Commander are responsible for issued computer equipment.
 - a. All computer equipment is issued on a DA Form 1348-1 and receipted by unit personnel as authorized by the commander.

1 June 1996

b. TACCS computers are MTOE equipment and NDI/non-tactical computers are CTA 50-909 equipment.

c. Inventory records are managed by the respective unit's Property Book Officer. HQ STARC staff's property is managed by the HQ STARC PBO.

d. Loss or damage of computer equipment requires immediate action by the Commander.

Appendix G

MAINTENANCE OF INFORMATION SYSTEMS HARDWARE

1. Purpose. To establish policy and standard practices for the maintenance of MicroComputers and their peripherals. See TAB 1 to Appendix G for Maintenance Allocation Chart (MAC) and User PMCS.
2. Policy. The following policies are in effect until changed or amended by the DOIM. The DOIM does not provide maintenance support for the Tactical Army Combat Service Support Computer System (TACCS) or the Electronic Information Display System (EIDS).
3. Maintenance Of Microcomputer Systems Equipment.
 - a. The CSMS is charged with the responsibility to provide maintenance for all information systems assigned to the Kansas Army National Guard. Requests for maintenance will be forwarded through channels to AGKS-CSMS. DA Form 5504 will be used for this procedure.
 - b. When system failure occurs, the user will attempt to determine whether the failure is a hardware or software problem. If user and/or supervisor cannot make this determination, call the closest IMAC rep and ask for assistance. Trained maintenance personnel have been certified and are in each MSC. These personnel will assist in making the proper determination and possibly fixing the computer on site.
 - c. When there is a hardware failure, user(s) or supervisor(s) will not attempt to perform maintenance on the system. Do not attempt to disassemble any components (i.e. the keyboard, cpu, terminal, printer, monitor etc.) of the hardware and then send in pieces or parts for repair. If it is not clear which component is defective, send in all components of the system. Submit a separate DA Form 5504 (Work Order) on each component that is individually serial numbered. Your property book officer provides the customer guidance concerning component accountability.
 - d. Units are responsible to coordinate the delivery to CSMS and pick-up of equipment requiring maintenance. Repair of computers should mirror the procedures customers use to submit anything for repair to the CSMS, with one exception. CSMS will either repair the item within 72 hours or replace it with a loaner comparable component (equal to or better than current component). If any serial numbered component is permanently replaced with a comparable component, there will be property accountability adjustments required.
 - e. There will be occasions when some equipment submitted for repair will be uneconomical to repair and will be salvaged. Disposition and turn in instructions for salvaged items will be

received through the same property book channels that are currently being utilized. It is economical to handle computers in the same manner as we have treated other salvaged equipment and allow the salvaged item(s) to remain at the CSMS pending USPFO receiving the customer turn in documents.

4. Cost Of Maintenance And Budget Considerations.

a. Users of information systems will follow procedures to ensure proper care and protection of assigned equipment. Following established operating procedures normally reduces maintenance costs and loss of utilization of automation equipment. Standard Automation platform is designated by the IMAC for upgrades as well as new acquisition. Budget constraints precludes us from automatically upgrading computers based on speed and convenience. Deviations from this standard must be addressed and approved by the IMAC.

b. The DOIM submits an annual budget to cover information equipment maintenance costs. This budget is based on previous years maintenance costs. Users shall implement proper operational and security procedures to reduce maintenance costs.

TAB 1 to APPENDIX G- Maintenance

MAINTENANCE ALLOCATION CHART
COMPUTERS

1. The below listed levels of maintenance are to be used when determining who is to accomplish services and repairs on computers. There is no TM published that identifies these requirements, so, this chart is intended to provide adequate guidance for all automation equipment users. The listed services are to be entered into the normal maintenance scheduling within the ULLS schedule of services, which will allow for an automated system to prompt the operator when services are due.

2. This column lists the various maintenance functions and indicates the lowest level of maintenance authorized to perform these functions:

- C - Operator
- O - Unit maintenance (personnel trained and certified at the CSMS).
- F - Direct support maintenance
- G - General support maintenance
- - Not Economically Repairable

3. The maintenance functions are defined as follows:

- A - Inspect. To determine serviceability of an item by comparing its physical, mechanical, and electrical characteristics.
- B - Test. To verify serviceability and to detect electrical/mechanical failure by use of test equipment.
- C - Service. To clean and preserve equipment.
- D - Adjust. To rectify to the extent necessary to bring into proper operating range.
- G - Install. To set up for use.
- H - Replace. To replace unserviceable items with serviceable like items.
- I - Repair. Those maintenance operations necessary to restore an item to serviceable condition through correction of material damage or a specific failure.
- J - Overhaul. Normally, the highest degree of maintenance performed by the KSARNG.

4. Service Interval (INT) Codes:

- M = Monthly
- Q = Quarterly
- A = Annually

5. All Class IX requisitioning and returns must be accomplished within current, established CSMS procedures.

6. COMMERCIAL PERSONNEL COMPUTER MAINTENANCE ALLOCATION CHART

GROUP	COMPONENT	MAINTENANCE FUNCTION	MAINTENANCE LEVEL				REMARKS
			C	O	F	INT	
100	COMPUTER ASSEMBLY	INSPECT	X				
		TEST	X			Q	
		SERVICE	X			M	
		REPLACE	X				
		REPAIR			X		
101	CPU	INSPECT	X				
		TEST	X			Q	
		SERVICE	X			M	
		REPLACE	X				
		REPAIR			X		
102	POWER SUPPLY	INSPECT	X				
		TEST	X				
		SERVICE	-	-	-		
		REPLACE			X		
		REPAIR			X		
103	CARDS PLUG-IN INTERNAL	INSPECT		X			FAX/MODEMS, IDE CONTROLLERS, SOUND BOARDS, NETWORK CARDS
		TEST		X		Q	
		SERVICE	-	-	-		
		REPLACE		X			
		REPAIR			X		
104	CHIPS PLUG-IN INTERNAL	INSPECT		X			MEMORY SIMMS ADDITION
		TEST		X			
		SERVICE	-	-	-		
		REPLACE		X			
		REPAIR			X		
105	BATTERY PLUG-IN	INSPECT		X			
		TEST		X		A	
		SERVICE					
		REPLACE	-	X	-		
		REPAIR			X		
106	BATTERY WIRE-IN	INSPECT		X			
		TEST		X		A	
		SERVICE	-	-	-		
		REPLACE			X		
		REPAIR			X		
107	MOUSE	INSPECT	X				
		TEST	X			Q	
		SERVICE	X			M	
		REPLACE	X				
		REPAIR	-	-	-		
200	KEY BOARD	INSPECT	X				
		TEST	X			Q	
		SERVICE	X			M	
		REPLACE	X				
		REPAIR		X			

GROUP	COMPONENT	MAINTENANCE FUNCTION	MAINTENANCE			LEVEL INT	REMARKS
			C	O	F		
300	MONITOR	INSPECT	X				
		TEST	X			Q	
		SERVICE	X			M	
		REPLACE	X				
		REPAIR			X		
400	PRINTER	INSPECT	X				
		TEST	X			Q	
		SERVICE	X			M	
		REPLACE	X				
		REPAIR			X		
500	MODEM, EXT	INSPECT	X				
		TEST	X			Q	
		SERVICE	-	-	-		
		REPLACE	X				
		REPAIR	-	-	-		
600	FAX, EXT	INSPECT	X				
		TEST	X			Q	
		SERVICE	X			M	
		REPLACE	X				
		REPAIR			X		
700	CD ROM	INSPECT	X				
		TEST	X			Q	
		SERVICE	X			M	
		REPLACE	X				
		REPAIR			X		
800	UPGRADES, HARDWARE	INSPECT					COMPLETE SYSTEM UPGRADE
		TEST				X	
		SERVICE				X	
		REPLACE				X	
		REPAIR				X	
900	FLOPPY DRIVES / HARDDRIVES	INSPECT	X				
		TEST	X			Q	
		SERVICE	X			M	
		REPLACE		X			
		REPAIR	-	-	-		
1000	CABLES, EXT INT	INSPECT	X				
		TEST	X			A	
		SERVICE	-	-	-		
		REPLACE	X				
		REPAIR	-	-	-		
1100	SURGE PROTECTORS	INSPECT	X				
		TEST	X			A	
		SERVICE	X			A	
		REPLACE	X			A	
		REPAIR	-	-	-		

7. Listed below are the scheduled services for operator PMCS on various common computer components and peripherals.

A. CPU

- * Clean cabinet with damp cloth.
- * Make sure vents are not blocked.
- * Check all cable connections to be sure they are firmly connected.
- * Clean diskette drives using a diskette cleaning kit weekly.
- * Clean tape drives using a tape cartridge kit weekly.
- * Clean keyboard, turn upside down and shake or tap gently.

B. MONITOR

- * Clean screen with a damp cloth.
- * Use a screen saver program or turn down or off when not in use.
- * Check cable and connections.

C. PRINTER

- * Check cables for tightness.
- * Remove paper debris and dirt from inside printer.
- * Clean outside with a damp cloth.
- * Never roll out labels backwards; tear off and form feed.

D. LASER PRINTER

- * When changing EP-S cartridge:
 - * replace the felt cleaning pad in the fixing assembly.
 - * clean the fixing assembly.
 - * clean the transfer corona.
 - * clean the primary corona.
 - * clean the transfer guides.
- * Clean outside with damp cloth.
- * Check cables and connections.

E. CD ROM DRIVE

- * Clean the lens with a CD drive cleaning kit.
- * Clean the disks with a soft cloth or disk cleaning kit.

F. HARD DISK DRIVE

- * Run a virus check program frequently, check all diskettes from outside sources.
- * Run CHKDSK or SCANDISK msdos 6.x.
- * Run DEFRAG msdos 6.x.

G. MOUSE

- * Clean outside with a damp cloth.
- * Clean trackball with a damp cloth.
- * Check cable and connections.

H. KEYBOARD

- * Turn upside down and shake gently to remove any debris.
- * Clean case and keycaps with damp cloth.
- * Check cable and connections.

I. MODEMS EXT.

- * Clean outside with damp cloth.
- * Check cable and connections.

J. FAX MACHINE.

- * Clean paper feed and document feed rollers.

1 June 1996

- * Clean print head.
- * Clean case with damp cloth.

K. FLOPPY DRIVES 3.5, 5.25.

- * Clean drive with diskette cleaning kit.

L. SURGE PROTECTOR.

- * Check for proper cable connections.
- * Check LED for proper operating status.
- * Check reset button.

8. NSN's for various cleaning kits:

- | | |
|-------------------------------------|------------------|
| * Cleaning kit, tape drive TACCS | 7035-00-348-1864 |
| * 60 Meg tape drive cleaning kit | 7035-01-373-5972 |
| * 40 Meg tape drive cleaning kit | 7035-01-154-1315 |
| * 5.25" diskette drive cleaning kit | 7045-01-154-1315 |
| * 3.5" diskette drive cleaning kit | 7045-01-309-3489 |
| * CD ROM cleaning kit | |
| * Mouse cleaning kit | |
| * FAX Machine Cleaning kit | |

Appendix H

COMPUTER TRAINING FOR INDIVIDUALS

1. Purpose. To establish policy and standards for the training of Kansas Army National Guard military and civilian employees in computer software applications supported by the DOIM.
2. Objective. To establish an ongoing computer training program within a professional learning environment for civilian and military personnel of the Kansas Army National Guard.
3. Policy. The following procedures concerning computer training of personnel are in effect until changed or amended by the DOIM.
 - a. All individuals who operate a computer should complete a software applications training, either through a military or civilian training program. Individuals requiring computer training may be scheduled for a course conducted at either the Professional Education Center (PEC) or the DOIM.
 - b. A primary operator of the computer system will be selected for training. Commanders/Supervisors will ensure that the primary operator will have first priority to attend computer training classes.
 - c. Commanders are responsible to ensure requests for training are submitted in a timely manner so that individuals will not be delayed in obtaining training.
 - d. Individual attendance must be coordinated through command channels to the DOIM. The Directorate is not obligated to permit an individual to attend a class if the individual's attendance has not been coordinated and approved. Computer training is generally contracted to commercial vendors. Vendors are contracted to teach 12-20 students per class, whether or not all students attend. Commanders/supervisors are to ensure those individuals who are scheduled for training attend as scheduled. Failure to attend as scheduled, i.e., 'last minute' withdrawals, represent lost revenue. Therefore, commanders will justify in writing to AGKS-DOIM, 'last minute' withdrawals from scheduled training.
4. Prerequisites. Individuals scheduled for training must meet all prerequisites prior to being scheduled for a specific computer course.
 - a. Pre-test. Students attending 40-hour courses are required to take an assessment test at the beginning of each course.
 - b. Post-test. Students attending 40-hour courses are required to take a test at the completion of each course. A

passing score of 70 percent is required. Students who do not satisfactorily complete a course, will not receive a Certificate of Completion, but will receive a DA Form 1059-1, Civilian Institution Academic Evaluation Report.

c. Students who do not pass a course may retake a different written test for the same subject as many times as required or they may be rescheduled for the same course at a later date.

d. Course Completion Certificates and DA Forms 1059-1, Civilian Institution Academic Evaluation Reports, as required, are furnished to 40-hour courses only.

5. Travel, Per Diem And Tuition. Travel and Per Diem costs are the responsibility of the member's organization. Tuition cost is the responsibility of the DOIM.

6. Computer Training Schedules And Special Instructions.

a. Training Schedules. Computer training schedules are managed and published by the DOIM. Schedules are distributed annually to KSARNG units/activities. Course prerequisites and general information are provided in the annual DOIM computer training schedule.

b. Reporting instructions to include location, dates and times of computer training classes being conducted will be included in the training schedules. Questions about formal computer training will be addressed through command channels to AGKS-DOIM, 2800 Topeka Ave, Topeka, Kansas 66611-1287.

Appendix I

AUTHORIZATION AND USE OF PERSONAL COMPUTERS

1. Purpose. To establish policy and procedures for the utilization of employee and unit owned computers within the military work place.
2. Policy. The following policies are in effect until changed or amended by the DOIM. Employee or unit owned computers, subsystems or software will not be used unless approval is obtained from the DOIM.
3. Employee/Unit Owned Computers. A unit owned computer is one purchased with the Unit (Armory) Fund. When authorization is granted, KSSOP 380-19, Information Systems Security, and the following guidelines will apply:
 - a. Under no circumstances will classified information be processed on these computers. Storage media information (floppy disks, etc.) becomes property of the KSARNG. Storage of information shall be managed IAW current directives.
 - b. Employee/Unit owned computers will remain a "stand alone" system and will not be networked or used to communicate with any federal system.
 - c. Employee/Unit owned systems are subject to removal for noncompliance with AR 380-19 security standards.
 - d. The KSARNG assumes no liability for loss, damage, theft or operational wear of employee/unit owned computer equipment.
 - e. No government supplies may be used (except paper) in support of employee/unit owned computers, nor will government funds be used for the maintenance or repair of privately owned computers.
 - f. Employee/Unit owned approved systems will be removed when government computer equipment capable of performing the same functions has been issued to the unit.
4. Procedures To Request Authorization For Use Of Employee/Unit Owned Computer.
 - a. Submit request through IMO channels to AGKS-DOIM, 2800 Topeka Ave, Topeka, Kansas 66611-1287. Request must be signed by the commander.
 - b. Provide description (manufacturer name, model etc.) and proposed location of equipment (building and room numbers).

c. Indicate intended use of the equipment (correspondence, rosters etc). Notify AGKS-DOIM when an employee or unit owned computer is removed.

d. Request for security accreditation must be submitted as an attachment to the request for authorization if sensitive information of any type, i.e. personnel rosters, are prepared on these systems.

e. Employee/unit owned laptops and all portable microcomputers are required to be accredited for use during IDTs, FTXs, and AT. Accreditation requests will reflect TDY location(s) and inclusive dates the portable will be in TDY status.

5. Accreditation Authority. Accreditation authority for the accreditation of personal computers is retained with the Director of Information Management, ATTN: AGKS-DOIM, 2800 Topeka Ave, Topeka, Kansas 66611-1287. Submit these requests through command channels.

6. Owner Responsibility. It is the responsibility of the commander and/or supervisor to see that the owner adheres to AR 380-19 with respect to security procedures. The owner is also responsible to adhere to the guidelines outlined in this regulation. Failure to comply with published directive(s) may be cause for removal of employee/unit owned computer systems.

Appendix J

FACSIMILE (FAX) OPERATIONS

1. Purpose. To provide policy and procedures for control and processing of facsimile communications via commercial, and/or DSN by both civilian employees and military members of the Kansas Army National Guard.
2. Policy. The FAX system is for OFFICIAL BUSINESS ONLY. The following policy is in effect until changed or amended by the Director of Information Management.
3. Facsimile Operations.
 - a. Facsimile communications is a non-secure method for transmitting fixed images by electronic means. CLASSIFIED information will not be transmitted via a non secure facsimile system. Facsimile equipment that has been tested and proven compatible with the Secure Terminal Unit (STU III) in Secure Data Mode, may be used to transmit classified data. Transmission of FOR OFFICIAL USE ONLY material is permitted over non-secure systems only within CONUS.
 - b. The facsimile systems are intended to be used when normal mail communication is impractical. The FAX system will not be used as a means of conducting routine day-to-day business.
 - c. Documents over twelve pages long will not be transmitted over facsimile systems. Connection period will not exceed fourteen minutes of continuous time nor exceed one hour per day total transmission time per unit.
 - d. Releasers of facsimile communications are the designated officials authorized to release narrative messages. Use will be closely monitored by supervisors. Documents that should have been transmitted via other means will be identified and action taken to establish correct procedures.
 - e. DA Form 4358-1, Facsimile/Telecopier Log, will be used to record all FAX transmissions. (Machine generated reports are acceptable)
 - f. Facsimile transmission logs will be reviewed periodically by the individual authorized to release narrative messages.
 - g. Facsimile Transmittal Header Sheet (DA Form 3918-R) will be used to transmit all outgoing communications. DA Form 3918-R WILL NOT BE MODIFIED TO REFLECT GRAPHIC UNIT HEADINGS. Without a header sheet, the document address (person for whom intended) will be difficult to determine.

1 June 1996

h. Facsimile/Imagery devices will be included on property books, hand receipts and Table of Distribution and Allowances, whichever is applicable.

4. Operational Management Of The Facsimile. Management of facsimile communications is the responsibility of the commander/office manager and/or supervisor, as appropriate. Internal controls will be established to assure proper use of the facsimile system IAW this regulation.

Appendix K

VISUAL INFORMATION PLAN

12.1.1.1 General

SECTION I - INTRODUCTION TO VISUAL INFORMATION

1-1. Purpose. To establish policy and standard procedures for the utilization of visual information devices under the guide lines of Defense Visual Information Account Number (DVIAN) A3574, which has been assigned to the Kansas Army National Guard. This appendix is included in order to inform personnel of the VI program. It is the mission of the Visual Information Section of the DOIM, KSARNG, to support the Kansas Army National Guard through the application of visual information technology products IAW Army and National Guard Bureau's regulations covering visual information functions and responsibilities.

1-2. Responsibility. The DOIM appoints a Visual Information Specialist within the Directorate of Information Management to be the KSARNG's primary point of contact with regard to the state's visual information assets. The scope and duties of the Visual Information Specialist includes the acquisition and inventory of VI products, related application activities, procedures, policy recommendations and planning. The VI Specialist is the advocate for the application of VI technology for the KSARNG.

1-3. Policy. The following visual information policy has been approved by the Adjutant General and will apply to all Audio Visual Support Centers established within the Kansas Army National Guard.

a. The support center will:

(1) Provide staff functions, management and administration of audio visual activities for all organizations within a defined geographic area or installation for nonproduction documentary purposes.

(2) Assist in the establishment, when approved by the NGB and the Adjutant General, of other geographically defined support centers within the Kansas Army National Guard.

b. Visual Information Support Centers established IAW DVIAN A3574 will support nonproduction equipment activities only. This equipment includes graphic art, library and presentation components only.

c. Each approved Visual Information Support Center will be responsible to support a geographically defined area as determined by the Adjutant General, the Chief of Staff or designated representative.

d. Personnel working in these Visual Information Centers will comply with existing directives concerning the control and issue of federal property. Centers will manage temporary and/or permanent issue on a PBO hand receipt (HR).

1-4. Mission. The mission of visual information is to provide commanders, staff, directorates and special staff with visual information products, consulting services, and equipment (AR 25-1, I02) to support the needs of the state's units and personnel in support of mobilization.

1-5. Definition. Visual Information (VI) technology is the use of visual media (with or without sound) to enhance communications and information. This includes electronic still video, motion video tape, manual and computer graphic arts, visual presentation services facilities, and visual information equipment (AR 25-1, I02).

1-6. Products And Services. In accordance with AR 25-1, the full range of visual information products and services include electronic still video, video teleconferencing, presentation services, VI libraries for product and equipment loan and manual and electronic graphics and illustrations. Products and services addressed in this document are based on identified requirements and are limited to activities authorized by regulation.

1-7. Authorized Activities. HQDA and NGB identify the levels of VI activities authorized for each state. Kansas is authorized to conduct activities which include:

a. Produce and deliver presentations combining computers, photos, imagery and audio. These presentations are developed for all command levels on an as needed basis, and the KSARNG staff on an availability basis.

b. Graphic Art Services - Clip art libraries (both computer and hardcopy), manual graphics (drawings and renderings), presentation development, pre-press layout, forms design, etc.

c. Video Taping for non-documentary purposes. This video will capture field training exercises, required briefings, OCS, NCOES, and other types of instruction -- weapons systems, movements, aviation and combat service support activities. It offers Commanders an added evaluation tool in addition to personal and written evaluations.

d. Video-Teleconferencing. Video teleconferencing is a Command Information Tool that facilitates person-to-person communications. Its intrinsic value may preempt the need for personnel travel, per diem, and lost days from duty stations.

e. Multimedia Imaging. This communications technique incorporates a myriad of emerging technologies and offers a

1 June 1996

presentation capability well suited for information dissemination or educational instruction.

f. VI Library Services - equipment loans, video tape management, testing services and VI based training materials.

1-8. Fielding Plan. The initial implementation for visual information products and services will be phased-in to provide sufficient time to obtain resources, train personnel and effectively administer the technology. Detailed milestones and deliverable dates will be developed to supplement this plan. Long term VI needs will be submitted to NGB as Capability Requirements Statements (CAPRS) for inclusion into a five year budget plan.

1-9. Audio Visual Activities. VI activities includes limited acquisition (purchase, lease, and/or rentals) of commercial off-the-shelf production equipment. Management of the VI Support Center will be the responsibility of the Directorate of Information Management.

12.1.2 Functional Requirements

SECTION II - FUNCTIONAL REQUIREMENTS

2-1. Requirements. All units/sections of the KSARNG have similar visual information requirements irrespective of their specific mission and unique needs. Requests for VI services should make use of the appropriate Forms referenced in AR 25-1.

2-2. Visual Information Support Center (VISC). The primary VISC is located in Tennessee. The principal mission of this facility is to support 'high-end' video production, video capturing and advertisement. The Tennessee VISC also is the facility that is responsible for duplication of existing video tapes.

2-3. Kansas Visual Information Support Center (KSVISC). The KSVISC manager (VIM) is responsible for the use and accountability of Visual Information Equipment (VIE). Department of Defense Visual Information Numbers (DVIAN) are required to be sent to NGB-AIS annually. Visual Information Support program (VISP) requirements are developed by the VIM. The KS VIM is the primary point of contact in the Kansas Army National Guard for needs assessment of VIE for Directorate Staff and commanders at all levels. Additionally, the VIM is the primary POC for affiliated agencies for coordination of video teleconferencing, and multimedia concepts and implementation.

a. Product loan, presentation development, and consulting services are specific responsibilities of the center. Additional requirements include the operation, maintenance and technical support of VI Library Services. VI Library Services will provide additional VI equipment as required on a temporary basis to sections/units of the KSARNG.

b. Specific requirements:

(1) Provide portable video capturing service to staff sections, directorates, and units.

(2) Produce high quality color graphics for all staff sections, directorates, and units within the KSARNG. Graphic products will be available on transparencies, hard copy. KSVISC customers have the option to provide color and or black and white line-art/pictures they want incorporated into their VI products.

(3) Assist in making video based multimedia briefings for all staff sections, directorates, and units within the KSARNG.

(4) Provide equipment for sections/units on temporary hand receipt. Equipment may include, but is not limited to, portable VCR/monitor, slide projectors, audio recorders and camcorders, overhead projectors, VGA color and monochrome

1 June 1996

projection panels, Videoshow presentation equipment (digital slides), etc.

(5) Provide equipment for VI Training Center to train sections/units on computer and VI equipment.

(6) Provide management level training for VI equipment in the VI Library and for software/hardware capabilities that supports VI, e.g. Harvard Graphics, Pagemaker, CorelDraw, color projection panels and other presentation hardware.

(7) Develop and maintain graphics art library for external and internal use. Library will include clip art on paper and computer graphics files.

(8) Provide library of VI reference manuals, videotapes, and video based training for external and internal use.

SECTION III - EQUIPMENT REQUIREMENTS

3-1. Requirements.

a. All units/sections of the KSARNG require different Visual Information equipment depending on their specific mission and unique requirements. Each unit/section will be authorized to be hand receipted specific equipment depending on their mission and requirements. Additionally, there will be a complete Information Management Equipment List staffed through all of the directorates for visual information equipment loan and permanent assignment.

b. Any permanent visual information equipment requirements will be forwarded to the DOIM, VI Branch, through the local information management officer (IMO). Upon review, the requirement will be processed by the Visual Information Branch. Unless authorized by Information Mission Area, Table 75, CTA 50-909, any VI equipment requirement must be submitted to and approved by NGB on an Equipment Changes in MTOE/TDA (DA Form 4610R). Once approved by NGB, equipment requisitions may then be processed by the state.

3-2. Kansas Visual Information Support Center (KSVISC). The KSVISC will facilitate VIE loans to directorates, units, and military associations directly associated with the Kansas National Guard.

a. Work orders for VI support will be taken daily. Priorities will be assigned to the job when received with a completion date given.

b. Each project will be reviewed by the Graphic Designer or the VI Specialist. Appropriate suggestions will be provided to customers of VI facilities.

SECTION IV - LONG TERM REQUIREMENTS

4-1. General. Requirements identified in this section are long term needs which will be submitted to NGB as Capability Requirements Statements (CAPRS) for proposed inclusion in the five year budgetary process (POM).

4-2. Requirements.

a. Video Teleconferencing. Provide video teleconferencing capability to state supplementing on-site conference capabilities. This includes the ability to send and receive video and audio information using satellite dish technology. It allows the Adjutant General and commanders worldwide access to visual command and control processes.

b. Visual Information Type B Production. Currently Kansas is authorized to conduct Type A Visual Information activities (reference section 1). Upgrading to Type B capability will expand VI authorization to allow production, reproduction and distribution of VI products such as edited video tapes.

c. Multimedia. Multimedia equipment will provide the capability to incorporate sound, computer graphics, still and full motion video and text for the production of training films and command presentations. Films and presentations will be completed more efficiently and effectively.

d. Electronic Multimedia Imagery Concept (EMIC). Electronic imagery capability replaces the current chemical processing for photographs with an electronic process. Electronic photography may be used by the Public Affairs Detachment and STARC for military photos, news coverage, etc. Photos can be easily integrated with multimedia or traditional printers.

e. Master Antenna. A master antenna system permits broadcasting audio visual signals from a single source such as a training site to multiple locations such as armories or other classrooms. The major benefit of this capability is that classes or presentations may be conducted at one location and received by students at geographically separate locations.

f. Closed Circuit Television. A closed circuit television system provides the capability to broadcast live classes, presentations, training videos and information releases to multiple buildings, classrooms and other geographically separate locations.

SECTION V - EQUIPMENT TERMS

Amplifier -- This equipment will be used in conjunction with microphones and speakers to amplify sound. Can also take input from cassette recorder/player. LIN 86183G

Audio Tape Recorder/Player -- Equipment may be of either the hand-held size or desk size depending on where it will be used. Recorder/players in the VISC library will be the portable, hand held size. All of these recorder/players will take the standard size cassette tape. LIN 86181G

Camcorder -- This 1/2" video camcorder will be used to document training and briefings. Equipment will use a standard S-VHS tape to record on. LIN 86176G

Color Postscript Printer This color thermal transfer printer will print directly on overhead film or thermal paper for quality products. Will accept output from Harvard Graphics, Corel Draw, Windows and other graphic packages. LIN 85240G

Color Scanner -- Scanner will provide the ability to incorporate existing clip art, color photographs and other graphics into VI products. Scanner will also be equipped with OCR software to allow scanning of text for incorporation into VI products. LIN 85265G

Degausser Equipment -- This demagnetizes (erases) audio and video tapes. Erasing the tapes allows them to be reused which will save on expenses of magnetic recording tapes. LIN 85270G

EIDS Computer System -- This interactive computer system will provide an interactive training system for the VISC Training Center. LIN E61338

Graphics Personal Computer -- This computer, which will be part of the VISC, will be dedicated to producing graphics for use in briefings and training. Will be 486 technology with graphics accelerator, SVGA monitor and 16MB RAM for speedy processing and design time.

Graphics Software -- The following software will be used on the Graphics Personal Computer to design and produce graphics for use in briefings and training:

a. Harvard Graphics 3.0 for Windows Software will aid in the design of viewgraphs. Windows version allows integration with other Windows software for a wider variety in available graphics.

1 June 1996

b. Corel Draw 5.0 Software is used to edit and create quality, vector based graphics. Since it is Windows based, it can export graphics for use in Harvard Graphics.

c. OmniPage Pro - Software is used as an OCR in cooperation with a flatbed scanner for scanning text and converting to ASCII. This is a Windows based program and can export to other Windows applications.

d. Aldus PageMaker 5.0 - Software will be used when it is necessary to mix both text and graphics in a VISC product. This is an ideal package for producing newsletters and similar publications. Since it is Windows based, software can take input from Harvard Graphics and Corel Draw.

e. Various Clip Art packages - These software packages are a collection of graphics for use in briefings and other VISC products. This clip art covers a wide range of subjects including military, industry, and business symbols.

Harvard Graphics 3.0 with Mouse -- This MS-DOS based software will be used to design viewgraphs for use in briefings and training. This software will be supported by existing MS-DOS computer systems. The mouse will be a two button serial type.

ID Camera System -- "Instant" photo camera system will consist of camera, photo cutter and laminator. LIN 86215G

Laser Pointer -- Laser pointers will allow briefer to indicate information on the screen as it is being projected. Laser pointers are more efficient than standard pointers because they allow mobility around the briefing area while still being able to indicate information on the screen. LIN 85269G

Lettering Machine -- This typewriter-like machine is used to produce text on an adhesive strip (Kroy type) for use in viewgraphs, graphic presentations and brochures. LIN 86185G

Lighting System -- This lighting system kit will consist of different size quartz lights for use with both camcorders and 35mm cameras. It will include lights, barn doors for light control, stands and carrying case. LIN 86207G

Microphone System -- This system will consist of one clip-on and one hand held wireless microphone. It will be used at the Kansas Military Academy, Adjutant General's briefing room, and the STARC armory auditorium. It will be used in conjunction with the amplifier and speakers. LIN 86198G

Monochrome Laser Printer -- This laser printer will be used to print black and white viewgraphs to use in briefings and training. Equipment will utilize postscript technology for best

possible printing results. Equipment will be used with existing MS-DOS computer systems producing output from Harvard Graphics 3.0. LIN 85240G

Overhead Projector -- Equipment is utilized to display overhead material for briefings/training. The overhead projectors in the VISC Library will be the portable type. LIN 86175G

Photo Mounting Equipment -- Equipment will be used to laminate or drymount photos and graphics on boards for briefings, seminars and training. LIN 86208G

Projection Screen -- These projection screens will be either wall mounted or portable, tripod type depending on the application. The screens that will be in the VISC Library will be the portable type. LIN 86216G

Slide Printer -- This hardware is hooked to a personal computer and will produce 35mm slides from Harvard Graphics, Corel Draw, Windows and other graphic packages. It will produce standard 2" x 2" slides for use in briefings and training.

Slide Projector -- Equipment is used to integrate slides into a training briefing or presentation. Slide projectors in the VISC Library will have a built-in 9" viewer for portability. All other projectors will be the standard carousel type. LIN 86174G

Slide/Sound Processor/Mixer -- This equipment is used in conjunction with two projectors to get a smooth, automatic fading from one slide to the next. The controller has built-in times and variable dissolve rate. LIN 86197G

Speaker System -- This equipment is a set of standard audio speakers that will be mounted on the walls of the Auditoriums, Museum and conference rooms. It will be used in conjunction with microphone and amplifier to amplify and improve sound quality. LIN 86184G

Still Camera Set -- This 35mm camera set includes all of the components necessary for quality pictures. Camera body, standard lens, lenses and a flash are included in this set. LIN 86178G

Still Video Camera -- Camera will be used to digitally document training, ceremonies, awards promotions or other events. Used in conjunction with still video viewer, equipment will eventually replace 35mm cameras. Photos taken can be utilized in briefings/training material produced by the VISC. LIN 85262G

Still Video Viewer -- Used to display, edit, and incorporate still videos into graphic products to be used for briefings training. Allows saving of digital images on diskette. LIN 85262G

1 June 1996

Television/Monitor -- This equipment will be used in conjunction with the VCR to show video based training. The screen can be any size depending on the location of the equipment. Most TV/monitor screen sizes will be either a 19" or 27" screen. LIN 86180G
Tripod System -- This transportable tripod will have a fluid pan and tilt head and quick release for easy operation. It will be used for both camcorders and 35mm cameras. LIN 86199G

VCR with Built-in Monitor -- This equipment consists of a VCR with a monitor that is built in for portability. Monitor can be any size depending on the application. Most of the equipment that will be fielded will have 19" monitors for group viewing. LIN 86209G

Video Cassette Recorder (VCR) -- These VCRs will accept standard 1/2" VHS tapes for training and briefings. Machines will have 4-heads for a quality picture and a remote control for better control during briefings. LIN 86182G

Video Laser Disc Player -- Equipment will provide ability to use training material that is available on standard 5" laserdiscs. A lot of commercial training (especially computer training) is fielded on 5" video discs. LIN 86226G

Video Graphics Processor -- This device will process 3D graphics, video and animations. It will be used to generate special effects for training videos. It will function as a video switcher, 3D animation generator and recorder, character generator and effects generator.

Video Graphics Processor Software -- The following software will be used on the Video Graphics Processor to design and produce graphics, animations and special effects for use in briefing and training videos:

a. Deluxe Paint IV AGA - Software for producing animations and graphic scenes and clip art for use in video presentations.

b. Art Department Pro - Software for converting the multitude of graphic formats to IFF format for importing to the Video Graphics Processor.

c. Lightwave 3D - Software for producing 3 dimensional animations and recording them for use on video as graphic sequences and special effects.

d. Image FX - Software for digital image retouching and processing. This software performs analysis for scanning, rendering and conversion to create 24 bit images.

e. Pixel Pro - Software for designing and rendering three dimensional objects for use in Lightwave 3D and video output.

f. Video Toaster 4000 - Software performs as switcher for video production. It has the capability of integrating 4 inputs, generating chroma key effects, digital wipes, frame buffering and digital video frame capture.

Video Projector -- Projector displays an image, up to 100" wide, onto a large screen. It can receive input from a VCR, Personal Computer, and video disc players. This is a necessary item when conducting video-based or PC-based training or briefings in large rooms. LIN 86172G

Appendix L

SECURITY REACCREDITATION REQUIREMENTS

1. Purpose. To establish security reaccreditation requirements for microcomputers assigned to all Kansas Army National Guard units.
2. Policy. The following procedures concerning the reaccreditation of microcomputers in the Kansas Army National Guard are in effect until amended by the Department of Army or the National Guard Bureau:
 - a. Reference paragraph 3-6, AR 380-19.
 - b. All automated information systems (AIS) will be formally reaccredited within 30 days after any of the following occurs:
 - (1) Addition or replacement of a microcomputer.
 - (2) A change in sensitive designation.
 - (3) A change in security mode of operation.
 - (4) A breach of security, violation of system integrity, or unusual situation that appears to invalidate the accreditation.
 - (5) A change in location that effects the physical security described in the existing accreditation.
 - (6) Three years has elapsed since the effective date of the existing accreditation.
3. Responsibility. It is the joint responsibility of the Commander, the Information Systems Security Officer (ISSO) and the Terminal Area Security Officer (TASO) to review periodically the existing accreditation documents to ensure they meet the above requirements. This responsibility includes maintaining a copy of the accreditation document files by the TASO.

Appendix M

NGNET AND AGKS BULLETIN BOARD SYSTEM
ACCOUNT AND USAGE PROCEDURES

1. Purpose. To establish policy and procedures on the usage of the National Guard Network (NGNET) and the AGKS Bulletin Board System (BBS).

2. Policy.

a. NGNET is the official electronic mail system for the Kansas Army National Guard. Each organization will have a NGNET account. Commanders will ensure their unit has an NGNET account. NGNET is checked daily. The organization will coordinate NGNET accounts through the USPFO Data Processing Installation (DPI).

b. The BBS is a unofficial communications system accessible by members of the National Guard.

3. NGNET Electronic Mail System. NGNET is the Army National Guard DOD standard electronic mail (E-mail) system used by the National Guard Bureau and every National Guard unit across the nation.

a. Provides an inexpensive medium for the exchange of text files (word processing files converted to ASCII format) and binary files (programs and data files in their unconverted state).

b. Provides a means of electronically receiving and sending official mail. Messages are official in nature and acted upon as any other correspondence. In accordance with DOD Directive 5200.28 "DDN communications are for use by government agencies, their employees, and authorized contractor personnel for the conduct of official DOD business only".

c. Provides electronic transmission of requesting and receiving individual orders.

d. Reduces the amount of time, supplies, and cost of hardcopy correspondence production and distribution.

4. AGKS Bulletin Board System.

a. Provides an inexpensive medium for the exchange of text files (word processing files converted to ASCII format) and binary files (programs and data files in their unconverted state).

b. Provides an unofficial means of electronically receiving and sending mail and binary files.

1 June 1996

- c. BBS users maintain their own BBS passwords.
 - d. TASO orders are not required to access the AGKS BBS.
5. Document Size. Limit NGNET messages to 25 pages or less of text, or 50,000 bytes (50K) or less of data. Contact the USPFO DPI for messages exceeding these size limitations.
 6. Equipment. The equipment specifications to access NGNET and the BBS are a computer, modem and communications software. The DOIM will provide formal training for the BBS. Training on the NGNET will be coordinated with USPFO DPI. Individuals should send requests to Directorate of Information Management, ATTN: AGKS-DOIM, 2800 Topeka Ave, Topeka, Kansas 66611-1287. DSN: 720-8034 or COMMERCIAL: (913)274-1034.
 7. NGNET Accounts. Passwords and IDs are required for each account set up by the USPFO DPI. The USPFO will not set up new accounts or issue passwords without TASO orders.
 8. Terminal Area Security Officer (TASO) orders. To request a NGNET account, prepare TASO orders and forward them to the USPFO Data Processing Installation (DPI). The organizations will appoint a primary and alternate TASO. TASO orders will include the individual's full name, rank, unit, SSN, effective date, assignment, duties to perform, and a list of hardware and software used to access NGNET. Organizations will ensure that the USPFO DPI has current TASO information.
 9. Passwords for NGNET. Individuals must sign for passwords. Only issue passwords to two or three individuals. Individuals keep passwords secure at all times. If you feel a password has been compromised, contact the DPI immediately at (913)274-1251 or DSN 720-8251.

Appendix N

STATE TEMPEST CONTROL OFFICER

1. Purpose. To establish policy for appointment of the State Tempest Control Officer (STCO) at AGKS level and Tempest Control Officers (TCO) for the subordinate major commands in the Kansas Army National Guard.

2. Policy. The following procedures concerning the Army National Guard Command Communications Security Tempest Program are in effect until changed or amended by AR 380-19-1, with changes, Chief, National Guard Bureau or the Adjutant General.

a. The Adjutant General has the authority and will implement the KSARNG Tempest Program by appointing a state Tempest Control Officer. The state Tempest Control Officer will be appointed on orders.

b. The Director of Information Management (DOIM) has command tempest responsibilities as part of the overall state Information Systems Security Program. The DOIM will insure knowledgeable person(s) are appointed as Tempest Control Officers for each major subordinate command/activity as required.

c. The DOIM will act as the focal point for the Kansas Army National Guard Tempest Program and will:

(1) Report directly to the Adjutant General on matters pertaining to the state Tempest Control Program.

(2) Insure a Tempest Control Officer is appointed for each major command or as required.

(3) Coordinate state tempest program requirements.

(4) Prepare Tempest guidance and provide advice and assistance to subordinate command Tempest Control Officers.

(5) Prepare command directives on implementation of KSARNG Tempest control policies and procedures.

(6) Review KSARNG Facility Tempest Risk Assessment/Risk Analysis (FTA/RA) requirements for the staff and field operating activities.

(7) Maintain information files for the KSARNG Tempest Program.

(8) Provide NGB-AIS-TS with copies of orders appointing Tempest Control Officers within the State.

d. Commanders of the MSC's will appoint a knowledgeable person as the Tempest Control Officer who will:

- (1) Be familiar with AR 380-19-1 with changes.
- (2) Provide copy of the appointment orders to the state Tempest Control Officers.
- (3) Cause a Facility Tempest Assessment/Risk Analysis (FTA/RA) to be completed for each facility or system that will electronically process classified information IAW AR 380-19-1.
- (4) Determine if appropriate Tempest counter measures are required prior to establishing, altering, relocating or expanding the facility or system because of the FTA/RA.
- (5) If a formal FTA/RA is required IAW AR 380-19-1, forward the completed FTA/RA through the STCO to NGB-AIS-TI.
- (6) All expenditures of resources for Tempest counter measures, including facility evaluations, inspections, and testing, shall be based on the results of review of the FTA/RA by the STCO and NGB-AIS-TS.
- (7) If appropriate, cause the processing of classified information to be discontinued until required tempest control measures are applied.
- (8) Conduct periodic surveys of the level and volume of classified information being processed. If changes warrant, prepare a new FTA/RA.
- (9) Request a waiver when tempest control measures cannot be met.

3. Liability. Commanders and Tempest Control Officers at all levels of command have responsibility for the proper management of the Commander Information Systems Security Program.

Appendix O

DISPOSITION OF EXCESS/DAMAGED AUTOMATION EQUIPMENT

1. Purpose. To provide procedures for the disposition of excess and/or damaged automation equipment. To also establish a procedure for the inventory and utilization of excess internal automatic data processing equipment (ADPE) components.
2. Policy. The following policies are in effect until changed or amended by the DOIM.
3. Turn-in Procedures.
 - a. The Information Management Advisory Council (IMAC) and the DOIM have a coordinated policy regarding the management, issue and reissue of automation equipment. This policy, in part, states the initial issue and subsequent reissue of automation equipment is managed by the DOIM. The policy recognizes the official inventory of ADPE is reviewed by the DOIM but managed by the respective PBOs of the major commands.
 - b. Turn-in of excess automation components shall be coordinated through the IMAC Rep to the DOIM, ATTN: AGKS-DOIM; 2800 Topeka Ave, Topeka, Kansas 66611-1287. Equipment turned in under this criteria will be subject to evaluation, test and repair as appropriate. Equipment may be returned to service by the DOIM. Systems and component evaluation is conducted by the Electronic Digital Computer Mechanic in the CSMS.
 - c. When the user organization determines they have damaged automation equipment assigned to their unit, the individual who is responsible for the operation and security of the equipment will coordinate the submission to the CSMS for repair.
 - e. After evaluation of excess assets has been accomplished by the DOIM, it becomes the responsibility of the hand receipt holder to transfer, by DA Form 2062, these assets to the Property Book Officer.
4. Management of Excess/Damaged Automation Equipment. Management of computer assets in the KSARNG is a responsibility delegated to the DOIM by AR 25-1, The Army Information Resources Management Program, by NGB-IMA and by the Adjutant General. Therefore, the DOIM will accomplish evaluation of excess automation inventories for possible re-utilization.
5. Damage to equipment will be evaluated IAW KSSOP 750-1 prior to classification or repair by CSMS.

Appendix P

COMMUNICATIONS BRANCH

1. Purpose. To establish policy and identify responsibilities and standard procedures for telecommunications services for the Kansas Army National Guard.
2. Applicability. These policies apply to all telecommunications services in support of the Kansas Army National Guard.
3. Policy.
 - a. Telephone equipment and services will be provided to satisfy mission-essential Federal/State requirements.
 - b. Operations and Maintenance funds are established for communications services for the transmission of Government information only. The use of telephone service will be limited to the conduct of official government business necessary to carry out assigned mission.
 - c. Usually, the most economical telephone instrument will be installed. The maximum allocation is one voice line for each three full time employees; or, one per unit level organization. Extensions may be authorized.
 - d. DSN will be the primary means of communications where available. FTS-2000 will be used for all non-DSN official telephone communications. Commercial long distance will only be used when the above services are not available.
 - e. No personal toll-calls will be made using federal/state telephones. If a personal call must be made, the individual must contact the local telephone company's operator and place the call collect or have it billed to his/her home phone or personal calling card.
 - f. Calling capability in individual station features will be limited to those required to perform official business.
 - g. Calling cards will be used for the following purposes only:
 - (1) When authorized calling card holders are away from their permanent duty station, the telephone number to be called is not available via FTS-2000, and there is a valid requirement to place an official call.
 - (2) For emergency recall of troops.

h. Monitoring of telephone conversations to determine whether the communications is for official purposes is prohibited. Incidental monitoring by telephone operators and maintenance personnel relating to communications management will be limited to mechanical and service quality control checks. Conversations for communications management control purposes will not be recorded.

i. Facsimile equipment is for the transmission of unclassified information when appropriate. Classified information will not be transmitted over unsecured facsimile equipment. A STU-III and secure facsimile machine will be used to send classified facsimile traffic.

j. Cellular phone service will be used primarily under circumstances where leaders responsiveness is critical to the health and welfare of soldiers and civilians and organic communications equipment cannot support essential requirements.

k. Pager service will be used for personnel that require immediate notification of critical events during duty hours.

4. Responsibilities.

a. The Communications Branch is responsible for:

(1) Planning and programming for new requirements, modernization, expansion, rehabilitation, and reconfiguration of telephone systems and circuits.

(2) Preparing and submitting requests for leased communications requirements and facilities.

(3) Validating requirements for leased dedicated communications services as being mission essential.

(4) Insuring that only authorized users are provided access to DSN.

(5) Reviewing on a continuing basis all telephone subscribers to determine if an appropriate class of service is provided.

(6) Developing programs that require users of telecommunications facilities to take personal interest in practicing communications economy and discipline.

(7) Reviewing all requests for procurement or lease of base telecommunications equipment and services.

(8) Validating requests for payment through commercial accounts.

b. Supervisors are responsible for:

(1) Verification of telephone usage as official/unofficial.

(2) Ensuring the telephone system is not being abused to include the voicemail system.

(3) Submitting requests for user usage.

(4) Providing information upon request to the Communications Branch for the justification and revalidation of communications services.

c. Individuals/users are responsible for:

(1) Ensuring the most economic and efficient use of communications facilities. These include:

(2) Organizing and planning conversations prior to initiating calls.

(3) Limiting calls to those that are official and authorized.

(4) Completing conversations as quickly as possible, usually within 5 minutes and no more than 10 minutes.

5. Procedures.

a. Telecommunications Services.

(1) Request for all telecommunications services must be submitted to the Communications Branch (AGKS-DOIM) on a AGKS FORM 2500 (see attached Form) at least 10 days in advance of anticipated activation to allow for proper processing, validation, and vendor contractual time limits. Ensure complete justification is included on all requests.

(2) Request for additional or new equipment must be submitted to the communications branch and fully justified via memorandum at least 10 days in advance.

(3) Report all telephone trouble calls (i.e. dead phone, phone not working correctly) to the Communications Branch at DSN 720-8033 or Comm (913) 274-1033. Under normal circumstances, the trouble should be corrected within 24 to 48 hours.

(4) Adds, moves, and changes to local phone service should be submitted on attached AGKS 2501-R to AGKS-DOIM at least 10 days prior to required date.

b. Telephone billings.

(1) Each month, all major commands will be provided a copy of their individual and subordinate units telephone bills to use as a management tool in reducing telephone toll costs. These statements will be used for the collection of fees for personal calls.

(2) All telephone bills will be validated and processed for payment by the Communications Branch.

c. Telephone Directory. The Kansas National Guard Communication Directory will be published once a year. All offices are encouraged to submit their updates of changes, additions, and deletions to the Communication Branch (AGKS-DOIM) quarterly.

d. Cellular Services. Request for cellular services will be forwarded to the Communications Branch (AGKS-DOIM) using a standard memorandum including full justification and approving signature of Director/Commander. Cellular phones are limited to organizations when there is no other communications available. Users may be required to provide funding.

e. Facsimile Services. Request for facsimile equipment must be forwarded to the Communications Branch (AGKS-DOIM) using AGKS FORM 2500. Requests for repairs can be made by calling DSN 720-8033 or COM (913) 274-1033. Under normal circumstances (if a vendor is available) local repairs can be completed within 24 hours.

f. Pagers. Request for pagers must be forwarded to the Communications Branch (AGKS-DOIM) using a standard memorandum which should include full justification and director/commander's signature. Pagers are limited to personnel whose mobility makes them difficult to contact during duty hours. Emergency numbers should be utilized during non-duty hours.

g. Frequent Number Database. All Kansas National Guard unit telephone numbers, commander's home numbers, commander's work numbers or any federal/state activity that is called on a frequent basis by units should be included in the Frequent Number database on F: drive. Telephone number can be added to the database by simply submitting a memo to AGKS-COS include name of Activity/Commander, telephone number, address of activity or commander. This database is limited to activities/commanders only, and does not include other personnel.

h. Voice Mail.

(1) Voice mail systems are for official government business. Personal messages may be left in the voice mail system as long as it does not interfere with official government business.

1 June 1996

(2) Requests for the availability of voice mail must be submitted in writing by supervisory authority on AGKS Form 2500.

(3) The Voice mail system will not be used to screen calls. All calls should be promptly returned.

(4) Update personal, internal and external greetings to reflect long periods of absences, when applicable.



Appendix Q

ADMINISTRATIVE SERVICES BRANCH

1. Purpose. To define the roles and responsibilities of the Administrative Services Branch of the Directorate of Information Management (DOIM), KSARNG.

2. Policy. The following policies are in effect until changed or amended by the Directorate of Information Management.

3. Responsibilities. The Administrative Services Branch provides direction and support in the areas of reproduction, mail, publications and forms, copier management, records management and administration of the federal Freedom of Information/Privacy Acts. It consists of six functional offices under the control and supervision of the Chief of Administrative Services:

a. Records Management Section. The Records Management Section manages the Modern Army Recordkeeping System which involves the systematic identification, maintenance, and the retirement and destruction of Army information. This section administers the federal Freedom of Information and Privacy Acts for the detachment headquarters and the Kansas Army National Guard. Specific responsibilities include:

(1) The dissemination of and records management policy pertaining to the Modern Army Record Keeping System (MARKS).

(2) Reviewing the appointments of Records Management Coordinators at division, brigade, battalion, unit, office and activity level. It also provides for and conducts statewide staff visits in MARKS in accordance with the provisions of Army Regulation 25-400-2, every two years. MSC's will submit a copy of appointment orders to AGKS-ASB

(3) The approval of file numbers from each unit, establishing and maintaining records holding area and the preservation of historical records.

(4) The maintenance of FOIA/PA control logs IAW DOD 5400.7-R. Logs case activity. It records information in logs based on annual reports from DD Form 2564. It forwards all requests to be denied or cases that are questionable to NGB-AD.

(5) Requests for FOIA/PA information from office of record and prepares final release letter. It prepares FOIA/PA annual reports.

(6) Guidance and direction to units and activities relative to correspondence management IAW AR 25-50.

b. Publications/Forms Management Section. Stocks forms and issues publications and forms to account holders. Specific responsibilities include:

- (1) Maintenance of the official record set of state/territory forms.
- (2) Inventories publications and reorders as necessary and distributes publications.
- (3) Managing the 12-series, pinpoint distribution.

c. Printing and Duplicating. Provides reproduction services for the department headquarters and major Kansas National Guard field commands and facilities. Responsibilities also include:

- (1) Managing the state printing/duplicating budget.
- (2) Performing cost analysis to determine most economical method of printing/duplicating.
- (3) Assists in the preparation of printing procurement requests.
- (4) Submission of the annual commercial printing report.

d. Information Distribution Center. Manages and conducts state and federal mail control programs involving the distribution of postage meters and postage stamps to all units. Additional responsibilities include:

- (1) Developing and submitting state budget for mail management, managing postage funding and establishing state mail management policies.
- (2) Procuring, accounting for, securing, and issuing postage stamps.
- (3) Serving as the approval authority for postage meter requests.
- (4) Consolidating, preparing and submitting quarterly postage meter reports.
- (5) Managing/Operating the state mail center, and maintaining security of mail center and postage equipment.

e. Copier Management. The copier manager's duties include:

- (1) Ensuring that units/activities are equipped with adequate copier support.
- (2) Inventorying records of copiers.

1 June 1996

(3) Reviews and monitors monthly, quarterly and annual copier readings and reports.

(4) May assist in coordination of copier repairs for all units/activities.

(5) Managing the copier budget under direct supervision of the Administrative Services Chief.

(6) Evaluating copier machine usage IAW AR 25-30.

(7) Preparing a consolidated year end report to NGB.

f. Department Publications and Forms Management. The department publications and forms manager's duties include:

(1) Reproduce the Adjutant General's Annual Report to the Governor.

(2) Control of logs and the assignment of publication numbers; reviewing and approving department publications and forms for format accuracy; and, assisting with corrections when needed.

(3) Reviewing and approving requests for reproduction.

4. The office symbol for the Administrative Services Branch of the DOIM is AGKS-ASB, DSN 720-8041 or 913-274-1041.



Appendix R

BLANK FORMS

1. AGKS Form 2500-R: Information Systems Requirement Document

a. Purpose: The AGKS 2500-R is used to request hardware or software for Automation and to request equipment or service for communications.

b. Procedure: AGKS 2500-R's are filled out by the user and submitted through the TASO-ISSO chain to the IMAC representative. The form can be reproduced electronically and submitted electronically.

c. Instructions for completion: (Part 1 by Requestor)

Block 1- Subject/Project: Major reason for the request. For instance: Software requirement, Hardware upgrade, Hardware requirement, New phone line etc.

Block 2- Requesting Unit: Requestor, Name, Phone number, Unit, address.

Block 3- Date Submitted: Date the form was filled out

Block 4- Priority: Check whether it is Routine (putting the requirement in for when we have money or time) or Urgent (causing mission failure)

Block 5- Automation: Check whether it is a hardware request or software request. Leave blank if it is a communication requirement.

Block 6- Communication: Check whether it is an equipment requirement or service requirement. Leave blank if it is an Automation requirement.

Block 7- Process Classified: Check either Yes or No if the requirement is concerning Classified material: Confidential or higher (either Voice or Automation).

Block 8- Sensitive Unclassified: Check either Yes or No if the requirement concerns FOIA information or Intelligence crypto data.

Block 9- Requirement/Description: The critical part of the form. The user is to identify WHAT the requirement is NOT what equipment they would like. For instance: "The NGB sends all information for this application on a CD with video segments. The software requires 40mg of memory and at least 8mg of RAM to operate". The user should NOT write in this block "I want a 486 COMPAQ so I can run CD Roms provided by NGB". This block should be as specific as possible so the right equipment can be bought to do the proper job.

Block 10- Justification: This narrative should answer the question of "Why do you need this software, hardware, commo equipment, or service?" You may attach written requirements by NGB if appropriate.

Block 11- Proposed Solution: If there are other ways to solve the requirement propose them here. Partitioning drives, LAN to share programs or data, alternatives in programming all are facts to be considered.

Block 12- Impact if Disapproved: Provide narrative explaining what will happen if the IMAC doesn't approve the request. Show what it will cost in the way of time or money. Explain what essential tasks cannot be performed, what reports or required information can no longer be submitted. If this is a proposal for future upgrade show how you can get along for the present but how your mission will degrade the longer you are without. Don't indicate Mission Failure if you are able to get the job done with current equipment.

Block 12a- Mission Impact Code: Identify either "A", "B", or "C" indicating by letter code what you put down in narrative in block 12.

d. Do NOT fill out any information on the reverse side of the AGKS 2500-R.

2. AGKS Form 2501-R: Meridian Telephone Worksheet

a. Purpose: The Meridian Telephone Worksheet is used to request changes in programable Meridian Telephone systems.

b. Procedure: The user should fill out the form any time there is a need to move a telephone instrument from one location to another or change the programming of the different services provided. The AGKS 2501-R should be given to the Telecommunication specialist responsible for the telephone system to be kept on file to show the changes that have occurred (in case of power failure and reprogramming needs)

c. Instructions to fill out AGKS 2501-R:

Requestor: The person filling out the form. Indicate POC's phone number.

Date of Request: The Day, Month, Year the request was submitted.

Date Service Required: The date that the changes should be made. Extensive changes or services that require outside resources may need longer lead time.

Phone number: The current phone number.

Name: The user of that Phone.

Old Jack Number: The coded number on the jack cover on the wall that leads to the phone. This should be the current Jack number if you are not moving the phone.

New Jack Number: The coded number on the jack cover on the wall that will lead to the phone in its new location.

Extension Busy: What phone number you want the call to forward to if the current phone is busy.

Extension No Answer: What phone number you want the call to forward to if the current phone is unanswered.

1 June 1996

Call Pick up Group: List the office that will be able to hear the phone ring and answer it.

Voice Mail: What phone number will the call be sent to if a caller presses "0" when directed.



PART II - TECHNICAL SOLUTION AND COSTING (Completed by DOIM)

13. ACQUISITION METHOD <input type="checkbox"/> PURCHASE <input type="checkbox"/> OTHER	14. ESTIMATED SYSTEM LIFE	15. CAPRS <input type="checkbox"/> YES <input type="checkbox"/> NO	16. COMMUNICATION FORMS REQUIRED <input type="checkbox"/> YES (Indicate below) <input type="checkbox"/> NO <input type="checkbox"/> ECONOMIC ANALYSIS <input type="checkbox"/> COMMERCIAL COMMUNICATION WORK ORDER <input type="checkbox"/> LOCAL SERVICE REQUEST
17. LOCAL FUNDING AVAILABLE <input type="checkbox"/> YES <input type="checkbox"/> NO	18. FUNDING REQUIREMENT <input type="checkbox"/> OMA <input type="checkbox"/> OPA		

19. COST DATA (Attach itemized listing)	PROJECTED COSTS		
	ONE TIME	ANNUAL RECURRING	ACTUAL
COMMUNICATION			
1.			
2.			
3.			
AUTOMATION EQUIPMENT			
1.			
2.			
3.			
SOFTWARE			
1.			
2.			
3.			
CONTRACTUAL SERVICES			
1.			
2.			
3.			
PERSONNEL (In house)			
1.			
2.			
3.			
SITE PREPARATION			
1.			
2.			
3.			
MAINTENANCE			
1.			
2.			
3.			
TRAINING			
1.			
2.			
3.			
OTHER			
1.			
2.			
3.			

PART III - VALIDATION/APPROVAL (For IMAC use)

20. IMAC	<input type="checkbox"/> REVIEWED ONLY <input type="checkbox"/> VALIDATED <input type="checkbox"/> APPROVED <input type="checkbox"/> DISAPPROVED
-----------------	---

