

Summary of Changes

USMEPCOM Regulation 25-3, April 28, 2008

Information Technology: Management of Subdisciplines

Managing USMEPCOM Information Technology Directorate (J-6/MIT) Resources

Incorporating Change effective March 9, 2012

See the following references for minor revision(s) that have been made:

- Paragraph 2-8: Added subparagraph y.

DEPARTMENT OF DEFENSE
HEADQUARTERS, UNITED STATES MILITARY ENTRANCE PROCESSING COMMAND
2834 GREEN BAY ROAD, NORTH CHICAGO, ILLINOIS 60064-3094

USMEPCOM Regulation
Number 25-3

April 28, 2008
Incorporating Change effective March 9, 2012

Effective date: May 26, 2008

**Information Technology: Management of Subdisciplines
MANAGING INFORMATION TECHNOLOGY RESOURCES**

FOR THE COMMANDER:

OFFICIAL:

D. R. O'Brien
Deputy Commander/Chief of Staff



J.M. Davis
USMEPCOM Publications Officer

DISTRIBUTION:

A (Electronic only publication)

Summary. This regulation consolidates several United States Military Entrance Processing Command (USMEPCOM) publications. The guidance contained is for implementing, managing, and using all USMEPCOM Information Technology (J-6/MIT) resources. It covers information assurance, system security of all hardware and software, system development and analysis, life-cycle management, user support and services, telecommunications, telephones, copiers, Enterprise Server and operations in support of these resources. Prescribes the use of USMEPCOM Forms 25-3-4-E (USMEPCOM Acceptable Use Policy), 25-3-5-E (Data-at-Risk), and 25-3-6-E (DAR Official Travel Authorization Card). Rescinds the use of USMEPCOM Forms 25-3-1-R-E (Information Mission Elements Need Statement (IMENS) and 25-3-2-R-E (Automation Equipment Log).

Applicability. This regulation applies to all users, planners, and developers of J-6/MIT systems within the command.

Supplementation. Supplementation of this regulation is prohibited without prior approval from Headquarters, United States Military Entrance Processing Command (HQ USMEPCOM), Attention: J-6/MIT, 2834 Green Bay Road, North Chicago, IL 60064-3094.

Suggested improvements. The proponent agency of this regulation is HQ USMEPCOM, J-6/MIT. Users will send comments and suggested improvements by memorandum or Department of the Army (DA) Form 2028 (Recommended Changes to Publications and Blank Forms) to HQ USMEPCOM, Attention: J-6/MIT, 2834 Green Bay Road North Chicago, IL 60064-3094.

Management control process. This regulation contains management control provisions and provides a management control evaluation checklist in appendix B (Management Control Evaluation Checklist - Managing Information Technology Resources) for use in conducting management controls.

*This regulation supersedes USMEPCOM Regulation 25-3, August 10, 1992; USMEPCOM Regulation 25-9, September 11, 1998; USMEPCOM Regulation 25-10, November 28, 1990; and USMEPCOM Memorandum 25-51, August 29, 2005. This regulation also rescinds USMEPCOM policy memorandums 5-1, November 16, 2004; 5-2, January 6, 2003; and 5-3, January 10, 2003.

Table of Contents (TOC)

	Paragraph	Page
<u>Chapter 1</u>		
Introduction		
Purpose	1-1	1
References	1-2	1
Abbreviations and terms	1-3	1
Responsibilities	1-4	1
Managing information resources and technology	1-5	5
Information as a resource	1-6	6
Use of J-6/MIT to improve mission efficiency and effectiveness	1-7	6
User/customer focus	1-8	7
Enterprise information systems and data sharing	1-9	7
Nonpolicy procedures	1-10	7
<u>Chapter 2</u>		
Information Assurance		
Overview	2-1	8
Designated approval authority	2-2	8
Information Assurance Program Manager	2-3	9
Information Assurance Network Officer	2-4	10
Information Assurance Manager	2-5	11
Information Assurance Officer	2-6	12
System Administrator	2-7	13
System users	2-8	14
<u>Chapter 3</u>		
Life-cycle Management		
Overview	3-1	17
Requirement identification	3-2	17
Configuration Control Board and Configuration		
Control Sub-Board Interface	3-3	17
Sharing J-6/MIT resources	3-4	17
Systems planning	3-5	17
Acquiring J-6/MIT hardware	3-6	17
Acquiring J-6/MIT software	3-7	18
Maintenance considerations	3-8	19
Excess J-6/MIT hardware and software	3-9	19
<u>Chapter 4</u>		
System Development		
Overview	4-1	20
Systems analysis	4-2	20
Software development	4-3	20
Software testing	4-4	20
Data administration	4-5	20
Software development support	4-6	21
Documentation	4-7	21
Software configuration management	4-8	21
Command enterprise Web development	4-9	21
Information architecture	4-10	21

	Paragraph	Page
<u>Chapter 5</u>		
USMEPCOM Data Communications Networks		
Overview	5-1	22
Network technical requirements	5-2	22
Network design	5-3	22
Network installation	5-4	22
Network operations	5-5	22
Temporary issuing of network equipment, computers, and peripherals	5-6	22
Network management	5-7	22
Network documentation	5-8	23
End-user network operations on the Local Area Network/Wide Area Network	5-9	23
Network, computer, and peripheral maintenance	5-10	23
Equipment warranties	5-11	24
Service outages	5-12	24
Access to USMEPCOM networks, devices, and services	5-13	24
User and Information Technology Specialist's responsibilities	5-14	24
USMEPCOM e-mail system	5-15	24
Non-governmental e-mail system	5-16	24
Assistance and problem resolution	5-17	25
Other networks	5-18	25
Internet access and monitoring	5-19	25
Intranets and extranets	5-20	25
External accesses to USMEPCOM network	5-21	25
<u>Chapter 6</u>		
Help Desk		
Help Desk	6-1	26
Help Desk operations	6-2	26
Request for assistance and reporting problems	6-3	27
Managing assistance and problems	6-4	27
<u>Chapter 7</u>		
Software Management		
Command software management program	7-1	28
Command Software Manager	7-2	28
Software residing on USMEPCOM PCs	7-3	28
Screensavers	7-4	28
Internet downloads	7-5	28
Site licensing	7-6	28
Original commercial-off-the-shelf software media	7-7	28
End-user training	7-8	28
<u>Chapter 8</u>		
Telephones		
Communications-specialist	8-1	29
Telecommunications Control Officer	8-2	29
Telephone controls	8-3	29
Request for telecommunications services	8-4	29
Telephone service ordering office	8-5	29
Government-owned telephone equipment	8-6	29

	Paragraph	Page
Verifications and certification of communications bills	8-7	29
Reimbursement for official telephone calls	8-8	30
Telephone toll credit cards	8-9	30
Collect calls	8-10	30
Facsimile equipment	8-11	30
Digital sender equipment	8-12	30
Headquarters public branch exchange phone systems	8-13	30
Wireless communications devices	8-14	30
Pagers	8-15	31

Chapter 9

Enterprise Server

Overview	9-1	32
Operating hours	9-2	32
Computer room access	9-3	32
Technical support	9-4	32
Enterprise Server telecommunications service	9-5	32
Billing and accounting (chargeback system)	9-6	32
Application approval	9-7	32
Users working group	9-8	32
Requests for building special print forms	9-9	32
Backup and recovery	9-10	32
Enterprise Server continuity of operations plan	9-11	33

Chapter 10

Web Infrastructure

Overview	10-1	34
USMEPCOM Internet Web site	10-2	34
USMEPCOM intranet Web site	10-3	34
USMEPCOM Internet item implementation process	10-4	34
USMEPCOM network intranet item implementation process	10-5	34
Web technical design, development, security, operations, and maintenance	10-6	34

Chapter 11

Copier Usage

Printing and self-service coping	11-1	35
Self-service copiers – new requirements	11-2	35
Self-service copiers – replacement of cost-per-copy/flat rate copiers	11-3	35
Self-service copiers – replacement of purchased copiers	11-4	35
Copier reports	11-5	36
Liaison support	11-6	36

Appendixes

A. References

B. Management Control Evaluation Checklist - Managing Information Technology Resources

C. Instructions for completion of Information Mission Elements Need Statement

D. Telephone service basis of issue

E. Format to request telecommunications service

Glossary

Chapter 1

Introduction

1-1. Purpose

This regulation establishes and assigns USMEPCOM responsibilities for the management of information resources and J-6/Information Technology Directorate (MIT). This regulation implements the provisions of the Clinger-Cohen Act (Public Law 104-106), [Army Regulation \(AR\) 25-1](#) (Army Information Technology) and other related Department of Defense (DOD) regulations listed in appendix A. It addresses the management of information as a USMEPCOM resource and the J-6/MIT resources to support those requirements. This regulation does not modify the Memorandum of Understanding (MOU) between DOD, J-6/MIT, and Selective Service System (SSS).

1-2. References

References are listed in appendix A.

1-3. Abbreviations and terms

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

1-4. Responsibilities

a. USMEPCOM Commander will:

(1) Delegate authority to the Director of Information Technology/Chief Information Officer for managing USMEPCOM J-6/MIT resources and to serve as the USMEPCOM Chief Information Officer (CIO).

(2) Ensure the CIO and Deputy CIO (DCIO) are professionally certified in the CIO competencies by a professional/government CIO counsel-acknowledged institution at the graduate educational level or higher or the equivalent.

b. Chief Information Officer/Director, Information Technology (J-6/MIT) will:

(1) Serve as the principal focal point for USMEPCOM matters with all outside agencies to include major commands, other military departments, federal agencies, academia and industry.

(2) Serve as principal advisor to the commander on all issues and initiatives.

(3) Set policies and requirements for the operation of the Enterprise Server in accordance with (IAW) guidance from the USMEPCOM Commander and support from the Director, SSS; and act in agreement with the MOU between the DOD and SSS.

c. Deputy Chief Information Officer/Deputy Director, Information Technology (J-6/MIT) will:

(1) Serve as the technical advisor to the DOIT/CIO and act with and for the director in his or her absence.

(2) Establish and manage the effectiveness of the Information Systems Security Program (ISSP) within the command.

(3) Ensure Homeland Security Presidential Directive-12 is implemented.

d. Information Assurance Manager (IAM) will:

- (1) Implement the overall security program, focusing on J-6/MIT security.
- (2) Provide initial and annual J-6/MIT security training for USMEPCOM personnel.

e. Enterprise Server Information Assurance Manager will:

- (1) Ensure the integrity of the USMEPCOM/SSS Enterprise Server system.
- (2) Control system access, and ensure only authorized individuals gain physical access to the facility.
- (3) Control access within the system for sensitive components and data sets administered by J-6/System Support Branch (J-6/MIT-SSB).
- (4) Provide assistance to users, as required, to maintain a coordinated overall system security program.

f. Information Assurance Network (IANO) Officer will:

Implement the network security program and act as the point of contact (POC) for all network security matters, virus protection and network backups.

g. Director, Facilities (J-4/MFA) will:

- (1) Identify all military entrance processing stations (MEPSs), sectors, and HQ USMEPCOM relocations or renovation projects requiring J-6/MIT actions through the Program Objective Memorandum (POM) process. J-6/Network Support Branch (J-6/MIT-NSB) will ensure that resources in support of J-4/MFA actions are submitted to J-8/Resource Management Directorate (J-8/MRM) or funding. J-6/MIT will identify, defend and execute funding resources to support all facility relocation or renovation projects.
- (2) Update J-6/MIT on the status of relocations and renovations to keep projects on track.

h. Director, Resource Management (J-8/MRM) will assist in obtaining funds to accomplish the J-6/MIT initiatives.

i. Directors, special staff officers, and sector and MEPS commanders will:

- (1) Apply security requirements outlined in [AR 25-2](#) (Information Assurance) and all applicable directives to any command J-6/MIT resource within their area of responsibility.
- (2) Ensure adherence to provisions of [AR 340-21](#) (The Army Privacy Program).
- (3) Ensure physical security and accountability of all J-6/MIT equipment and associated J-6/MIT program products IAW [AR 190-13](#) (The Army Physical Security Program) and [AR 190-51](#) (Security of Unclassified Army Property [Sensitive and Nonsensitive]).
- (4) Ensure sufficient supply of J-6/MIT consumables is on-hand, IAW USMEPCOM Regulation 710-2 (Requisition and Issue of Supplies and Equipment).

(5) Ensure only authorized software resides on J-6/MIT systems.

(6) Ensure adherence to guidance for proper use of all resources including equipment, software and servers, such as electronic mail (e-mail) and Internet capabilities.

(7) Appoint an alternate to the MEPS information technology specialist (ITS) to manage day-to-day use of J-6/MIT resources within their area of responsibility.

(8) Adhere to prescribed procedures for requesting J-6/MIT resources electronically via USMEPCOM MKS system. Instructions for completing this electronic form are in appendix C (Instructions for completion of Information Mission Elements Need Statement [IMENS]).

(9) Ensure appropriate training on J-6/MIT resources.

j. Sector and MEPS commanders will:

(1) Work with directorates to ensure proper preparation of sites for installation of J-6/MIT equipment.

(2) Monitor maintenance procedures at their sector or MEPS and ensure calls are placed to the proper maintenance personnel in a timely manner, when service is required.

(3) Serve as the POC for relocation and alignment of J-6/MIT resources to comply with allowance documents and table 3 of MEAD within their area of command.

(4) Enforce compliance with USMEPCOM configuration management and security directives and property accountability regulations.

(5) Adhere to prescribed procedures for requesting J-6/MIT resources for USMIRS equipment and software, through J-6/Plans and Policy Branch (J-6/MIT-PPB) and J-3/Liaison Branch (J-3/MOP-CO-LA) by following all required guidelines.

(6) Designate in writing the Telecommunications Control Officer (TCCO).

(7) Appoint an alternate to the MEPS ITS to manage day-to-day use of J-6/MIT resources within their area of responsibility.

k. Sector and MEPS ITSs will:

(1) Act as the liaison for all matters concerning J-6/MIT resources within their MEPS or sector.

(2) Prepare and maintain a file IAW guidance prescribed in [AR 25-400-2](#) (The Army Records Information Management System (ARIMS) of all locally requested and approved Information Mission Elements Needs Statement (IMENS) forms for all MEPS or sector acquired equipment and software.

(3) Maintain a current inventory of all hardware resources in coordination with the supply technician and/or property book officer (PBO).

(4) Maintain all USMIRS equipment and USMIRS related equipment requests, following guidelines as directed from J-6/MIT-PPB and J-3/MOP-CO-LA.

(5) Conduct an annual inventory of all commercial-off-the-shelf software (COTS) packages in the MEPS or sectors, reporting all discrepancies to HQ USMEPCOM ATTN: J-6/MIT, Command Software Manager, 2834 Green Bay Road North Chicago, IL 60064-3094.

(6) Provide introductory and annual refresher training for local J-6/MIT users and acquaint them with J-6/MIT hardware and software operations.

(7) Validate requirements with functional proponent for all hardware/software and prepare the IMENS form for submission to J-6/MIT-PPB.

(8) Ensure physical security and accountability for all J-6/MIT-IAO equipment within their area of responsibility.

(9) Complete applicable portions of the Internal Management Control Review checklist annually for forwarding to J-6/MIT-PPB.

(10) Receive and secure new deliveries of COTS, government-off-the-shelf (GOTS) and USMEPCOM unique software.

(11) Conduct personal computer (PC) hard drive audits on an annual basis to ensure no copyright/license violations exist within their areas of responsibility. The ITS have the authorization to remove any unapproved software programs and /or files during the audit.

(12). Ensure information security procedures are followed within the MEPS.

(13) Assist other organizations in maintaining an accurate inventory of their equipment on site, which includes the receipt and return of equipment to other organizations.

(14) Ensure the anti-virus program is properly installed on all PCs and laptops and kept current using updates from USMEPCOM approved sources only.

(15) Maintain a network documentation folder IAW paragraph 5-9.

(16) Ensure the backup individual is trained in J-6/MIT Help Desk procedures IAW chapter 6.

(17) Enter and/or monitor submission of Problem Reporting (PR) and System Change Proposal (SCP) data into the Software Configuration Management (SCM) IAW chapter 4.

(18) Ensure periodic maintenance of the PCs hard drives by deleting unnecessary temporary files and running utilities on at least a quarterly basis.

(19) Provide initial and annual J-6/MIT-IAO security training and USMEPCOM Integrated Resources System (USMIRS) training to all sector and MEPS personnel.

[TOC](#)

l. Privileged users. Privileged users are authorized users who have access to system control, monitoring, administration, investigation, database, or compliance functions. Privileged user access explicitly authorizes access by specific users to processes, computers, computer resources, or protected information.

(1) Persons holding these positions will be designated as IT-I or IT-II and appropriate security investigations will be completed as described in [AR 25-2](#), section V, chapter 4-14. Appropriate

investigation paperwork will be submitted prior to being granted “privileged user” access.

(2) Persons holding these positions will be trained and certified IAW [DOD Directive 8570.01](#) (Information Assurance Training Certification), and Workforce Management and Department of Army (DA) Best Business Practice (BBP) 05-PR-M-0002: Information Assurance Training.

(3) Privileged User access is granted IAW applicable laws and requirements for background investigations, special access, and IT position designations. Privileged user access will be requested in writing utilizing a [DD Form 2875](#) (System Authorization Access Request (SAAR)). The complete [DD Form 2875](#) will be submitted to the J-6/MIT-IAO office.

(4) Only the J-6/MIT-IAO has the authority to grant Privileged User access. Only Privileged Users will be granted administrative privileges.

(5) Privileged users will enforce system access, operation, maintenance, and disposition IAW local policies and practices.

(6) Privileged users will verify that personnel meet required security investigation, clearance, authorization, mission requirement, and supervisory approval before granting access to the IS.

(7) Only privileged users may install, modify, or remove any hardware or authorized software (i.e. freeware/shareware, security tools, etc.)

m. End users. End users will follow and adhere to all guidance and policy stated in this regulation or to guidance and procedures stated in any referenced regulation or document. Supervisors are responsible for any employee not following these guidelines. Any user found non-compliant with published guidance may be subject to disciplinary actions. Users will certify compliance with J-6/MIT-IAO security training that is conducted annually. Ensure that all Common Access Card requirements are met and adhered to.

1-5. Managing information resources and technology

a. Information resources, according to [AR 25-1](#) refers to all resources and activities employed in the acquisition, development, collection, processing, integration, transmission, dissemination, media replication, use, retention, storage, retrieval, maintenance, access, disposal, security, and management of information. Information resources include policy, data, equipment, and software applications and related personnel, services, facilities, and organizations, except those areas covered by separate regulation.

b. IAW [AR 25-1](#), any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by USMEPCOM. Responsibility includes computers, ancillary equipment, software, firmware and similar procedures, services, and related resources.

[TOC](#)

c. The J-6/MIT-SSB Enterprise Server supports USMEPCOM and SSS on a data service center basis to include computer operations, job scheduling, input/output (I/O), tape library support, telecommunications processing, physical and data security, and system software support.

d. IAW [AR 25-1](#), this regulation supports the precept that information is a strategic defense asset in peacetime and conflict. The peacetime information infrastructure must support wartime requirements by providing information services for sustainment of armed forces.

1-6. Information as a resource

a. Information is a valuable resource and will be managed as any other asset, such as funds, personnel and equipment. IAW [AR 25-1](#) the costs of collecting, processing, distributing and storing information make it impossible to view information as a free commodity. Except where restricted for reasons of security, privacy, sensitivity or proprietary rights, information will be managed as a shared resource which will be made available to all those needing it to accomplish their mission and functions. Requirements for information and the supporting technology will be carefully identified. Supporting J-6/MIT and related investments will be evaluated in terms of their support of USMEPCOM processes and their corresponding information requirements.

b. J-6/MIT-DICO will maintain and ensure all data it collects is readily accessible to whoever requires it. This includes actively pursuing and identifying organizations that could benefit from the data and establishing data transfer methodologies that conform to the Joint Technical Architecture standards. This practice promotes economic use of resources by eliminating duplication, improving synchronization and reducing costs. J-6/MIT-DICO provides standard data to those who require it, relieving them from the requirement of creating data for their particular system.

c. Information will be managed through centralized control and either centralized or decentralized execution. Approved DOD-wide methods, approaches, models, tools, data, J-6/MIT and information services will be used.

1-7. Use of J-6/MIT to improve mission efficiency and effectiveness

a. Provides capabilities that can save manpower, reduce redundancy, increase accuracy, increase speed transmission, and increase availability of information. When available, appropriate and cost-effective J-6/MIT will be used to support USMEPCOM processes.

b. Information in electronically readable format is easily stored, replicated, distributed, shared, and presented in a manner useful to support USMEPCOM processes and decision-making. Whenever possible, information will be stored in an electronically readable format and shared horizontally and vertically with those requiring the information.

c. Integration of information resource systems throughout the organization generally reaps dividends in the form of increased efficiency resulting from better coordination among functional areas and the availability of consistent information.

d. Proponent functional requirements are necessary for J-6/MIT systems to be effective and must be accurately defined. Verification of compliance with these requirements is a critical step in ensuring that only quality systems are fielded. It is imperative that professionals establish and follow comprehensive and thorough systems quality assurance evaluations prior to release for use on any platform.

1-8. User/customer focus

a. Provides information capabilities and services. These capabilities and services are not an end in themselves. Ultimately, they have value only in their support of the mission or to those who provide other forms of support to the mission area. Because of its support role, the J-6/MIT community must maintain a constant focus on the needs of its user community.

b. This focus will include awareness of the current requirements for support, the quantity and quality of support provided, future customer requirements, and emerging J-6/MIT capabilities that can benefit the customer. A relationship between the J-6/MIT community and users, in which both the customer and the service provider take responsibility for communicating with each other. Each J-6/MIT management process will foster this dialogue. Although primary responsibility will be assigned for the various aspects of that process to work, both parties must remain actively engaged for it to succeed.

c. Customers must be sensitive to the J-6/MIT community's need to be involved in seemingly unrelated management issues because of potential impacts. Participate actively in the support process, especially in the definition of their requirements, and be aware of and conscientiously apply all appropriate information security measures. The J-6/MIT community will embrace accountability to the customer as an essential element of the J-6/MIT management process. Service and accountability to the user population will be incorporated in the decision to outsource or consolidate and will be included in agreements and contracts for J-6/MIT support capabilities.

1-9. Enterprise information systems and data sharing

The concept of the USMIRS encompasses an enterprise wide data integration concept. This includes the full integration of workload data with budget, facilities, personnel, equipment, and command planning data requirements. The design/development of each system will address its requirements to function within the Enterprise Data Sharing model.

1-10. Nonpolicy procedures

All nonpolicy procedures are located on [Sharing Policy Experience And Resources \(SPEAR\)](https://spear/Headquarters/J-6%20MEIT/SitePages/Home.aspx), at the link (<https://spear/Headquarters/J-6%20MEIT/SitePages/Home.aspx>). Updates to SPEAR information will be available by email from the USMEPCOM proponents.

Chapter 2

Information Assurance

2-1. Overview

Information assurance (IA) is the component of J-6/MIT-IAO program management that assures operational readiness by providing for the continuous availability, reliability and confidentiality of information and its supporting technological infrastructures. It is the responsibility of the entire command to understand and abide by all regulations, policies, and procedures designed to meet these information security goals. This section provides general guidance to be used for all J-6/MIT resources. See Office of Management and Budget (OMB) Circular (Cir) A-130 (Management of Federal Information Resources); National Institute of Standards and Technology (NIST) Special Publication 800-12 (An Introduction to Computer Security (The NIST Handbook)); [DOD Directive 8500.1E](#) (Information Assurance); Title 17, U.S. Code; Title 18, U.S. Code; and [AR 25-2](#) for additional information. This section addresses IA functions and responsibilities of managers, system administrators, and users. All personnel will be held liable for violating the punitive provisions of [AR 25-2](#).

2-2. Designated approval authority (DAA) will:

a. Be a United States (US) citizen and US Government employee, with minimum grade requirement of Senior Executive Service 1 (SES1).

b. Have the authority to accept the risk of operating all information systems under the DAA's jurisdiction.

c. Ensure a highly trained and qualified security staff to support technically correct security assessments of the information systems under his or her jurisdiction.

d. Understand the operational need for the system(s) and the operational impact if any of the information systems are taken out of service.

e. Ensure IA is incorporated as an element of DOD information system life-cycle management processes.

f. Ensure the security of DOD information systems or enclaves under his or her purview.

g. Ensure all IA-related positions are assigned in writing, include a statement of IA responsibilities, and appointees to positions receive appropriate IA training.

h. Establish the command's formal Certification and Accreditation (C&A) program. The DAA is responsible for the following C&A actions:

(1) Ensure each system is properly certified and accredited based on the system environment and sensitivity levels.

(2) Issue a written accreditation/certification statement after formal review of the System Security Authorization Agreement (SSAA).

(3) Grant final and interim accreditation of the network in a specified security mode.

(4) Review the SSAA to confirm compliance with DOD established policy and review the risk

assessment to ensure risk levels are within acceptable limits.

(5) Establish working groups to resolve issues regarding those systems requiring multiple or joint accreditation. Document condition or agreements in memoranda of agreement (MOA).

(6) Ensure when sensitive but unclassified (SBU) information is exchanged between logically connected components, the content of this communication is protected from unauthorized observation by acceptable means, such as encryption, and/or Protected Distribution Systems (PDS).

(7) Ensure IA-related events or configuration changes will impact accreditation are reported to affected parties, such as Information Owners and DAAs of interconnected DOD information systems.

i. Ensure the establishment, administration, and coordination of security for systems that the DAA's command or organization operates.

j. Ensure an incident reporting program is established and security incidents or events are reported to affected parties (i.e., interconnected systems, data owners, etc.) IAW [AR 25-2](#).

k. Ensure organizations plan, budget, allocate and spend resources to achieve and maintain an acceptable level of security and to remedy security deficiencies.

l. Ensure an education, training and awareness program is in place.

m. Complete training and certification.

2-3. Information Assurance Program Manager (IAPM) will:

a. Hold a US Government security clearance and access approval commensurate with the level of information processed by the information system.

b. Ensure a contractor will not permanently fill this position. Temporary assignment of contractor personnel for a specified time, as an exception, is authorized until the position can be properly filled.

c. Complete the prescribed training and certification.

d. Establishing, managing, and assessing the effectiveness of all aspects of the IA program within USMEPCOM.

e. Develop, manage and maintain a formal IA security program includes defining the IA personnel structure and ensuring the appointment of an IANO, and IAM.

f. Implement and enforce Chairman, Joint Chiefs of Staff, DOD and IA policy.

g. Ensure IA personnel review and implement bulletins and advisories that affect the security of their information systems.

h. Ensure all IA personnel receive the necessary technical (e.g., operation system, network, security management, system administration) and security training to carry out their duties and maintain their certifications.

[TOC](#)

- i. Serve as the primary POC for IA-related actions. This includes, Information Assurance Vulnerability Alert (IAVA) reporting, compliance, vulnerability assessments, and feedback on current or upcoming IA policies.
- j. Ensure the Defense Information Technology Certification and Accreditation Process (DITSCAP) program is implemented.
- k. Ensure the development of system C&A documentation.
- l. Ensure approved procedures are in place for clearing, purging, and releasing system memory, media, output and devices.
- m. Ensure DAAs maintain a repository for all system C&A documentation and modifications.
- n. Ensure security violations and incidents are reported to the Continental United States Regional Computer Emergency Response Team (CONUS RCERT).
- o. Ensure protective and corrective measures are implemented for vulnerabilities or incidents per direction of the CONUS RCERT.
- p. Verify data ownership responsibilities (including accountability, access, and special handling requirements) for each information system (IS) or network.
- q. Establish, conduct, and oversee a command program of announced and unannounced IA assessments.
- r. Program, manage, execute, and report Information Technology Directorate Information Assurance Office (J6/MIT-IAO) IA budgets.
- s. In coordination with the J-3/MOP-C0-LA and J-6/MIT-IAO, provide technical and non-technical information to support the Information Operations Condition (INFOCON) program.
- t. Ensure program controls are in place to confirm user access requirements.

2-4. IANO will:

- a. Hold a US Government security clearance and access approval commensurate with the level of information processed by the information system.
- b. Complete the prescribed training and certification.
- c. Perform as the program manager of the Information Systems Security (INFOSEC) program, oversight of the Security, Awareness, Training and Education (SATE) Program, and C&A Program.
- d. Advise the IAPM or DAA on the use of specific network security mechanisms.
- e. Evaluate network threats and vulnerabilities to ascertain the need for additional safeguards.
- f. Assess changes in the network, its operational and support environments, and operational needs that could affect its accreditation.

- g. Oversee periodic use of authorized scanning and assessment tools.
- h. Assist the IAPM in monitoring and enforcing the IAVA processes.
- i. Develop, coordinate, and ensure implementation of policy to secure all USMEPCOM information systems, by ensuring confidentiality, authorization, nonrepudiation, integrity, and availability of networks within USMEPCOM.
- j. Reviews joint and service level information systems procedures and policies for integration into the USMEPCOM program.
- k. Acts as the principal advisor to the CIO for all information systems security concerns.
- l. Administers Information Systems Security Risk Management program.
- m. Coordinates with designated agencies to resolve INFOSEC issues.
- n. Ensures appropriate countermeasures exist and are implemented to respond to identified threats or assessed vulnerabilities.

2-5. IAM will:

- a. Hold a US Government security clearance and access approval commensurate with the level of information processed by the information system.
- b. Complete the prescribed training and certification program.
- c. Appoint an information assurance officer (IAO) in writing for each information system and network, and ensure they receive proper technical training and they are following information system policies and procedures.
- d. As needed, appoint other information assurance professionals in writing (e.g., IAOs, Terminal Area Security Officers, Information Technology Officers, etc.) to assist with the implementation and enforcement of IA-related policy and guidance. Ensure they receive proper technical training to carry out their tasks.
- e. Implement the IA program within their command and ensure all systems are accredited IAW the DITSCAP and USMEPCOM C&A program.
- f. Maintain a repository of all systems that have certified and accredited documentation.
- g. Inform the IAPM of any changes impacting the IA posture.
- h. Conduct periodic reviews of the systems and networks under their jurisdiction to ensure changes have not occurred that affect security and negate the accreditation.
- i. Review threat and vulnerability assessments to determine appropriate security measures are in place to manage the risk to systems and networks under their jurisdiction.
- j. Oversee the execution of the IA training and certification program within his or her jurisdiction.

- k. Enforce the established policy for review of weekly alerts, bulletins and advisories.
- l. Assess the impact to security based on reports from the DOD Computer Emergency Response Team (CERT) or service CERTs, and comply as prescribed in Incident and Vulnerability Reporting.
- m. Establish a program to review the systems and networks audit trails, and maintain an archive of all required audit records.
- n. Respond to IAVAs, Information Assurance Vulnerability Bulletins (IAVBs), and other vulnerability notification using the Network Common Relevant Operational Picture/Network Event Alert Reporting (NETCROP/NEAR) or the Asset and Vulnerability Tracking Resource (A&VTR) Systems.

2-6. IAO will:

- a. Hold a US Government security clearance and access approval commensurate with the level of information processed by the information system.
- b. Successfully complete technical and security training.
- c. Ensure a copy of IAO appointment letter is forwarded to the IANO.
- d. Ensure the information system is operated, used, maintained, and disposed of IAW Army Best Business Practice – Reuse of Army Computer Hard Drives 03-PE-O-0002.
- e. Ensure the network, site, system, or application information system is certified and accredited IAW the DITSCAP.
- f. Ensure accreditation and/or certification support documentation package responsibility for the system is developed, maintained, and updated as required.
- g. Ensure users and system support personnel have the required security clearances, authorization and need-to-know. Training and familiarity with internal security practices are required before granting access to the information system.
- h. Maintain copies on all issued accounts for User Memorandum of Agreement for the information systems or networks under their jurisdiction.
- i. Prepare, distribute, and maintain plans, instructions, guidance and standing operating procedures (SOPs) concerning the system operation security.
- j. Enforce security policies and safeguards on all personnel having access to the information system for which the IAO is responsible.
- k. Initiate protective or corrective measures to maintain security on information systems.
- l. Ensure warning banners are placed on all monitors and appear when a user accesses a system.
- m. Notify the IAM or IANO when changes occur on information system(s) that might affect accreditation/certification.

- n. Report security incidents to the IAM or IANO, IAW paragraphs 2-7(6), 2-8(24) and 6-2(b).
- o. Report the security status of the accredited environment as required by the DAA, and update the SSAA as the information system is modified or new components are added.
- p. Conduct periodic reviews to ensure compliance with the accreditation or certification support documentation package.
- q. Ensure approved security patches are installed as directed.
- r. Occasionally employ password-cracking tools to identify weak or non-compliant passwords.

2-7. System administrator (SA) will:

- a. Hold US Government security clearance and access approval commensurate with the level of information processed by the information system.
- b. Complete SA training and certification.
- c. Maintain information system and networks to include hardware and software.
- d. Monitor information system performance and system recovery processes to ensure security features and procedures are properly restored.
- e. Work closely with the IAO/IAM to ensure the information system or network is used securely.
- f. Report security incidents to the IAO/IAM immediately IAW this regulation.
- g. Provide customer support, ensure users have been granted the required security clearances, authorization, need-to-know, and are aware of their security responsibilities before granting access to the information system.
- h. Ensure the system is operated, maintained, and disposed of IAW this regulation, local directives, and as outlined in the Certification and Accreditation support documentation package.
- i. Assist the IAM and IAO in development and maintenance of C&A support documentation package.
- j. Conduct periodic reviews to ensure compliance with the C&A support documentation package.
- k. Establish audit trails and conduct reviews weekly, and ensure, as directed by the IAAO and IAPM, that audit records are archived for future reference.
- l. Provide backup of system operations.
- m. Ensure IAVAs, IAVBs, and other vulnerability notifications are applied to appropriate operating systems.
- n. Evaluate known vulnerabilities to ascertain if additional safeguards are needed.

[TOC](#)

- o. Advise the IAPM of odd, peculiar or strange security or integrity loopholes.
- p. In coordination with the IAO, administer user identification and authentication mechanism(s) of the information system or network.
- q. Administer and protect SA passwords. The minimum standard for all SA system passwords is a mix of 10 characters using four character sets (uppercase letters, lowercase letters, numbers, and special characters). SAs are prohibited from using their user identification (ID), common names, birthdays, telephone numbers, consecutive numbers or letters, alphanumeric sequential combinations, or dictionary words.
- r. Safeguard passwords at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system.
- s. Periodically, at the direction of the IAPM, will employ password tools to identify weak or non-compliant passwords.
- t. Ensure all high risk mobile information systems authorized for travel (i.e. laptops and removable storage devices such as thumb drives) are identified and appropriately configured and labeled. Thumb drives will be labeled with SF Form 710 (Unclassified Label for ADP Media in SCI Facilities). Laptops will be labeled with [USMEPCOM Form 25-3-5-E](#) (Data-At-Risk). When a laptop leaves USMEPCOM, sectors, or MEPSs from the controlled facility, it will be accompanied by a completed [USMEPCOM Form 25-3-6-E](#) (DAR Official Travel Authorization Card).

2-8. System users

End users (individuals/information system users, e.g., DOD military, civilians, and contractors) will:

- a. Be held liable for violating the punitive provisions of [AR 25-2](#).
- b. Ensure a [DD Form 2875](#) is completed for all account deactivations prior to departing USMEPCOM employment.
- c. Complete the INFOSEC training before gaining access to a USMEPCOM network or information system. Complete annual training as directed.
- d. Complete [DD Form 2875](#) (System Authorization Access Request (SAAR)) to request a new system or network account.
- e. Complete an [USMEPCOM Form 25-3-4-E](#) (USMEPCOM Acceptable Use Policy) annually.
- f. Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.
- g. Use DOD information systems only for official use and authorized purposes IAW [Department of Defense Instruction \(DODI\) O-8530.2](#), (Support to Computer Network Defense (CND)), **CAC login required**); and [DOD 5500.7-R](#) (Joint Ethics Regulation (JER)).
- h. Only access data or use operating systems or programs as authorized.

[TOC](#)

i. Not use private Government accounts off-site (e.g., at home, etc.) for USMEPCOM-related business, unless specifically authorized in writing by the USMEPCOM Commander.

j. Not use a private commercial Internet Service Provider (ISP) account (e.g., yahoo, hotmail, etc.) for USMEPCOM-related business.

k. Use US Government acquired hardware and software for USMEPCOM-related business. Use of personally owned hardware, software, shareware, or public domain software (such as peer-to-peer software) is prohibited unless a written waiver is granted by the DAA.

l. Protect controlled unclassified information and classified information to prevent unauthorized access, compromise, tampering or exploitation of the information.

m. Properly mark and safeguard sensitive-but-unclassified information so only authorized persons have access, it is used only for its intended purpose, and it retains content integrity.

n. Not share, disclose or display your password to anyone. Manage and protect passwords for systems requiring logon authentication. The USMEPCOM standard for user passwords is a mix of ten characters minimum using all four character sets. Users are prohibited from using their user ID, common names, birthdays, phone numbers, consecutive numbers or letters (888Aaa!*), alphanumeric sequential combinations (987AbC!@), or dictionary words.

o. Submit a waiver request to the DAA if a group account is needed.

p. Safeguard passwords at the confidentiality level for unclassified systems. Passwords will be classified at the highest level of information processed on that system.

q. Manually screen-lock the workstation when leaving the immediate work area. The default timeouts invoke password-protected screen savers must be set for 10 minutes or less. Log off the workstation at the end of each working day or when leaving the work area for 15 minutes or more.

r. Allow no maintenance to be performed on any workstation by anyone but authorized ITS. Virus-check all information prior to uploading onto any DOD or USMEPCOM information system.

s. Not load any unauthorized executable or program files (e.g., .exe, .com, .vbs, or .bat) onto DOD or USMEPCOM information systems. Any software or program file that is not a part of the approved USMEPCOM baseline, required for use by a user in execution of his or her mission will be approved by the DAA via the IMENS process.

t. Not engage in "streaming" content from audio, visual or data streaming media sources for non-mission related purposes. Viewing or listening to radio stations, news channels, stock updates, sports scores, or other non-mission related content for general, personal education or entertainment purposes is prohibited on government systems.

u. Immediately report any malicious or unintentional damage of government computer equipment or any unexplained/suspicious changes in configuration, operation, or data to the appropriate SA, IAO, or appropriate local law enforcement officials.

v. Not use the Internet for personal gain. Do not visit unauthorized Web sites (i.e., pornographic, gambling, or hate crime sites).

[TOC](#)

- w. Not write malicious code (e.g., virus or trojans).
- x. Report all security incidents immediately to their IAO.
- y. Not upload any sensitive-but-unclassified or personally identifiable information (PII) data files to Common-shared drive folders on any USMEPCOM IT system.

Chapter 3 Life-cycle Management

3-1. Overview

Ensure the life-cycle planning for all J-6/Infrastructure Support Division (J-6/MIT-ISS) resources. This is critical for the Command Information Management Plan.

3-2. Requirement identification

a. Planning for J-6/MIT resources at all levels concentrates on identifying future requirements, justifying and funding them. The IMENS process provides an electronic mechanism to evaluate requested changes to the command approved hardware and command approved software lists.

b. To request changes to the command approved hardware and command approved software lists, the functional proponent's MEPS or sector ITS will submit the Automated IMENS form using the MKS software for review and coordination. The IMENS request will contain sufficient justification to ensure the request to change the command approved hardware and software lists or to automate a function justifies the proposed expenditure of resources. The IMENS form will describe the requirement in terms of the functional need it will satisfy, rather than the specific equipment or products to meet the requirement. Once the functional requirement stated on the IMENS form is analyzed and moves through the approval chain, J-6/MIT will either approve or disapprove the request. The originator of an IMENS will receive an automated e-mail response if the IMENS is disapproved. At anytime through the approval process the originator can review the current state of an IMENS.

3-3. Configuration Control Board (CCB) and Configuration Control Sub Board interface (CCSB)

J-6/MIT may, upon their own initiative, request review by the CCSB or CCB any IMENS that represents a significant change to command approved hardware or software list or which may require significant expenditure of resources. Additionally, if an IMENS has been denied by J-6/MIT-ISS, the functional proponent that submitted the IMENS may request a review of that decision by the CCSB or CCB.

3-4. Sharing J-6/MIT resources

Wherever possible, ITS will satisfy requirements with existing J-6/MIT-ISS resources. To facilitate sharing, the CIO maintains a central record of the description, quantity, application, and location of all J-6/MIT resources.

3-5. Systems planning will:

a. Review the IMENS form for validity of functional requirements and conformance to USMEPCOM policy. If a proposed procurement will benefit all sectors and MEPSs, a command-wide buy will be initiated to approve the item for all sectors and MEPSs. J-6/MIT-ISS also monitors technology developments for opportunities that could support business process improvement.

b. Ensure appropriate architecture plans are in place and properly coordinated with and linked to the command strategic plan.

c. Develop and maintain the command J-6/MIT strategic plan.

3-6. Acquiring J-6/MIT hardware

a. DoD requirement contracts will satisfy requirements for J-6/MIT hardware when practical.

[TOC](#)

However, it is the contracting officer's decision what source of supply best meets the Government's needs. The activity may recommend a source but the contracting officer is not obligated to buy from that source. Only J-6/MIT-PPB will procure hardware and software. Whenever possible, all purchases will be shipped directly to the requesting MEPS with the exception of software. The IMENS will be reviewed to ensure conformance with established J-6/MIT standards and guidance. Any discrepancies must be coordinated and resolved prior to procurement.

b. Use of personally owned hardware to support USMEPCOM mission is prohibited. Personally owned computer equipment will not be used to access USMEPCOM networks, databases, or the Enterprise Server.

c. Printers, communications devices (hubs, switches, routers, modems, etc.), fax machines, copiers, telephones, and admin PCs, servers, and terminals will be procured by J-6/MIT-PPB. The MEPSs and sectors ITSSs will submit an Automated IMENS form (see app. C) for procurement of hardware from the command approved hardware list. J-6/MIT-PPB will process these requests, when funding is available and the functional requirement of the requests is approved. Acquisition of "free" hardware from outside sources such as Defense Reutilization Management Office by a sector or MEPS is not authorized.

d. Requests for functional use of USMIRS hardware will be submitted by IMENS, which is forwarded to J-3/MOP-CO-LA within the automated approval process. J-3/MOP-CO-LA will analyze the functional requirement supporting the request and, if approved, will recommend approval for processing to J-6/MIT-PPB.

e. With prior approval from J-6/MIT-PPB, sectors and MEPSs may locally purchase any hardware devices (i.e., A/B switch boxes, cables, and speakers) that are compatible with the operating system of the PC, as long as the device does not adversely affect the performance or security of the PC and the network. There will be no local procurements that will change the command approved hardware list or network capabilities of the J-6/MIT systems in sectors or MEPSs. All hardware device procurements for USMEPCOM will be processed by J-6/MIT.

f. Existing discretionary funds or supply funds (if appropriate) will be the only funds authorized for the purpose of local procurement of J-6/MIT-PPB hardware/devices. No additional funds will be authorized.

3-7. Acquiring software

The command software manager maintains the official five-part command approved software list. This list establishes all COTS, GOTS, USMEPCOM-unique software programs and applications approved for use within the command. The command approved software list may be printed as needed. Part I lists mandatory COTS software that will be purchased and installed on all admin PCs in the command. Part II lists COTS and command standard software that can be installed on any admin PC with prior IMENS approval from J-6/MIT-PPB. Part III lists approved software for USMIRS PC. Part IV lists approved software for Meal Check PC. Part V lists approved software for the Fingerprint PC.

a. The COTS software will be purchased as a command wide buy whenever possible to include upgrades to command standard software. A command wide IMENS will be prepared by J-6/MIT-PPB for the procurement of all software on Part I and Part II of the command approved software list. All COTS software procurements for HQ USMEPCOM, sectors, and MEPSs will be processed by J-6/MIT.

b. No personally owned software will be authorized for use within USMEPCOM. Only Government owned and approved software will reside on USMEPCOM PCs.

[TOC](#)

c. Each MEPS will submit an automated IMENS form to J-6/MIT-PPB for COTS software requirements stating the purchase will be funded by the MEPS. These IMENS forms will be reviewed to ensure conformance with established standards and directions. Any discrepancies will be coordinated and resolved by J-6/MIT-PPB prior to procurement. Depending on funding availability, the COTS software will be purchased and shipped to J-6/MIT-PPB and then redistributed to the MEPS. A copy of DD Form 250 (Material Inspection and Receiving Report) will be e-mailed to POC in J-6/MIT-PPB, not later than 14 working days after receipt of COTS software.

d. USMIRS users will submit requests for changes to USMIRS software IAW procedures outline in paragraph 4-3 of this regulation.

3-8. Maintenance considerations

MEPSs and sectors ITSs will promote preventive maintenance practices for J-6/MIT (e.g., keeping equipment dust-free, removing debris which accumulates inside printers, ensuring fans are not blocked, etc.) as suggested by the manufacturer.

3-9. Excess hardware and software

a. Hardware. Identify and report excess hardware resources IAW USMEPCOM Regulation 710-2 (Acquisition and Issue of Supplies and Equipment).

b. Software. Disposition of software is IAW chapter 7 of this regulation and current procedures located on SPEAR at the link (<https://spear/Headquarters/J-6%20MEIT/SitePages/Home.aspx>).

Chapter 4 System Development

4-1. Overview

J-6/MIT-Acquisition and Initiatives Division (J-6/MIT-A&I) provides all application software systems analysis, development, and maintenance support IAW industry standards for all areas of the command.

4-2. Systems analysis

J-6/MIT-A&I systems (software and hardware), working with the functional proponents to identify and properly specify functional requirements. Projects can include integrating new technologies into business practices, improving and automating manual processes, or enhancing current systems. The system requirements specification shall describe such things as functions and capabilities of the system; business, organizational and user requirements; safety, security, human-factors engineering (ergonomics), interface, operations and maintenance requirements; and design constraints and qualification requirements. J-6/MIT-SDB will ensure the system meets the functional requirements within cost, time, and resource constraints.

4-3. Software development

Software development procedures contain detailed requirements for proper documentation, review of program logic, and programmer testing procedures for all developed software to include database changes. In-process reviews are required at critical junctures to ensure adherence to design specifications and documentation requirements. System design documents are produced prior to programming, to validate compliance with user requirements. J-6/MIT-A&I is responsible for establishing, monitoring and enforcing software-programming standards.

a. New software development requests and changes to existing applications will be submitted as a SCP using the automated Software Configuration Management System (SCMS) tool.

b. J-6/MIT-A&I will be responsible for development or maintenance of all command-approved software except that approved by the USMEPCOM Commander, or the Chief of Staff, for outside contractor development or maintenance. USMEPCOM developed software will be utilized for internal use only. If a MEPS or directorate wishes to field their locally developed applications to other command users, a SCP utilizing SCMS will be developed which will be forwarded to the functional proponent for approval. Upon approval, J-6/MIT-A&I will review the application and modify it, if necessary, to command standards before assuming responsibility of the application and fielding it to appropriate command users.

4-4. Software testing

Formal software testing will be accomplished on all software. This testing requires rigid disciplined procedures to be followed which provide a detailed, step-by-step, process for validating that the software performs according to the original requirements and design. This is a critical part of the software development process and cannot be bypassed for any platform. J-6/MIT-A&I and the functional proponent will validate and complete a master test plan for use within the command. The master test plan will encompass unit testing, acceptance testing, and integration/system testing phases. A controlled test environment is maintained by the J-6/MIT-Quality Assurance Branch (J-6/MIT-QAB). This reflects the MEPS environment for both hardware and software.

4-5. Data administration

The data administration program establishes the necessary framework for identifying, organizing, and managing data to support the development and implementation of information systems. The program

[TOC](#)

focuses on managing information requirements from data modeling down to the data element level of detail including data mapping. These procedures and processes will be conducted IAW [DOD Instruction 8320.2](#) (Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense) and requires the active involvement of both functional experts and system developers. The program assists in understanding what the information requirements are, where official data is maintained and who will be using the data.

4-6. Software development support

This support includes application software system management, software interface and electronic data transfer support, and management and administration of production databases. This includes all J-6/MIT-A&I developed or supported electronic data transfer requirements and provides technical expertise in support of the J-6/MIT-Help Desk and all users of J-6/MIT-A&I systems. It implements all completed software systems/changes, software configuration management for all J-6/MIT-A&I developed/maintained software, and provides one-time special ad-hoc reporting requirements technical support, that cannot be supported by J-5/Program Analysis and Evaluation Directorate (MAE) using Quantitative Information Comparison-Redesigned (QuIC-R).

4-7. Documentation

Software applications will be documented within the code following Application Development and User Interface Standards. Change documents will be developed for all USMIRS application releases. User manual documentation or on-line help will be available for all applications to assist the user in using applications.

4-8. Software configuration management (SCM)

SCM is the responsibility of J-6/MIT-A&I. These procedures ensure proper maintenance and effective tracking of the change process of base-line applications software for all systems/platforms. This function includes version identification, development and production software library maintenance, and preparation and release of all software change packages. Users at HQ USMEPCOM, sectors, or MEPSs will utilize PR submitted to SCM, via automated SCMS tool, for fielded software problems identified. In addition, SCM will be utilized for SCP submissions.

4-9. Command enterprise Web development

J-6/MIT-A&I will develop, maintain, and coordinate the command's Enterprise Web strategy and architecture ensuring it aligns with the J-6/MIT strategic plan. Development and maintenance of the command's intranet ([SPEAR](#)) and Internet sites will be done IAW [AR 25-1](#), chapter 5.

4-10. Information architecture

Documented information architecture will be maintained to ensure cohesive development of disparate systems within the command. This architecture will fully describe the business process supported by information systems, their information requirements, business rules, applications, and supporting infrastructure.

Chapter 5

USMEPCOM Data Communications Networks

5-1. Overview

J-6/MIT-NSB (Network Support Branch) will be responsible for all aspects of the network servers, the Local Area Networks (LANs), Wide Area Network (WAN), and data communication connectivity between each MEPS, sector, and HQ USMEPCOM. These networks are designed for SBU data only. Users are not authorized to send any classified data across the network.

5-2. Network technical requirements

Responsible for all technical requirements for USMEPCOM data communication networks including all network equipment (which includes servers). Technical requirements need to meet applicable government and USMEPCOM standards including security and interoperability. J-6/MIT-NSB is also responsible for the technical requirements for any equipment that is used on the network. Any other military service equipment put on a USMEPCOM network will be coordinated with J-6/MIT-NSB.

5-3. Network design

J-6/MIT-NSB will be responsible for the design of the Networks used in MEPS, sectors, and HQ USMEPCOM. Any changes to the design will be approved by J-6/MIT-NSB.

5-4. Network installation

J-6/MIT-NSB will be responsible for the installation of network equipment including Enterprise switches, hubs, routers, servers, patch panels, and network drops. J-6/MIT-NSB will approve anyone else installing any network equipment in MEPSs, sectors, and HQ USMEPCOM including other service contractors.

5-5. Network operations

J-6/MIT-NSB will be responsible for the network operation in all MEPSs, sectors, and HQ USMEPCOM. J-6/MIT-NSB may restrict or allow MEPS personnel to access certain network equipment. J-6/MIT-NSB establishes guidelines, standards, policies, and procedures for effective LAN and WAN operations. J-6/MIT-NSB controls and coordinates installation and maintenance of computer network resources. J-6/MIT-NSB oversees the planning, installation, operation, and maintenance of command-wide data communications network servicing all levels of USMEPCOM. Responsible for configuration management, performance analysis, and fault analysis of all network components. J-6/MIT-NSB establishes guidelines, standards, policies, and procedures for effective LAN/WAN operations and monitors day-to-day network operations by utilizing network-monitoring tools to ensure network availability and interconnectivity via the Recruiting Services Network (RSN) at all USMEPCOM locations.

5-6. Temporary issuing of network equipment, computers, and peripherals

J-6/MIT-NSB may temporarily issue network equipment, computers, laptops, or peripherals. All requests for network equipment, computers, laptops, and peripherals should be made at least one week in advance to the J-6/MIT-Help Desk (Chapter 7 Software Management). This type of transaction needs to be coordinated with J-8/MRM-AD-LB (Logistics Branch) for temporary hand receiving process.

5-7. Network management

J-6/MIT-NSB will be responsible for managing all the USMEPCOM networks. J-6/MIT-NSB may work with other organizations to oversee or manage parts of the network. Responsibilities will include but not limited to:

- a. Configuration management, performance analysis, and fault analysis of all network components.

b. Testing new devices and network-related software prior to installation on the network; providing connection control and approval; network administration policy and guidance; and architecture and standards policy.

c. J-6/MIT-NSB will be responsible for all integration efforts onto the communications backbones and departmental LANs as well as engineer LAN technical solutions and author's implementation plans. Technicians manage the operational effectiveness of present hardware, communications software, and WAN and LAN configurations within USMEPCOM.

d. Establishing and maintaining configuration management processes; testing new devices and network-related software prior to installation on the network; providing connection control and approval; network administration policy and guidance; architecture and standards policy; and other associated issues pertaining to the backbone.

5-8. Network documentation

J-6/MIT-NSB will be responsible for the overall network documentation. MEPS ITSs are required to maintain a Network Documentation folder IAW guidance prescribed in [AR 25-400-2](#) (The Army Records Information Management System (ARIMS)). Responsibilities will include, but is not limited to:

a. Network map showing key network devices (router, hubs, and circuits). The map will also contain other devices to provide additional information (PCs, printers, USMIRS devices, Computer Adaptive Testing-Armed Services Vocational Aptitude Battery (CAT-ASVAB), etc.)

b. Internet protocol (IP) addresses used in MEPS (in spreadsheet format) Column 1 is the device name and Column 2 is the fourth set of numbers (octet) in the device's IP address. If desired, other columns may be added to provide additional information.

c. Information Sheets section. USMEPCOM instructions or suggestions relating to network, PC, software, and hardware are stored. Additional categories may be saved here, if desired.

5-9. End-user network operations on the Local Area Network/Wide Area Network

End-users are connected to network file servers via the LAN/WAN as a part of the J-6/MIT-NSB network backbone that can to some extent appear to be autonomous. However, the more the users and WAN require support while using the network, the less autonomy they will have. Even with a total autonomy it will need to comply with universal standards for hardware and software utilization. A user connected to the network for e-mail, USMIRS, CAT-ASVAB, or world-wide Web (WWW) access will comply with the standards established by J-6/MIT-NSB. USMEPCOM is responsible for complying with certain DoD practices. Responsibility for assuring these practices are followed by the end-user is delegated to the designated ITS.

5-10. Networks, computer, and peripheral maintenance

J-6/MIT-NSB will be responsible for network, computer, and peripheral maintenance. Identification of maintenance issues is a shared responsibility of every USMEPCOM employee. Each USMEPCOM employee who identifies a maintenance issue should report it to the J-6/MIT Help Desk.

5-11. Equipment warranties

J-6/MIT-NSB maintains warranty and maintenance contracts to repair or replace certain network equipment, computers, and peripherals, where cost effective or mission critical. ITSs or other personnel in MEPSs, sectors, or HQ USMEPCOM are not authorized to invalidate those warranties or maintenance contracts on equipment. Any questions on warranties or maintenance should be directed to J-6/MIT-NSB.

5-12. Service outages

Periodic maintenance, upgrades, and services to equipment may be required. Scheduled outages will be announced in advance and scheduled as much as possible on weekends and evenings. J-6/MIT-NSB will attempt to minimize unscheduled network equipment outages.

5-13. Access to USMEPCOM networks, devices, and services

Each user requiring access to the network will have a signed [DD Form 2875](#) on file, to include liaisons in MEPS, before they are granted access to any portion of the network. Each MEPS and sector will maintain access forms on personnel in the MEPS including liaisons IAW guidance prescribed in [AR 25-400-2](#). J-6/MIT-NSB will maintain access forms for USMEPCOM. Each year this form will be reviewed and updated. J-6/MIT-NSB is responsible for the management of passwords, logins, and e-mail accounts IAW paragraph 2-8(14) and [AR 25-2](#).

5-14. User and Information Technology Specialist's responsibilities

A user connected to the network for e-mail, USMIRS, CAT-ASVAB, or WWW access will comply with the standards established by the DOD regulations listed in appendix A. HQ USMEPCOM, sectors, and MEPSs are responsible for complying with practices IAW established regulations. Sector and MEPS commanders will delegate the ITS to assure these practices are followed.

5-15. USMEPCOM e-mail system

This is the only official e-mail system allowed at USMEPCOM. The e-mail system allows electronic transfer of information, including files and messages, between internal command users and external customers of the command.

a. The e-mail system provides rapid delivery of software updates. When e-mail is transferred between USMEPCOM personnel, it is transmitted over the USMEPCOM private LAN/WAN, including the RSN.

b. E-mail transferred between USMEPCOM personnel and external customers is transmitted over the DoD Non-secure Internet Protocol Router Network (NIPRNET) and/or commercial Internet.

NOTE: The USMEPCOM e-mail system is only cleared for unclassified information. Users will not transmit classified information over the USMEPCOM e-mail system. In addition, the ONLY OFFICIAL e-mail system and method of transferring e-mail is through the USMEPCOM provided e-mail system.

5-16. Nongovernmental e-mail system

E-mail services such as "Hotmail," "Yahoo mail," "Excite mail," "AOL," etc., are not official e-mail. These e-mail services are not approved methods for transmitting work-related e-mail and will not be supported. These systems are outside the control of HQ USMEPCOM, sectors, and MEPSs personnel and security measures which do not provide proper security, virus scanning and backup capabilities.

5-17. Assistance and problem resolution

HQ USMEPCOM, sectors, and MEPSs personnel will contact their local SA/ITS for any computer or network assistance or problems. The SA/ITS will report the problem to the J-6/MIT Help Desk for tracking and resolution. Service liaisons having trouble with USMEPCOM equipment or network issues should contact the MEPS ITS. Service liaisons having trouble with their own service equipment should contact their recruiting service for instructions.

5-18. Other networks

J-6/MIT-NSB is responsible for coordinating access and providing appropriate security for other networks including access to the Internet and USMEPCOM intranet and extranets.

5-19. Internet access and monitoring

J-6/MIT-NSB is responsible for coordinating and monitoring access to the Internet including access to the military portion known as the NIPRNET. J-6/MIT-IAO may gather information IAW [AR 25-2](#), if an employee's usage of the Internet is questioned. USMEPCOM, sectors, or MEPSs commanders, directors/special staff officer, or SA/ITS, if directed, may request a review of the log files. The request will include the IP address to be reviewed and the date and times accessed. A report will be returned to the supervisor that includes a summary of sites visited during the review period along with access times and any recommendations. Monitoring and privacy rights are an evolving process. J-6/MIT-IAO will direct requests for monitoring to the Staff Judge Advocate/MJA for review. Local supervisors are responsible to ensure Internet policies are understood and followed. USMEPCOM personnel who access an Internet site are responsible for their own actions.

5-20. Intranets and extranets

J-6/MIT-NSB is responsible for maintaining Web servers that are accessed across the Internet. [SPEAR](#) is the current USMEPCOM intranet site. J-6/MIT-NSB is responsible for USMEPCOM extranets.

5-21. External accesses to USMEPCOM network

J-6/MIT-NSB is responsible for providing remote access to the USMEPCOM networks for authorized personnel. Unauthorized access will be reported as a security violation to the USMEPCOM IAM.

Chapter 6 Help Desk

6-1. Help Desk

Provides a single POC for all J-6/MIT supported services and equipment within USMEPCOM. This encompasses all technical assistance and problem resolution for systems and software applications, including service interfaces, computers, e-mail, Web, LAN, WAN and components of the communications infrastructure. J-6/MIT Help Desk processes all requests received from MEPSs, sectors, and HQ USMEPCOM and facilitates J-6/MIT Help Desk problem determination and resolution.

6-2. Help Desk operations

J-6/MIT Help Desk operational hours and procedures are based on USMEPCOM priorities and resources. Requirements for additional support should be e-mailed to J-6/MIT-Help Desk (J-6/MIT-CSB) at least one week in advance. Current hours of operation are 0001 – 2300, Monday – Saturday excluding Federal holidays.

a. J-6/MIT Help Desk is the central POC to facilitate problem, determination, and resolution. Provide general systems information, and respond to customer requests.

b. The following problems or inquiries will be resolved directly by J-6/MIT Help Desk personnel, if possible, or escalated to the next higher level of support.

(1) Hardware maintenance will be called into the appropriate vendor by J-6/MIT Help Desk personnel after a trouble ticket has been submitted. Any time a piece of equipment is moved or replaced J-8/MRM-AD-LB coordination is required.

(2) Technical assistance for J-6/MIT systems/applications (e.g., USMIRS, CAT-ASVAB, Personal Digital Assistant (PDAs) used to generate ASVAB QuickScores, and Remote Centralized Testing Scoring (R-CTS))”.

(3) USMIRS software, Microsoft system software, command unique software, service interface and database technical problems will be troubleshot and resolved by J-6/MIT Help Desk technicians. Problems determined to be beyond the scope of capabilities of the J-6/MIT Help Desk technicians will be escalated to Level III technicians for resolution.

(4) E-mail issues.

(5) RSN outages reported and status tracked with United States Army Recruiting Command (USAREC).

(6) COTS application loading and/or operation issues.

(7) Functional or policy inquiries will be directed to J-3/Operations Center “MOC” (J-3/MOP-CO).

c. The J-6/MIT Help Desk hours of operations. These hours may be adjusted to accommodate exceptional circumstances or to facilitate changes in support requirements.

(1) The J-6/MIT Help Desk is staffed from 0500 - 2100 Monday-Friday.

(2) Saturday processing coverage is from 0500 - 2000.

[TOC](#)

(3) USMEPCOM functional experts are available ON CALL, for software problem resolution and additional assistance on mission days and Saturday processing.

6-3. Requests for assistance and reporting problems

The ITS will notify J-6/MIT Help Desk personnel by phone if the issue is critical (i.e., server, router, Enterprise switch, LAN, or WAN not operational) for completion of mission. J-6/MIT Help Desk management system is used to log all entries and provide reports.

6-4. Managing assistance and problems

Each ITS will assist the J-6/MIT Help Desk personnel in resolving problems and notify the J-6/MIT Help Desk as soon as possible after an issue has been resolved. Notification will be done not later than the next duty day. Failure to notify the J-6/MIT Help Desk provides inaccurate information to decision makers and wastes USMEPCOM resources.

Chapter 7 Software Management

7-1. Command software management program

The Management Reform Act mandates that Federal Agencies inventory their computer equipment, hardware and software, and maintain an inventory of excess and surplus assets.

7-2. Command Software Manager

J-6/MIT-CIO designates the command software manager to implement the USMEPCOM Software Management Program. The command software manager serves as the focal point for USMEPCOM in all matters pertaining to licensing, copyright, and management of software.

7-3. Software residing on USMEPCOM PCs

Software whether COTS, GOTS, USMEPCOM-unique applications or programs, residing on USMEPCOM-owned PC's require an approved IMENS submission prior to software installation. USMEPCOM-owned PCs will be subject to annual audits. On an annual basis the sectors and MEPSs will forward all audit reports to HQ USMEPCOM, ATTN: J-6/MIT-PPB, 2834 Green Bay Road, North Chicago, IL 60064-3094. The contractor personnel employed by USMEPCOM may install or retain on government computers (both PCs and laptops) software purchased or supplied by the sponsor company only after obtaining written permission from J-6/MIT. In the situation of software being mailed or delivered to USMEPCOM in the contractor's name, J-6/MIT-PPB will be advised prior to delivery.

7-4. Screensavers

Screensaver programs other than those that come with the computer's operating system, (currently Windows XP) are not authorized. IMENS submissions for additional screensaver programs will not be approved.

7-5. Internet downloads

Critical updates of command approved programs can be downloaded only by authorized ITSs, as required, with proper notification/approval of the IMENS process and command network manager. IMENS authorization is required for downloading of any program packages prior to the download. Downloads of documents, forms and/or briefings are authorized if they are directly related to the job and do not exceed 2 (megabytes) MB in size.

7-6. Site licensing

Site licensing for COTS software will be used in all areas of USMEPCOM as directed by [AR 25-1](#).

7-7. Original commercial-off-the-shelf software media

The command software manager, software technician, or MEPS or sector ITS will secure all original software media.

7-8. End-user training

J-6/MIT-ISS, in coordination with the J-1/Human Resources Directorate-Training Development Division (J-1/MHR-TR), is responsible for coordinating and providing initial PC training for end-users. Users should take the initiative to go through the tutorials provided with the PC, as well as COTS software manuals. Before using J-6/MIT hardware, personnel will receive introductory training to ensure users can properly and safely operate their system. The MEPS and sectors ITS will provide initial introductory PC training at their level. Follow-up training will be accomplished as priorities and requirements in the command change.

Chapter 8 Telephones

8-1. Telecommunications specialist

The telecommunications specialists are assigned the additional responsibility of all communications services for USMEPCOM, all subordinate activities and locations. J-6/MIT-PPB and J-6/MIT-NSB are responsible for processing all requests for local communication services submitted to the Base Communications Office, Great Lakes Naval Training Center, Great Lakes, IL.

8-2. Telecommunications Control Officer

Sector or MEPS commanders will designate in writing a telecommunications control officer (TCCO). A copy of the appointment document will be forwarded to J-6/MIT-NSB no later than 7 working days following the appointment. The TCCO is responsible for the administration of the telecommunications program within sectors and MEPSs.

8-3. Telephone controls

The use of DoD telephone systems will be limited to the conduct of official business. Official business calls will include emergency calls and calls that are necessary in the interest of the Government. Commanders are responsible for proper use of official telephone service.

8-4. Request for telecommunications services

Requests for telecommunications services and facsimile (FAX) machines will be processed through the local TCCO. The TCCO in turn will submit their requirements through their respective sector to J-6/MIT-Help Desk at USMEPCOM IAW instructions located in appendix E (Format to request telecommunications service). IMENS requests are only required for new fax machines. The replacement of defective FAX equipment will be handled through the J-6/MIT Help Desk. In addition, MEPS TCCOs are authorized to contact the local telephone company, vendor, or telecommunications representative to obtain cost estimates for required telephone equipment and/or services.

8-5. Telephone service ordering office

a. Telecommunications Ordering Officers (TCOO) assigned to J-6/MIT-NSB are authorized to issue the [DD Form 1367](#) (Commercial Communications Work Order) and requests for Communications Service Authorizations (CSAs) for HQ USMEPCOM, sectors, and MEPSs. TCOOs are appointed and authorized to act as telecommunications coordinators under the technical supervision of the Chief, Office of Acquisition and HQ Network Enterprise Technology Command (NETCOM), Fort Huachuca, AZ. Telecommunication coordinators prepare the appropriate portions of [DD Form 1367](#).

b. The USMEPCOM appointed TCOOs are responsible for review of existing CSAs on a continuing basis to ensure changes (e.g., prices, addresses, etc.) requiring a modification are promptly reported to HQ NETCOM, Acquisition Office, Fort Huachuca, AZ. This also includes the yearly options for review during the life of the existing contract which is normally 5 years total.

8-6. Government-owned telephone equipment

Government-owned digital telephone systems installed at a sector or MEPS, consist of a digital main central processing unit, voicemail, digital and analog telephone instruments, an uninterruptible power supply and necessary interconnecting horizontal and vertical cabling.

8-7. Verification and certification of communications bills

The purpose of verification is to collect payment from those personnel making unauthorized calls. Each MEPS must verify and certify all telephone bills. To ensure timely payment of phone bills, verification

and certification should be completed as soon as possible of receipt but not later than 5 days after receipt. The MEPS are authorized to pay their local telephone invoices using the Government charge card. These bills are kept for a two year period, IAW guidance prescribed in [AR 25-400-2](#), for review by the Inspector General (IG) at the MEPS.

8-8. Reimbursement for official telephone calls

Charges for official local and long distance telephone calls for USMEPCOM personnel (military and civilian) are reimbursable. This includes personnel performing temporary duty in a travel status and personnel performing official duties away from normal duty within local travel area. Use of personal telephones, including cellular telephones, will be held to a minimum.

8-9. Telephone toll credit cards

MEPS commanders will be aware of the abuse and misuse that normally accompany the use of telephone credit cards. Therefore, the use of these credit cards will be limited to mission essential business only. Telephone credit cards are authorized for use in USMEPCOM on an exception basis. Credit card issuance will be limited to USMEPCOM command group and directors/special staff officers, sector and MEPS commanders, and other personnel, as designated and justified by command group, directors/special staff officers and commanders. Telephone credit cards are provided through MCI (Verizon Business long distance provider) or other competitively awarded government contract through GSA.

8-10. Collect calls

Station-to-station collect calls may be accepted. Person-to-person collect calls are prohibited. Collect calls are an important tool that may be both mission responsive and cost effective. However, each call does incur a surcharge that varies in cost depending on the time and distance called. These calls should be limited.

8-11. Facsimile equipment

USMEPCOM personnel will be aware of the high cost of record communications machines over any media. Fax use will be restricted to those circumstances that require a copy of any original document be received within a short time frame. Faxes will not be used as a routine means of replying to suspense but will be considered instead of courier service or express mail. Fax machines are provided as a means to satisfy the requirement for electrical transmission of time sensitive documents.

8-12. Digital sender equipment

HQ USMEPCOM, sectors, and MEPSs have digital sender equipment capability which allows documents to be sent via the network instead of faxing documents. This is quicker and much more cost effective and should be used to the maximum extent possible.

8-13. Headquarters public branch exchange phone systems

All additions, changes, and deletions to HQ USMEPCOM, sectors, and MEPSs public branch exchange (PBX) telephone systems will be submitted to J-6/MIT Help Desk either by generating an in-house help ticket or by contacting extension 7800. This should be done at least 5 working days prior to the service implementation date, especially for the assignment of new personnel.

8-14. Wireless communications devices

Any authorized cellular telephones will be used only when conventional telephones are not available, or use of the cellular telephone is more cost effective for the Government (i.e., local toll areas are already included in the cellular contract). Cellular telephones are not to be considered convenience items. Long distance calls outside the local service provider's coverage area will be kept to a minimum, as roaming charges and long distance charges can be costly. These additional charges show up on a separate telephone bill, which is currently paid by the headquarters. Those having individual coverage issues with

[TOC](#)

contracts will be handled on a case by case basis to establish service along with payment of the yearly service. These are handled by J-8/MRM-AD-LB (Logistics Branch) in coordination with J-6/MIT-PPB and J-6/MIT-NSB. The use of a J-6/MIT calling card or its number is a much more cost effective method and saves the command dollars.

8-15. Pagers

The only time a pager will be obtained is on a case-by-case basis for special needs employees. This action needs to be coordinated with Equal Employment Opportunity/Equal Opportunity (MEEEO-EO) office.

Chapter 9

Enterprise Data Center (EDC)

9-1. Overview

The EDC is available to support HQ USMEPCOM, sectors, MEPSs, and SSS processing and system requirements.

9-2. Operating hours and system availability

The EDC is staffed 0001 hours Monday – 2300 hours Saturday, excluding Federal holidays. Most functions are accessible 24x7. Changes to hours of operation will be requested through the Director, J-6/MIT. Occasionally, it is necessary to bring critical systems down or there is an unexpected outage. At these times, appropriate personnel are notified prior to any scheduled outage, or immediately for any unexpected outage.

9-3. Computer room access

The EDC is a "LIMITED ACCESS RESTRICTED AREA." Access is granted only to personnel with a valid requirement and proper security credentials. The computer room is operated as a "closed shop" (i.e., personnel not directly involved in computer operations will obtain permission to gain access). Personnel requiring access will need to be escorted at all times while in the EDC. Security of the Enterprise Server is discussed in chapter 1 (Responsibilities).

9-4. Technical support

Technical support is provided for Enterprise Server application programmers and users.

9-5. EDC telecommunications services

Enterprise Network Connectivity services will be routed through J-6/MIT-NSB.

9-6. Billing and accounting (chargeback system)

Users are charged IAW the MOU between DOD and the SSS.

9-7. Application approval

HQ USMEPCOM, sectors, and MEPSs requests for approval of new application systems will be submitted in writing by functional proponents to J-6/MIT-SSB. SSS Operations manager, will submit SSS requests for approval of new application systems in writing to J-6/MIT-SSB. They will be approved before being installed on the Enterprise Server.

9-8. Users Working Group

There is a quarterly work group between USMEPCOM and SSS.

9-9. Requests for special print forms

Requests to build special form definitions for the high-speed printer will be submitted in writing to J-6/MIT-SSB.

9-10. Backup and recovery

J-6/MIT-CSB provides for backup and off-site storage and subsequent retrieval of the Enterprise Server operating system and USMEPCOM application system data. This includes pulling and transporting tapes to and from off-site storage. The backup tapes are retrieved on schedule or as required to reconstruct data lost through hardware and/or software malfunctions. At all times, tapes are maintained offsite for reconstruction of the Enterprise Server operating environment in the event of a major catastrophe. J-6/MIT-CSB does not provide backup and storage for SSS.

[TOC](#)

9-11. Enterprise Server continuity of operations plan

J-6/MIT-PPB maintains an Enterprise Server Continuity of Operations Plan (COOP) to ensure a viable COOP site is available with a properly configured Automated Data Processing (ADP) system and appropriate environment and security for processing the USMEPCOM and SSS critical workload.

Chapter 10 Web Infrastructure

10-1. Overview

J-6/MIT-SDB is responsible for the command's Internet and intranet site design, Web site traffic management/analysis, and Web site security. Requests for additions and changes for the Internet site will be submitted to Public Affairs Office (MPA) following procedures outlined on the Web page. Requests for additions and changes to the intranet site are performed by HQ USMEPCOM directorate/special staff office content managers, following procedures outlined on [SPEAR](#).

10-2. USMEPCOM Internet Web site

The goal of the Internet site is to provide outside agencies and the public with basic USMEPCOM information. MPA is the proponent and releasing authority for the site. J-6/MIT-SDB is the functional manager and responsible for creating, maintaining, securing, and monitoring the Web site.

10-3. USMEPCOM intranet Web site

[SPEAR](#) is a secure private intranet site provided to USMEPCOM employees. [SPEAR](#) provides USMEPCOM specific information such as publications, calendars, budget information, and briefings, and is intended to help fill the requirement for distributing material to sectors and MEPS, and reduce the requirement for printed information and its physical reproduction and distribution costs. USMEPCOM Directorate Content Management POC is the proponent for content of their individual directorate pages. J-6/MIT-SDB is the functional proponent for the intranet site and is responsible for creating, maintaining, securing, and monitoring the Web site.

10-4. USMEPCOM Internet item implementation process

Request for major changes or additions to the current Web site are submitted via Web change request. The Web Steering Committee analyzes the request and identifies a need. J-6/MIT-SDB verifies the technical feasibility and MPA gives approval/disapproval of idea for publication worthiness.

10-5. USMEPCOM network intranet implementation process

Request for content changes are submitted to the individual directorate POC who is responsible for ensuring the director or deputy director approves the content before they post the information onto their directorate's individual pages.

10-6. Web technical design, development, security, operations, and maintenance

J-6/MIT-SDB is responsible for all Web infrastructure, technical design, development, security, operations and system maintenance.

Chapter 11 Copier Usage

11-1. Printing and self-service copying

a. The USMEPCOM, command printing manager serves as the POC for all matters relating to USMEPCOM copiers and printing.

b. Sectors and MEPSs are responsible for ensuring compliance with policies concerning printing, duplication, and self-service copiers. MEPS commanders will implement an aggressive program for conserving resources and will ensure adherence to the policies outlined in [AR 25-30](#), chapter 7. All Government employees have the duty to protect and conserve government property and not use such property, or allow its use, for other than authorized purposes.

c. All official letterhead stationery will bear the DoD seal and will be computer generated.

11-2. Self-service copiers – new requirements

a. The ITS at the requesting MEPS will fill out an IMENS through the IMENS (MKS) system for new copier requirements.

b. The command copier manager (CCM) will conduct a cost benefit analysis, as required by [AR 25-30](#), and attach to the IMENS.

11-3. Self-service copiers – replacement of cost-per-copy/flat rate copiers

a. Those MEPS who are under a cost-per-copy or flat rate program will budget yearly for their copier support.

b. Cost-per-copy copiers are replaced when the contract terminates. The CCM will notify the MEPS when the copier contract is about to run out and provide information on new copiers and pricing.

11-4. Self-service copiers – replacement of purchased copiers

a. Life-cycle replacement. The CCM will budget for purchased copiers and initiate action to replace the copiers at the MEPS based on a 5-year life-cycle.

b. Replacement prior to end of life-cycle. Replacement of owned copiers prior to completing the end of their life-cycle (5 years) will be considered on a case-by-case basis.

c. Key operators

(1) Each office which has a copier installed in or near their area will designate a primary and alternate key operator. Key operators will assist with paper jams, ensure copier paper and supplies are available, and report malfunctions to the copier manager. Copier managers will ensure key operators are trained in assisting with above duties. A sign identifying key operators will be posted near copiers.

(2) Copier managers and key operators will ensure that only products (i.e., toner and developer) authorized by the manufacture or General Services Administration (GSA) approved are used.

11-5. Copier reports

a. [USMEPCOM Form 25-3-3-E](#) (Quarterly Copier Cost and Production Report) will be used for submitting quarterly copier reports. Instructions for completing the report are on the form.

b. The USMEPCOM CCM will maintain the current and official copier inventory list for all Government-owned or leased self-service copiers.

11-6. Liaison support

Under the guidance of [AR 601-270](#) (Military Entrance Processing Station (MEPS)), USMEPCOM is responsible for providing copier support to all Service liaisons and guidance counselors physically located at each MEPS.

Appendix A References

Section I

Required Publications

(The publications needed to comply with this regulation.)

AR 25-1

Army Knowledge Management and Information Technology. Cited in paragraphs 1-1; 1-5a, b, and d; 1-6a; 4-9; and 7-6.

(Internet users: http://www.army.mil/usapa/epubs/pdf/r25_1.pdf)

AR 25-2

Information Assurance. Cited in paragraphs 1-4i(1), 1-4l(1), 2-1, 2-2j, 2-8, 5-13, and 5-19.

(Internet users: http://www.army.mil/usapa/epubs/pdf/r25_2.pdf)

AR 25-30

The Army Publishing Program. Cited in paragraphs 11-1(b) and 11-2b.

(Internet users: http://www.apd.army.mil/pdf/r25_30.pdf)

AR 25-400-2

The Army Records Information Management System (ARIMS). Cited in paragraphs 1-4k(2), 5-8, 5-13, and 8-7.

(Internet users: http://www.army.mil/usapa/epubs/pdf/r25_400_2.pdf)

AR 190-13

The Army Physical Security Program. Cited in paragraph 1-4i(3).

(Internet users: http://www.army.mil/usapa/epubs/pdf/r190_13.pdf)

AR 190-51

Security of Unclassified Army Property (Sensitive and Nonsensitive). Cited in paragraph 1-4i(3).

(Internet users: http://www.army.mil/usapa/epubs/pdf/r190_51.pdf)

AR 340-21

The Army Privacy Program. Cited in paragraph 1-4i(2).

(Internet users: http://www.army.mil/usapa/epubs/pdf/r340_21.pdf)

AR 601-270

Military Entrance Processing Station (MEPS). Cited in paragraph 11-6.

(Internet users: http://www.apd.army.mil/pdf/r601_270.pdf)

DOD Directive 8320.2

Data Sharing in a Net-Centric Department of Defense. Cited in paragraph 4-5.

(Internet users: http://www.dtic.mil/whs/directives/corres/pdf/d83202_120204/d83202p.pdf)

DOD Directive 8500.01E

Information Assurance (IA). Cited in paragraph 2-1.

(Internet users: http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf)

DOD Directive 8570.1

Information Assurance Training Certification. Cited in paragraph 1-4l(2).

(Internet users: http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf)

DOD Regulation 5500.7

The Joint Ethics Regulation (JER). Cited in paragraph 2-8g.

(Internet users: http://www.defenselink.mil/dodgc/defense_ethics/ethics_regulation/)

Homeland Security Directive 12

Policy for a Common Identification Standard for Federal Employees and Contractors. Cited in paragraph 1-4c(3).

(Internet users: <http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>)

NIST Special Publication 800-12. Cited in paragraph 2-1.

An Introduction to Computer Security: The NIST Handbook.

(Internet users: <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>)

OMB Circular A-130. Cited in paragraph 2-1.

Management of Federal Information Resources.

(Internet users: <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>)

Title 17, United States Code

Copyrights. Cited in paragraph 2-1.

(Internet users: <http://www.access.gpo.gov/uscode/title17/title17.html>)

Title 18, United States Code

Crimes and Procedure. Cited in paragraph 2-1.

(Internet users: <http://www.access.gpo.gov/uscode/title18/title18.html>)

USMEPCOM Regulation 710-2

Requisition and Issue of Supplies and Equipment. Cited in paragraph 1-4i(4).

(Internet users: <http://www.mepcom.army.mil/publications/pdf/regs/r-0710-002.pdf>)

Section II***Related Publications***

(These publications are a source of additional information. Users may read them to better understand the subject, but do not have to read them to comply with this regulation.)

AR 25-11

Record Communications and the Privacy Communications System

(Internet users: http://www.army.mil/usapa/epubs/pdf/r25_11.pdf)

DFAR 237.74

Defense Federal Acquisition Regulation

(Internet users: <http://www.acq.osd.mil/dpap/dars/dfars/pdf/r20060123/tocpdf.htm>)

DOD Directive 8000.1

Management of DOD Information Resources and Information Technology

(Internet users: http://www.dtic.mil/whs/directives/corres/pdf/d80001wch1_022702/d80001p.pdf)

Public Law 104-106. Cited in paragraph 2-1
Clingler-Cohen Act
(Internet users: <http://knet.ndu.edu/docs/policy/ITMRA96.pdf>)

USMEPCOM Regulation 10-1
United States Military Entrance Processing Command
(Internet users: <http://www.mepcom.army.mil/publications/pdf/regs/r-0010-001.pdf>)

Section III

Prescribed Publications

(Publications prescribed by this regulation.)

None

Section IV

Required Forms

(The forms needed to comply with this regulation.)

DA Form 11-2
Management Control Evaluation Certification Statement. Cited in paragraphs B-3 and B-7.

DD Form 250
Material Inspection and Receiving Report. Cited in paragraphs 3-7c.
(Internet users: <http://www.dscp.dla.mil/subs/support/qapubs/sub4155/250.pdf>)

DD Form 1367
Commercial Communication Work Order. Cited in paragraph 8-5a.
(Internet users: <http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd1367.pdf>)

DD Form 2875
System Authorization *Access Request*. Cited in paragraphs 3-9 and 6-14.
(Internet users: http://eda.cols.disa.mil/users_guide/userGuidance/attachments/formDD2875/DD2875.pdf)

Section V

Prescribed Forms

(The forms prescribed by this regulation)

USMEPCOM Form 25-3-3-E
Quarterly Copier Cost and Production Report. Cited in paragraph 11-5a.
(Internet users: <http://www.mepcom.army.mil/pubs/pdf/forms/f-0025-003-03.pdf>)

USMEPCOM Form 25-3-4-E
USMEPCOM Acceptable Use Policy. Cited in paragraph 2-8e.
(Internet users: (<http://www.mepcom.army.mil/publications/pdf/forms/f-0025-003-04.pdf>))

USMEPCOM Form 25-3-5-E
Data-At-Risk. Cited in paragraph 2-7t.
(Internet users: <http://www.mepcom.army.mil/publication/pdf/forms/f-0025-003-05.pdf>)

USMEPCOM Form 25-3-6-E
DAR Official Travel Authorization Card. Cited in paragraph 2-7t.
(Internet users: <http://www.mepcom.army.mil/publications/pdf/forms/f-0025-003-06.pdf>)

Appendix B

Management Control Evaluation Checklist - Managing Information Technology Resources

B-1. Function

The function covered by this checklist is Managing Information Technology Resources.

B-2. Purpose

The purpose of this checklist is to assist commanders and managers in evaluating the state of management controls in this program (or functional) area.

B-3. Instructions

Answers must be based on actual testing of key management controls (document analysis, direct observation, sampling, simulation, etc.). Explain answers indicating deficiencies and take necessary corrective actions. Formally evaluate these controls at least once every 5 years. Certify that evaluations have been accomplished by completing [DA Form 11-2](#) (Internal Control Evaluation Certification).

B-4. Test questions

a. Automation resource control and accountability. The purpose of this objective is to ensure prescribed policies, procedures, and responsibilities contained in regulations are followed to protect and account for Government property.

b. Data processing resources. The purpose of this objective is to ensure hardware and software obtained beyond the command standard is properly requested and authorized.

(1) Does each software package have an approved Information Mission Element Need Statement (IMENS) that was processed through the MKS system? (par. 7-3)

(2) Does each piece of accountable ADP hardware have an approved IMENS processed through MKS system? (par. 3-6a)

c. Software management. The purpose of this objective is to ensure that prescribed policies, procedures, and responsibilities contained in regulations are followed to protect and account for software:

(1) Is all commercial-off-the-shelf (COTS) software accounted for by a signed hand receipt? (USMEPCOM Reg 710-2, ch. 7)

(2) Are the original media (CD-ROM and/or diskettes) and manuals secured by the command software manager? (par. 7-7)

(3) Has the command software manager conducted the annual audit of the non-MIRS PC hard drives to ensure no copyright violations exist? (par. 7-2)

(4) Does the command software manager and the ITS keep a current copy of the Command Approved Software List and the USMEPCOM approved COTS List (the approved IMENS)? (par. 3-7)

(5) Does the command software manager have the correct and updated command approved software list that corresponds to the IMENS? (par. 3-7)

(6) Has a back-up for the ITS been assigned? (par. 1-4j(7))

[TOC](#)

d. Network management. The purpose of this objective is to ensure that prescribed policies, procedures, and responsibilities contained in regulations are followed to protect and account for the network:

(1) Is there an up-to-date Network Documentation folder? (par. 5-8)

(2) Are all network connected devices authorized for use on a USMEPCOM network? (par. 5-4)

e. Telecommunications Management. The objective of telecommunications management is to provide communications capability to accomplish the mission while utilizing limited budgetary resource in an intelligent manner:

(1) Is a TCCO appointed by an informal memorandum? (par. 8-2)

(2) Is the TCCO aware of his or her duties and responsibilities? (par. 8-2)

(3) Are the telephone lines and instruments in accordance with the basis of issue authorization? (par. D-2)

(4) Are personnel aware of restrictions regarding making personal telephone calls using government telephones? (par. 8-3)

(5) Are persons making unauthorized long distance calls paying for them? (par. 8-7)

(6) Are copies of each certified telephone bill and related correspondence retained for a minimum of a year by the TCCO? (par. 8-7)

f. Information Assurance Office. The purpose of this objective is to ensure prescribed policies, procedures, and responsibilities contained in the management control checklist in AR 25-2 (Information Assurance) are followed to protect network security.

B-5. Supersession

This checklist supersedes appendix B of USMEPCOM Regulation 25-3, 10 August 1992.

B-6. Comments

Submit comments on this inspection program through your sector to HQ USMEPCOM, J-6/MIT.

B-7. DA Form 11-2 (Internal Control Evaluation Certification)

Use [DA Form 11-2](#) to document management control evaluations.

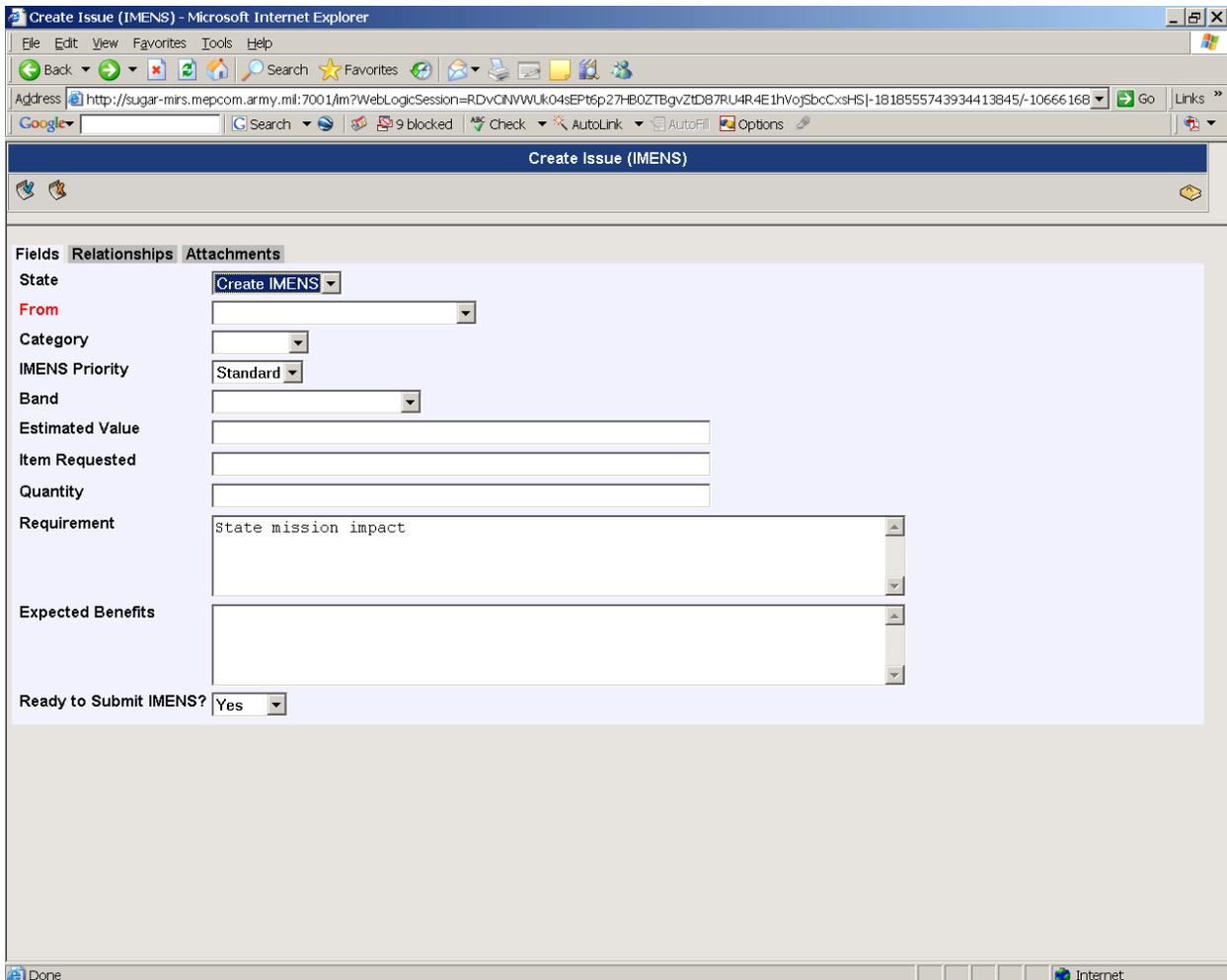
Appendix C Instructions for the Completion of an Information Mission Elements Need Statement (IMENS)

The IMENS provides the vehicle for individuals to submit requests for J-6/MIT resources to meet J-6/MIT requirements. Requesters submit electronically IMENS to ensure the stated functional requirements are valid and conform to USMEPCOM policy. Requesters must complete the IMENS for all hardware and software requirements, regardless of cost or urgency. Procurement actions will not start until the appropriate authority approves the IMENS.

Automated IMENS:

[Automated IMENS Guide Book 1.1.pdf](#)

IMENS must be submitted electronically. The requestor will complete section 1.



Appendix D

Telephone Service Basis of Issue

D-1. General

The following telephone service basis of issue (BOI) will be applied to requests for telephone service to ensure authorized levels of telephone lines and instruments are within established guidelines. Requests for service exceeding the BOI will be handled on a case-by-case basis. Such requests must include detailed justification and be submitted through the sector TCCO to J-6/MIT Help Desk. A copy of all approved exceptions to the BOI will be maintained at the sector and applicable MEPS ([AR 25-1](#)).

D-2. Authorization

Authorization for telephone service is based upon the number of personnel authorized and assigned as listed in the tables of distribution and allowances (TDA). Telephone service for personnel assigned for periods of less than 6 months is not authorized.

- a. Telephone service for USMEPCOM, sectors, and MEPSs will be determined by J-6/MIT-NSB.
- b. MEPS will have no more than one main line per four authorized and assigned personnel but where possible, only one main number with a hunt group will be installed with options off the auto-attend for different sections as well as extensions.
- c. In addition to the above, the following telephone services are authorized:
 - (1) A commercial or GSA mainline for each fax machine.
 - (2) A dedicated line for each education services specialist (ESS) to be associated with the 1-800 ASVAB number.
 - (3) A dedicated modem line for the support group supervisor (SGS).
 - (4) One conference room telephone is authorized for use by the MEPS connected to an extension off the main telephone system and not a separate line.
- d. Special features and service limitations.
 - (1) Installation of telephone answering devices will be limited to those authorized by proper documents. Answering devices are funded for and obtained through logistics channels. Communication funds will be used only for installation of a telephone jack required to connect the answering device to a telephone line.
 - (2) It is recommended the majority of telephone lines servicing the activity be installed on a rotary hunt basis, utilizing a single main telephone number.

**Appendix E
Format to Request Telecommunications Service**

(Appropriate Letterhead)

(OFFICE SYMBOL) (ARIMS NUMBER) (Month/day/year)

MEMORANDUM THRU (Appropriate sector)

FOR Director, J-6/MIT Plans and Policy Division, North Chicago, Illinois

SUBJECT: Request for (Commercial or GSA) Telephone Service (Installation, Relocation, Removal, or Exception to Policy).

IAW USMEPCOM Regulation 25-3, the following information is submitted for telephone service as indicated:

- a. Present address. (Used when relocation/removal is requested).
- b. Proposed installation address. (Name of activity, building, room, street, city, state, county, and zip code where service is desired.) (NOTE: Identification of the county involved is extremely important.)
- c. Activity complement. (Total number of personnel authorized by TDA and assigned at the MEPS where service is desired.) (Do not include Army guidance counselors or liaison personnel.)
- d. Addition/relocation/deletion desire. (Indicate only the specified change[s] desired, not the total of existing and desired services.) Specifically, the type of service (commercial or GSA) and the number of main lines.

Examples:

- (1) Commercial lines required - i.e., one, two, etc.
- (2) Commercial lines to be removed - (indicate telephone number[s]).
- (3) Commercial lines to be relocated from present to new address.

NOTE: The following information is required when requesting a jack for an answering device: type of jack (e.g., RJ11C, RJ13C), model, Federal Communications Commission registration numbers, and ringer equivalency.

- e. Justification. (See appendix F (Telephone service basis of issue) for authorization guidelines.) Detailed justification is required for service to be installed as in d, above. The phrase "mission essential" is not sufficient.
- f. Date desired. (Date specified will allow sufficient time [60 days] for staffing the request. Urgent requirements are not to be routinely submitted as a substitute for proper planning.)
- g. Contact individual. (Rank, name, address and telephone number.)
- h. Servicing telephone company. (Name and address of company.)
- i. Billing address. (Address of MEPS TCCO to which bills are to be sent.)
- j. Remarks. (Other information that will assist in the procurement of the requested services.)

FOR THE COMMANDER:

(SIGNATURE BLOCK)

Glossary

Section I

Abbreviations

ADP

automated data processing

AR

Army regulation

BOI

basis of issue

C&A

certification and accreditation

CAT-ASVAB

Computer Adaptive Testing-Armed Services Vocational Aptitude Battery

CCB

Configuration Control Board

CCM

command copier manager

CCSB

Configuration Control Sub-Board

CIO

chief information officer

CONUS CERT

Continental United States Regional Computer Emergency Response Team

COOP

continuity of operations plan

COTS

commercial-off-the-shelf

CSA

communication service authorization

DA

Department of the Army

DD

Defense Department

DAA

designated approval authority

DASD

direct access storage device

DITSCAP

Defense Information Technology Certification and Accreditation Process

DOD

Department of Defense

DSN

Defense Switching Network

e-mail

electronic mail

fax

facsimile

GOTS

Government-off-the-shelf

GSA

General Services Administration

HQ USMEPCOM

Headquarters, United States Military Entrance Processing Command

IA

information assurance

IAM

information assurance manager

ID

identification

IAO

information assurance officer

IANO

information assurance network officer

IAPM

information assurance program manager

IAVA

Information Assurance Vulnerability Alert

IAVB

information assurance vulnerability bulletin

IAW

in accordance with

IMENS

information mission elements needs statement

INFOSEC

Information Systems Security

I/O

input/output

IP

Internet protocol

IT

information technology

ITS

information technology specialist

JCL

job control language

LAN

local area network

MB

megabytes

MEAD

USMEPCOM Equipment Authorization Document

MEPS

military entrance processing station

MOU

memorandum of understanding

MPA

USMEPCOM Public Affairs

NETCOM

Network Enterprise Technology Command

NIPRNET

Nonsecure Internet protocol router network

NIST
National Institute of Standards and Technology

OMB
Office of Management and Budget

PBX
public branch exchange

PC
personal computer

POC
point of contact

PR
problem report

Reg
regulation

SA
system administrator

SCM
software configuration management

SCMS
Software Configuration Management System

SCP
system change proposal

SSAA
System Security Authorization Agreement

SBU
sensitive but unclassified

SPEAR
Sharing Policy Experience And Resources

SSS
Selective Service System

TCCO
telecommunications control officer

TDA
tables of distribution and allowances

TCOO

telecommunications ordering officers

US

United States

user ID

user identification

USMEPCOM

United States Military Entrance Processing Command

USMIRS

USMEPCOM Integrated Resource System

WAN

wide area network

WWW

World Wide Web

Section II

Terms

certification

The process by which the telephone bill is annotated to be correct. This process is the acknowledgment that all calls were approved by the TCCO.

Clinger-Cohen Act

Public Law 104-106.

collect call

A call placed through the operator and charged to the called number.

communications service authorization

A contract issued by 7th Signal Command to J-6/MIT Network Support Division (J-6/MIT-SD) Telephone Operations, sectors, MEPSs, and vendors. The CSA is used as authorization to pay telephone invoices and order telephone services.

contracting officer

A military or DA civilian employee who has been delegated authority for the execution, distribution, administration of all telecommunications service contracts within a designated area, consisting of one or more Army installations or activities.

data set

A device that converts the signals of a business machine to signals that are suitable for transmissions over communications lines.

Defense Metropolitan Area Telephone System

A centrally managed DD telephone service program for military activities in specified metropolitan areas.

[TOC](#)**Facsimile**

Transmission of letters, memorandums, pictures, maps, diagrams, etc. The image is scanned at the transmitter, reconstructed at the receiving station, and duplicated on some form of paper.

monitoring

Covert listening to telephone conversations by use of mechanical, acoustical and electronic devices. Monitoring is strictly prohibited.

specialty software

Specialty software is defined as software products that are extremely limited in use. Typically used by the J-6/MIT personnel and/or hardware vendors to assist in support of the computer environment.

system software

System software is defined as Operating System and related software products that are not directly accessed by the end user.

telecommunications

Telecommunications services are those Government or leased services provided by all types of systems and facilities to transmit or receive information between two or more points by means of radio, wire, cable, satellite and other electronic media. Included are telephone, telegraph, teletypewriter, and data transmission facilities. Also included are local post, camp or station fixed or mobile facilities that are interconnected to systems providing these types of services.

telecommunications control officer

The TCCO is a noncommissioned officer, or petty officer, E-6 through E-9, or a civilian grade GS-6 or above who is responsible for the administration of the unit telecommunication program.

user software

User software is defined as software products that are available for use by the end user community.

verification

The process by which the local telephone invoice/bill or other charges are checked by the TCCO. Once charges are verified as being correct, the bill is certified and forwarded to J-6/MIT-SD telephone operations for further processing.