DEPARTMENT OF DEFENSE
HEADQUARTERS, UNITED STATES MILITARY ENTRANCE PROCESSING COMMAND
2834 GREEN BAY ROAD, NORTH CHICAGO, ILLINOIS 60064-3091

USMEPCOM Regulation
No. 25-1

Effective date: September 10, 2019

Information Technology: Management of Subdisciplines
Managing Information Technology Resources

FOR THE COMMANDER:

CUNNINGHAM.JOANNE.THERESE.1091128434 Digitally signed by CUNNINGHAM.JOANNE.THERESE.1091128434 Date: 2019.09.10 12:38:07 -05'00'

J. Cunningham
Deputy Commander/Chief of Staff

DISTRIBUTION:
Unlimited. This Regulation is approved for public release.

Executive Summary. This regulation provides guidance for implementing, managing, and using all USMEPCOM Information Technology (J-6/MEIT) resources. It covers Cybersecurity, Information Assurance, system security of all hardware and software, system development and analysis, life-cycle management, user support and services, telecommunications, telephones, copiers, and operations in support of these resources. Prescribes the use of USMEPCOM Form 25-1-7-E (USMEPCOM Sanitization Validation Form) and, DD Form 250 (Material Inspection and Receiving Report), Information Technology Equipment (ITE) Basis of Issue (BOI).

Applicability. This regulation applies to all users, planners, and developers of J-6/MEIT 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/MEIT, 2834 Green Bay Road, North Chicago, IL 60064-3091.

Suggested Improvements. The proponent agency of this regulation is HQ USMEPCOM, J-6/MEIT. 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/MEIT, 2834 Green Bay Road North Chicago, IL 60064-3091.

Internal 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, April 28, 2008; USMEPCOM Policy Memorandum (PM) 5-2, 25 Sep 2013; PM 5-7, 25 Sep 2013; PM 5-8, 22 Aug 2017; PM 5-9; 22 Aug 2017; PM 5-10; 22 Aug 2017; PM 5-11, 2 Sep 2014; PM 5-12, 22 Sep 2014; PM 5-13,9 Dec 2014; PM 5-14, 30

Jun 2015; PM 5-15, 26 Feb 16; PM MEIT-15, 29 Sep 2015; MEIT PM-19, 7 Mar 2019; USMEPCOM Forms (UMF) 25-3-3, UMF 25-3-4-E, UMF 25-3-5-E, UMF 25-3-6-E, UMF 25-3-7-E; INFO-12-03MAR-070; INFO-15-07JUL-173; INFO-15-09SEP-218; USMEPCOM19022744Y0 - INFO MSG

Summary of Changes

Major revisions have been made to this USMEPCOM Regulation (UMR), changes are in red text. Information that is obsolete and will be deleted is in red text with ~~strikethrough~~.

Incorporating changes effective September 10, 2019

- Paragraph 1-4b(5)(c): Added CIO responsibility to appoint Activity CP-34 Program Managers (ACPM).
- Paragraph 1-4h(7): Added BSD responsibility to oversee USMEPCOM Architecture Team for IT
- Paragraph 1-4n(24): Updated hand-receipt responsibilities for the MEPS ITS.
- Paragraph 1-4o(8): Added VPN paperwork requirement
- Paragraph 1-5: Added IT requirements for levels of access requirements (replaces PM 5-9).
- Paragraph 1-6: Added to address Machine and User Based Network Logon Enforcement (replaces PM 5-8) and aligned text with DoDI 1000.13
- Paragraph 1-8: Added to address access to controlled IT spaces (replaces PM 5-10).
- Paragraph 1-14: Outlined CP-34 programs.
- Paragraph 2-8b(2): Added to address vulnerability management, and technical controls (replaces INFO-15-03MAR-218).
- Paragraph 3-7a(4): Removed
- Paragraph 3-10d(1): Removed
- Chapter 4: Renamed to IT Business Services Division
- Paragraph 4-14: Moved to New Paragraph 1-6
- Paragraph 5-18: Added to address requesting additional network services within USMEPCOM controlled facilities (replaces INFO MSG USMEPCOM19022744Y0).
- Paragraph 5-24: Added to address Wireless Local Area Network (WLAN) (replaces PM MEIT-19).
- Paragraph 8-15: Added to address use of mobile telephones overseas.
- Chapter 10: Renamed to USMEPCOM Enterprise Architecture Team for Information Technology (MEIT-EA)
- Throughout: Changed Risk Management and Compliance Office (RMO) to Cyber Security Office (CSO) (replaces INFO-15-03MAR-173).
- Throughout: Changed Help Desk to Service Desk (replaces INFO-12-03MAR-070).
- Throughout: Changed Enterprise Systems Architecture & Integration Office (EAO) to USMEPCOM Enterprise Architecture Team for Information Technology (MEIT-EA)
- Throughout: Changed Blackberry(ies) to Mobile Device(s)
- Paragraph 1-4 and 3-9: Removed References to INFORMATION MESSAGE INFO-11-08AUG-232 (Logistics Policies and Procedures for Property Accountability Operational Guide) UPDATE 1.

Table of Contents (TOC)

TOC

Chapter 1
General

1-1. Purpose

This regulation establishes and assigns United States Military Entrance Processing Command (USMEPCOM) responsibilities for the management of Information Technology (IT) resources and J-6/Information Technology Directorate (MEIT). This regulation implements the provisions of Public Law (PL) 104-106 (Clinger-Cohen Act) (Information Technology Management Reform Act), Army Regulation (AR) 25-1 (Army Knowledge Management and Information Technology), Army Regulation 25-2 (Information Assurance) and related Army and Department of Defense (DoD) regulations listed in Appendix A. This regulation addresses the management of information as a USMEPCOM resource and the J-6/MEIT resources to support those requirements.

1-2. References

References are listed in Appendix A, References.

1-3. Abbreviations and Terms

Abbreviations and terms used in this regulation are explained in Appendix J, Glossary.

1-4. Responsibilities

a. USMEPCOM Commander will:

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

(2) Ensure the CIO and Deputy Chief Information Officer (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 and ensure they hold the appropriate clearance and Information Assurance (IA) baseline certifications or higher.

(3) Establish policies and procedures to guide Information Technology Asset Management (ITAM) in support of USMEPCOM's strategic vision, goals, and objectives.

(4) Provide manpower and funding necessary to operate a comprehensive ITAM program to monitor IT assets to include hardware, software, applications, and databases within USMEPCOM.

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

(1) Serve as the principal focal point for USMEPCOM IT 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 IT issues and initiatives.

(3) Set policies and requirements for the operation of the MEIT Enterprise Data Center (EDC) in accordance with (IAW) guidance from the USMEPCOM Commander.

(4) Assume overall responsibility for management and administration of the ITAM program.

TOC

(a) The CIO advises the Commander and other senior management personnel on all IT issues. It is critical to ensure IT is acquired and information resources are managed consistently with established investment decisions and priorities.

(b) Per 40 United States Code (USC) Subtitle III, the role of the CIO, J-6/MEIT is to manage command, control, communications, and computers/information technology (C4/IT) and primarily, execute Information Resources Management (IRM) functions.

(c) Chapters 2 and 3 of AR 25-1 identify and describe the CIO mission and functions. The efficient and effective use and management of information resources has a direct impact on the USMEPCOM's ability to perform its missions.

(5) Serves as the USMEPCOM Career Program Manager (CPM) for Army Civilian Training, Education & Development System (ACTEDS), Information Technology Management, Career Program 34 (CP-34).

(a) Identifies resources required to fulfill the Commands responsibilities for training and development.

(b) Advises the USMEPCOM and Military Entrance Processing Station (MEPS), Battalion, and Sector Commanders on IT/Cyber training requirements, workforce development, and career management.

(c) Appoints, in writing, Activity Career Program Manager (ACPM) and POC for CP-34 to assist with the management and distribution of information for the Career Program 34.

c. Deputy Chief Information Officer/Deputy Director, Information Technology (J-6/MEIT) 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 Cybersecurity Implementation Program within the command.

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

(4) Supervise the daily operations of the J-6 including the Core Services Division (J-6/MEIT-CSD), IT Business Services Divisions (J-6/MEIT-BSD), Cyber Security ~~Risk Management and Compliance~~ Office (J-6/MEIT-CSO ~~RMO~~), ~~Enterprise Systems Architecture and Integration Office (J-6/MEIT-EAO)~~ and Plans and Resources Office (J-6/MEIT-PRO).

(5) Oversee IT financial management and analysis, technical review of proposed plans or technology such as Business Processing Reengineering (BPR) analysis, Portfolio Management, and external Defense Business System (DBS) reporting in Army Portfolio Management Solution (APMS) requirements and DoD's Select and Native Programming – Information Technology (SNaP-IT).

d. Program Information System Security ~~Assurance Program~~ Manager (P-ISSM) ~~(IAPM)~~ will:

(1) Implement the overall Command Cybersecurity program, focusing on J-6/MEIT security.

TOC

(2) Serve as the Security Technical Advisor to the Authorizing Official (AO), USMEPCOM Commander, CIO, and DCIO.

(3) Hold the appropriate clearance and Information Assurance baseline certification or higher IAW DoDD 8140.01.

(4) Will annually validate ITAM report to ensure all IT assets (hardware, software, applications, and databases) on USMEPCOM's Defense Accession Network (DAN) are approved for use on the Department of Defense Information Network (DoDIN). ~~within Land Warrior Network (LandWarNet)~~ DAN includes all USMEPCOM networks.

(5) Will ensure IT asset discrepancies, whenever identified, are reported to the J-6/MEIT-PRO asset management team through a J-6/MEIT-CSD-CSB-Service Desk ticket.

(6) Will resolve the service desk ticket when hardware components are replaced within J-6/MEIT-CSO ~~RMO~~ span of control and transfer the ticket to the J-6/MEIT-PRO asset management team for IT asset management database update and ticket closure.

(7) When tracking is implemented, will resolve the service desk ticket when application and database versioning is changed within J-6/MEIT-CSO ~~RMO~~ span of control to include identification characteristics, transfer the ticket to the J-6/MEIT-PRO asset management team for IT asset management database update, and ticket closure.

e. USMEPCOM Enterprise Data Center (EDC) Manager will:

(1) Ensure the integrity of the USMEPCOM EDC. ~~/Selective Service System (SSS) EDC~~.

(2) Review/Approve/Grant access to the EDC for approved personnel.

(3) Provide assistance to EDC users and ensure sufficient space, power and environmental controls for all hardware as required.

(4) Manages the placement of all hardware including power and environmental controls in the EDC.

(5) Act as the J-6 single point of contact for any IT related matters for MEPS, Remote Processing Stations (RPS), or other USMEPCOM facilities relocations/renovations, to include security requirements.

f. J-6/MEIT Plans and Resources Office (PRO) will:

(1) Be the J-6 proponent for ITAM and will manage the ITAM database.

(2) Be responsible for oversight of the ITAM database and maintains primary responsibility for establishing asset records for hardware, software, and when implemented, applications and databases within the USMEPCOM environment.

(3) Track all IT assets using the ITAM database ensuring asset documentation is comprehensive, accurate, and changes posted within five business days of notification. Complete documentation in ITAM

TOC

database will include procurement date, cost, and contract number, terms and conditions of warranty, warranty contact information, expected lifecycle date, software and applications installed to include versioning information, and license counts utilized.

(4) Update the ITAM database and close assigned resolved service desk tickets within five business days.

(5) Provide ITAM information to responsible parties at HQ/Sectors/Battalions/MEPS necessary to perform annual validation of hardware and software.

g. J-6/MEIT-Core Service Division (CSD) will:

(1) Annually validate ITAM report to ensure all IT assets (hardware, software, applications, and databases) are documented.

(2) Ensure all IT assets (hardware, software, applications, and databases) are reported to the J-6/MEIT-PRO asset management team through a service desk ticket.

(3) Ensure discrepancies, whenever identified, are reported to the J-6/MEIT-PRO asset management team through a service desk ticket.

(4) Coordinate with J-6/MEIT-PRO prior to approval of any "Change Request" that implements the addition of software/hardware licensing or the updating of existing software/hardware to new versions.

(5) Review ITAM database to determine warranty/support status of asset ITAM database and will provide information needed when reporting a faulty asset to manufacturer for replacement or technical support.

(6) Request replacement assets IAW vendor generated procedures.

(7) Mark "resolved" on the service desk tickets when hardware components are replaced across the enterprise and transfer the ticket to the asset management team for IT asset management database update and ticket closure.

(8) When tracking is implemented, will resolve the service desk ticket when application and database versioning is changed to include identification characteristics, transfer the ticket to the asset management team for IT asset management database update, and ticket closure.

h. J-6/MEIT-Information Technology Business Service Division (BSD) will:

(1) Annually validate ITAM report to ensure all IT assets (hardware, software, applications, and databases) are documented.

(2) Ensure discrepancies, whenever identified are reported to the J-6/MEIT-PRO asset management team, through a service desk ticket.

(3) Coordinate with J-6/MEIT-PRO prior to approval of any "Change Request" that implements the addition of software/hardware licensing or the updating of existing software/hardware to new versions.

TOC

(4) Resolve the service desk tickets when hardware components are within J-6/MEIT-BSD span of control and transfer the ticket to the asset management team for IT asset management database update and ticket closure.

(5) Resolve the service desk tickets when software licenses or versioning are replaced within J-6/MEIT-BSD span of control and transfer the ticket to the asset management team for IT asset management database update and ticket closure.

(6) Resolve the service desk ticket when application and database versioning within J-6/MEIT-BSD span of control is changed to include identification characteristics, transfer the ticket to the asset management team for IT asset management database update, and ticket closure when tracking is implemented.

(7) Oversee USMEPCOM Enterprise Architecture Team for Information Technology (MEIT-EA) as outlined in Chapter 10 of this regulation.

i. Director, Human Resources Directorate (J-1/MEHR) will apply security requirements outlined in DoDI 8510.01 (Risk Management Framework (RMF), DoDI 8500.01 (Cybersecurity), AR 25-2, and all applicable directives within their area of responsibility, adhering to physical and environmental controls within their purview.

j. Director, Facilities and Acquisitions Directorate (J-4/MEFA) will:

(1) Identify all USMEPCOM facilities relocations or renovations projects (including Military Entrance Processing Stations (MEPS), Sectors, HQ USMEPCOM, RPS, or other USMEPCOM locations) requiring J-6/MEIT actions through the Program Objective Memorandum (POM) process. J-6/MEIT will ensure that resources in support of identified J-4/Facilities and Acquisitions Directorate (J-4/MEFA) actions are submitted to J-8/Resource Management Directorate (J-8/MERM) for funding. J-6/MEIT will identify, defend, and execute funding resources to support all facility relocation or renovation projects.

(2) Update J-6/MEIT on the status of relocations and renovations to keep projects on track.

(3) Apply security requirements outlined in DoDI 8510.01, DoDI 8500.01, AR 25-2, and all applicable directives within their area of responsibility, adhering to physical and environmental controls within their purview.

(4) Coordinate and get approval from J-6/MEIT on all USMEPCOM facilities projects included in construction/renovation contracts/plans that relate to IT issues including IT-related conduit, wiring, drops, and power; physical space, air conditioning, heating, and ventilation.

(5) Ensure that all management and accountability functions of receipt, storage, inventory, issue, and shipment fully utilize available Automated Information Technology for property accountability.

(a) J-4 Logistics Division (MEFA-LD) as proponent for the USMEPCOM property accountability system, currently Property Book Unit Supply Enhanced (PBUSE); provide periodic (monthly) data reports to J-6/MEIT PRO to validate USMEPCOM's property accountability and IT asset management systems.

(b) Provide members of the J-6/MEIT-PRO Asset Management Team with read-only/query access to USMEPCOM property accountability system.

k. Director, Resource Management (J-8/MERM) will assist in obtaining funds, reporting on funds, expending funds, and providing status of funds to accomplish the J-6/MEIT initiatives.

l. Directors, Special Staff Officers, Sector, Battalion, and MEPS Commanders will:

(1) Apply security requirements outlined in DoDI 8510.01, DoDI 8500.01, AR 25-2 (Information Assurance) and all applicable directives to any command J-6/MEIT resource within their area of responsibility.

(2) Ensure a DD Form 2875 (System Authorization Access Request) is completed for all account deactivations within 72-hours prior to departing USMEPCOM's employment.

(3) Ensure adherence to provisions of AR 340-21 (The Army Privacy Program).

(4) Ensure physical security and accountability of all J-6/MEIT equipment and associated J-6/MEIT program products IAW AR 190-13 (The Army Physical Security Program) and AR 190-51 (Security of Unclassified Army Property [Sensitive and Non-sensitive]).

(5) Ensure a 30-day operational ~~sufficient~~ supply of J-6/MEIT consumables is on-hand. ~~in accordance with (IAW) INFORMATION MESSAGE INFO-11-08AUG-232 (Logistics Policies and Procedures for Property Accountability Operational Guide) UPDATE 1.~~

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

(7) Adhere to prescribed procedures for requesting J-6/MEIT resources electronically via USMEPCOM Parametric Technology Corporation (PTC) - formerly Mortice Kern System (MKS). Instructions for completing this electronic form are in Appendix C (Instructions for Completion of a Problem Reporting (PR), System Change Proposal (SCP), and Information Mission Elements Need Statement (IMENS)).

(8) Ensure appropriate training on J-6/MEIT resources.

(9) Ensure initial and annual Cybersecurity training is completed by all Sector, Battalion, RPS, and MEPS personnel as prescribed by J-6/MEIT-CSO. ~~RMO~~

(10) Annually validate ITAM report to ensure all IT assets (hardware, software, applications, and databases) are documented.

(a) Validate sufficient software licensing and correct versioning is available in collaboration with the J-6/MEIT Change Control process.

(b) Perform an annual self-audit to reconcile software entitlements against actual license use within USMEPCOM.

(11) Ensure any requirements for data collection or storage must include data retention requirements that are coordinated with applicable branch(es) within J-1/MEHR and provided to applicable

TOC

branch(es) and offices in J-6/MEIT.

(12) Will annually validate ITAM report to ensure all IT assets (hardware, software, applications, and databases) are documented.

m. Sector, Battalion and MEPS Commanders will:

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

(2) Monitor maintenance procedures at their Sector, Battalion, MEPS, or RPS 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/MEIT resources to comply with allowance documents and Information Technology Equipment (ITE) Basis of Issue (BOI) 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/MEIT resources for USMIRS equipment and software, through J-6/Plans and Resource Office (J-6/MEIT-PRO) and J-3/Accessions Division (J-3/MEOP-AD) by following all required guidelines.

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

(7) Appoint MEPS Information Technology Specialist (ITS) to perform the duties of an Information Assurance Support Officer (IASO) and Information Assurance Technical Level I (IAT-1) IAW Department of Defense 8570.01-M, Information Assurance Workforce Improvement Program. Use the format described in Appendix F.

(8) Appoint Optional Auxiliary MEPS Information Technology Specialist (ITS) to manage day-to-day use of J-6/MEIT resources within their area of responsibility. Use the format described in Appendix G. The following criteria shall be adhered to concerning the selection of and provisioning for an Auxiliary ITS:

(a) Requirements:

1. This appointment will be a service member (Army, Navy, Air Force, Marine, or Coast Guard) from the respective MEPS assigned to USMEPCOM.

2. This appointment will be in writing and the service member will be assigned this role as an additional duty.

3. The Auxiliary ITS must be trained to conduct ITS roles and responsibilities.

(b) Roles and Responsibilities:

TOC

1. Auxiliary ITS will serve as the Information Technology (IT) focal point in the absence of the ITS.

2. They will have knowledge of procedural requirements needed in supporting IT functions.

3. They will utilize the Battalion IT Subject Matter Experts (SMEs), the Sector ITS, and the USMEPCOM J-6/MEIT-CSD-CSB-Service Desk to resolve issues in the absence of the ITS.

(c) Special Considerations:

1. The Auxiliary ITSs are required to obtain certification IAW DoD 8570.01-M within 6 months of appointment.

2. The Auxiliary ITS may be granted elevated permissions if they are certified and have completed the necessary requirements. This would enable the Auxiliary ITS to physically perform administrative functions in the absence of the ITS.

3. Elevated permission would be granted on a temporary basis and will be removed upon the return of the ITS.

4. Elevated permission may be granted by the respective Sector Commander for an ITS absent greater than 5 business days only after J-6/MEIT Information Technology Directorate has verified the request and noted the duration.

5. Emergencies will be handled on a case-by-case basis with recommendations made from Sector leadership.

Note: Funding for the Auxiliary ITS training and/or certification shall be at the discretion of the Battalion Commanders through use of Battalion training funds. At each MEPS Commander's discretion, Auxiliary ITS may pursue off-duty education and/or coordination training with local military units to obtain certification IAW DoD 8570.01-M.

(9) Overall Command Responsibility to ensure Sector staff and Subordinate MEPS Commanders adhere to ITAM.

(a) Ensure Administrative Services Technician (AST) and Information Technology Specialists (ITS) follow management controls to provide assurance that Command ITAM policy and procedures identified in this regulation are met.

(b) Ensure effective and efficient utilization of IT resources provided to the Sector, Subordinate MEPS, and RPS for mission accomplishment.

(c) Coordinate ITAM actions with the J-6/MEIT-CIO, J-6/MEIT-PRO staff, and J-4 Logistics Division prior to execution.

n. Sector, Battalion and MEPS ITSs will:

(1) Apply security requirements outlined in DoDI 8500.01, DoDI 8510.01, AR 25-2, and all

TOC

applicable directives within their area of responsibility.

(2) Ensure information security procedures are followed within the MEPS or RPS at the direction of the J-6.

(3) Ensure a DD Form 2875 is completed for all account deactivations within 72-hours prior to departing USMEPCOM's employment whenever possible.

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

(5) Ensure the Host Based Security System (HBSS) agent is properly installed on all workstations and laptops.

(6) Ensure vulnerabilities are patched on all workstations and laptops and kept current using updates from USMEPCOM approved sources only. Vulnerabilities shall be mitigated within 30 days from date of publication.

(7) Act as the organizational agent for all matters concerning J-6/MEIT resources within their MEPS, Sector, or Battalion.

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

(10) Maintain all USMIRS equipment and USMIRS related equipment requests, following guidelines as directed from J-6/MEIT-PRO and J-3/MEOP-AD.

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

(12) Validate requirements with functional proponent for all hardware/software and prepare the IMENS form for submission to J-6/MEIT-PRO. Other organizations that USMEPCOM may support such as Navy Liaisons in the MEPS will not place requirements directly onto IMENS, but be directed to go through their Chain of Command.

(13) Ensure physical security and accountability for all J-6/MEIT-CSO ~~RMO~~ equipment within their area of responsibility.

(14) Complete applicable portions of the Management Internal Control Review checklist annually for forwarding to J-6/MEIT-PRO.

(15) Receive and secure new deliveries of Commercial off the Shelf (COTS), Government-off-the-Shelf (GOTS) and USMEPCOM unique software.

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

(17) Assist other organizations in maintaining an accurate inventory of their equipment on site,

TOC

which includes the receipt and return of equipment to other organizations.

(18) Maintain a network documentation folder IAW Paragraph 5-7.

(19) Ensure the backup individual is trained in J-6/MEIT-CSD-Enterprise Customer Service Branch-Service Desk (J-6/MEIT-CSD-CSB-Service Desk) procedures IAW chapter 6.

(20) Enter and/or monitor submission of Problem Reporting (PR) and System Change Proposal (SCP) data into the automated PTC ~~PCT~~ tool IAW Chapter 4-3.

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

(22) Ensure initial and annual Cybersecurity training is completed by all Sector, Battalion, MEPS, and RPS personnel as prescribed by J-6/MEIT-CSO ~~RMO~~.

(23) Ensure a Virtual Private Network (VPN) access request form is submitted and approved for users that may require access ~~prior to installing and configuring on a user's laptop~~.

(24) Maintain an inventory of IT assets that consist of physical IT assets (computers, printers, monitors, network devices, etc.) and logical IT assets (physical/digital software, software licensing, and applications). The inventory supports the ITAM program and not the Property Accountability program.

(a) Identify physical location and ownership of all IT assets, and collect IT asset management data for each asset for which they are responsible.

(b) Update and maintain the asset inventory as assets are acquired, transferred within the enterprise, and/or disposed of throughout the asset lifecycle.

(c) Identify the asset, e.g. ID number, type or description of asset, make or manufacturer, model, serial number, etc.

(d) Identify the relationships and dependencies between physical and logical assets.

(e) Will annually validate ITAM report to ensure all IT assets (hardware, software, applications, and databases) are documented.

(f) Will ensure discrepancies are reported to the J-6/MEIT-PRO asset management team through a J-6/MEIT-CSD-CSB-Service Desk ticket whenever identified.

(g) Will, when an Enterprise ITAM tool exists; review ITAM database to determine warranty/support status of asset.

(h) Resolve the service desk tickets when hardware components are installed and transfer the ticket to the asset management team for IT asset management database update and ticket closure, where applicable.

(i) Resolve the service desk tickets when software licenses or versioning are installed or replaced and transfer the ticket to the asset management team for IT asset management database update and ticket closure, where applicable.

(25) Provide support to non-USMEPCOM personnel as directed by J-6/MEIT which includes organization that USMEPCOM has agreement(s) to support such as Navy Liaisons, outside inspectors, or other organizations such as Service Liaisons/Counselors.

o. 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 DoDD 8140.01.

(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 2875. The complete DD 2875 will be submitted to the J-6/MEIT-CSO ~~RMO~~ office.

(4) Only the J-6/MEIT-CSO ~~RMO~~ 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.).

(8) Ensure a Virtual Private Network (VPN) form is approved prior to installing and configuring on a user's laptop.

p. End Users.
End Users are to 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. Further details on these actions are included in Paragraph 2-8.

(1) Users will certify their compliance with J-6/MEIT-CSO ~~RMO~~ security training is conducted annually.

(2) Ensure that all Common Access Card requirements are met and adhered to.

(3) Register in Army Training and Certification Tracking System (ATCTS) as directed by J-6/MEIT-CSO ~~RMO~~.

(4) Users will annually certify that they will adhere to USMEPCOM acceptable use policy.

1-5. General and Privileged Level Access
USMEPCOM employees who have access to IT Systems must meet specific IA requirements in order to obtain access. These requirements must be maintained in order to retain access. All employees, to include military and contractors, must register in the Army Training and Certification Tracking System (ATCTS) at http://atc.us.army.mil. This system is the database of record for IA Compliance for general and privileged level access accounts.

a. All users will receive a General User account. General Users are required to take IA training initially and annually thereafter. General Users are to sign the Automated Acceptable Use Policy upon initial login, and annually thereafter.

b. Individuals requiring privileged level access fall into one or more additional categories. Each has its own specific requirements for authorization, retention, and may be considered an IA position. The type of category must be identified in the individual's ATCTS profile. The six categories are:

(1) Power User - Personnel with limited administrative privileges to their workstation only. For example, personnel assigned the USMIRS OPS Admin* role are power users. This is not an IA position.

(2) IA Support Officer (IASO) - IASO personnel verify that all requirements for system access to an Information System are met and are the lowest IA management level.

(3) IA Technical (IAT) Level I/II/III- IAT personnel make the Computing Environment (CE), Network Environment (NE), and enclave less vulnerable by correcting flaws and implementing technical controls in the hardware or software installed within their operational systems. For example, Information Technology Specialists and personnel assigned the USMIRS SYS Admin Role are IAT personnel.

(4) IA Management Level (IAM) I/II/III - IAM personnel are responsible for the implementation and operation of an Information System (IS) within their CE, NE, or enclave. Personnel in these positions perform a variety of security related tasks, including the development and implementation of system information security standards and procedures. They ensure the IS are functional and secure within the environment. For example, CSO personnel and supervisors who manage IAT personnel.

(5) IA System Architect and Engineer Level I/II/III-IASAE personnel apply knowledge of IA policy, procedures, and workforce structure to design, develop, and implement a secure CE, NE, and enclave.

(6) Cybersecurity Defense Analyst - CSD-A personnel use data collected from a variety of IA tools (including intrusion detection systems alerts, firewalls, network traffic logs, and host system logs) to analyze events that occur within their environment.

c. Special Staff Office ATCTS management will be maintained by J-6/MEIT-CSO personnel.

d. Directorates are to maintain ATCTS for their respective areas.

e. Sector Battalion, and MEPS Information Technology Specialist (ITS), Auxiliary ITS are to maintain ATCTS for their respective areas. When a MEPS does not have an ITS, the Battalion IT SME

TOC

and/or Sector ITS will fill this role for the MEPS.

f. Administration of ATCTS includes ensuring all personnel register in ATCTS, meet annual training requirements, and are properly identified per paragraph a. and b. of this policy, and ensure departed personnel are marked inactive.

g. Individuals filling IA positions, to include military and contractors, performing collateral and/or functions require to be assigned to the IA positions by appointment.

h. USMEPCOM's P-ISSM is responsible for appointing personnel to the applicable category and level. Categories and levels vary and personnel are appointed upon reporting to duty; whether civilian, military, or contractor.

i. All personnel have mandatory IA training requirements. Individuals who fail to meet general user training may have their network access revoked until requirements are met.

j. Civilian and military personnel performing privileged level functions must meet training requirements prior to receiving their privileged level access account. Civilian and military personnel have six months to complete certification requirements for their position. Failure to meet or maintain certifications will result in revocation of privileged level access. Inability to comply with the certification requirements may result in reassignment or removal from duties, consistent with applicable law. Power Users have additional training requirements. IA appointed positions have additional training and certification requirements. Individuals who fail to meet training and certification requirements for privileged level access, may have their elevated access revoked until requirements are met.

k. Contractor personnel performing privileged level functions must meet training and certification requirements prior to onboarding with USMEPCOM. Failure to maintain certifications will result in removal from contract.

1-6. Authorized Users

a. Only government civilian employees, military service members, and contract personnel shall have access to government automated resources. Applicants shall only be granted supervised access for the purpose of completing official processing functions (e.g. in CAT-ASVAB testing, Defense Language Proficiency Test (DLPT), Red Carpet Survey).

b. All users are required to use a CAC for network logon. User accounts will no longer be created with a username and password. The Electronic Data Interchange Personal Identifier (EDIPI) recorded on the CAC must be enclosed on a System Authorization Access Request in order to process the request.

(1) If a user forgets to bring their CAC to work, they will have to go and retrieve it. Otherwise, their supervisor will need to request temporary CAC exempt status or ensure they have work that can be done without logging onto a workstation.

(2) If the CAC Pin gets locked, it will have to be reset at the nearest CAC Pin Reset Station.

(3) Any lost CACs must be reported immediately to the nearest issuing office to have the CAC cancelled. Once the CAC is cancelled, a new one may be issued.

TOC

(4) The J-6/MEIT and user will ensure all necessary actions are taken to reduce the period of exemption. However, supervisors may request user exceptions from the J-6/MEIT Service Desk for the following reasons:

(a) 1-day exemption due to forgotten CAC.

(b) 30-days exemption due to technical difficulties rendering the CAC unusable.

c. All Users will assure that USMEPCOM systems and data are safe and secure from unauthorized access that might lead to the alteration, damage, or destruction of automated resources and data, unintended release of data, and denial of service.

d. Pursuant to DoDI 1000.13 (Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals), users will keep their CAC in personal custody at all times. ~~Users will remove their CAC when the computer is left unattended.~~

e. The USMEPCOM J-6/MEIT-CSD-CSB-Service Desk serves as a focal point for incident reporting and subsequent resolution. All incidents will be handled in accordance with the J-6/MEIT Incident Response Plan located on the J-6 Cyber Security Office SPEAR page.

1-7. Managing Information Resources and Technology

a. Information resources. In accordance with AR 25-1, 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 are subject to this regulation. 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 are subject to this regulation. Responsibility includes computers, ancillary equipment, software, firmware and similar procedures, services, and related resources.

c. The J-6/MEIT-CSD-CSB supports USMEPCOM on a data service center basis to include computer operations, tape library support, telecommunications processing, and physical and data security.

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.

1-8. Physical Access for Controlled IT Spaces

a. Access to controlled IT spaces will be limited to individuals with an established duty or business requirement for access. This includes physical access to key IT assets, as well as the areas in the vicinity of the assets, within the controlled IT space. Controlled IT spaces are defined as rooms, closets, or sections of a building that house key IT assets, such as routers, switches, network management devices, servers, network security devices, and Voice-over-IP (VoIP) equipment. This list should be considered illustrative, not exhaustive. Areas under the control of the Administrative Services Technician (MEPS Supply Technician) for maintaining excess IT equipment should not be included in this list.

b. The individual responsible for establishing the duty requirement (known as the Access Authority) is based on the location of the space. At each MEPS, the Access Authority is the MEPS Commander (or his/her designee). The Access Authority for USMEPCOM-controlled spaces within Building 3400 is the Chief Information Officer of the command (or his/her designee).

c. The Access Authority will determine when unescorted access privileges are warranted. Unescorted access privileges will be limited to individuals with a recurring need for unsupervised access to controlled IT spaces. Unescorted access privileges require an appropriate background investigation and the use of an authorized and valid access credential. Investigation and credential requirements are detailed in Directive-Type Memorandum (DTM) 09-012, Interim Policy Guidance for DoD Physical Access Control. Additionally, individuals that will install, configure, modify, or maintain IT assets will also meet the requirements detailed in AR 25-2 and DoD 8570.01-M.

d. Individuals with irregular or one-time entry requirements will be treated as visitors, and escorted at all times by a USMEPCOM employee with unescorted access privileges. Contractors, regardless of held privileges or credentials, are not authorized to act as escorts. If the visitor's onsite activities involve the maintenance of IT assets, the escorting employee will be an individual with the technical expertise to detect unauthorized modifications.

e. All controlled IT spaces will have a completed Access Control List (ACL) available for ready review. For each space, the ACL will be affixed to the inside of the entry door, near eye-level. The ACL will contain the names of all individuals authorized unescorted access privileges to that space, and will be signed and dated by the pertinent Access Authority.

f. The IASO, for the Sector/Battalion/MEPS/RPS ITS, and ISSO, for CSO personnel, will review the ACL for validity at a minimum of once per quarter, and will immediately remove names that meet the following criteria:

(1) The individual no longer has a duty or business requirement for unescorted access

(2) The individual no longer works for (or no longer has an active contract with) USMEPCOM

(3) The individual no longer meets security fitness and IA requirements (if any) for unescorted access

1-9. 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/MEIT and related investments will be evaluated in terms of their support of USMEPCOM processes and their corresponding information requirements.

b. DCIO will maintain all data collected and ensure the data is readily accessible when requested by an approved source. This includes actively pursuing and identifying organizations that could benefit from the data and establishing data transfer methodologies that conform to the DoD Joint Technical Architecture (JTA) standards. This practice promotes economic use of resources by eliminating duplication, improving synchronization and reducing costs. DCIO 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/MEIT and information services will be used.

1-10. Use of J-6/MEIT 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/MEIT 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/MEIT 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.

1-11. 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/MEIT 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/MEIT capabilities that can benefit the customer. A relationship between the J-6/MEIT community and users, in which both the customer and the service provider take responsibility for communicating with each other, is necessary. Each J-6/MEIT 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/MEIT 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/MEIT community will embrace accountability to the customer as

TOC

an essential element of the J-6/MEIT 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/MEIT support capabilities.

1-12. 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.

1-13. Non-Policy Procedures

All non-policy procedures are located on the USMEPCOM Sharing Policy Experience and Resources (SPEAR). Updates to the SPEAR information will be available by email from the USMEPCOM proponents.

1-14. Information Technology Management Career Program (CP-34)

a. All USMEPCOM Headquarters, Sector, and MEPS personnel who belong to Career Program 34 are highly encouraged to register for a CP-34 certification. CP-34 Certification registration allows the careerist to take advantage of US Army paid, short term and long term, training.

(1) CP-34 Certification: Focuses on targeting courses and experiences.

(2) CP-34 Outreach Training: Takes advantage of online group training. A careerist may also apply for individual Outreach Training through GoArmyEd. The CP-34 Outreach Training will not pay for TDY or per diem. The CP-34 will not pay for a professional certification (e.g. CompTIA Security+) unless the certification is included in the price of the course.

(3) Academic Degree Training (ADT) Program: The Army may pay and/or assist Army Civilian employees in obtaining an academic degree up to a Master's Degree if the training meets identified organizational training needs. More information can be obtained from GoArmyEd.

b. The CP-34 careerists includes Army Civilians in Occupational Series 0301, 0308, 0332, 0335, 0382, 0390, 0391, 0392, 0394, 1001, 1020, 1060, 1071, 1084, 1410, 1411, 1412, 2210, and 0343 - when preponderance of duties involve Records Management functions.

TOC

Chapter 2
Cybersecurity

2-1. Overview

Cybersecurity is the component of J-6/MEIT-CSO ~~RMO~~ program management that assures operational readiness by providing for the continuous confidentiality, integrity and availability of information, and it's 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/MEIT resources. See Office of Management and Budget (OMB) Circular (Cir) A-130 (Managing Federal Information as a Strategic Resource); National Institute of Standards and Technology (NIST) Special Publication 800-12 (An Introduction to Computer Security: The NIST Handbook); DoD Directive 8500.01; DoD Instruction 8510.01; NIST Special Publication 800-53 Rev 4 (Security and Privacy Controls for Federal Information Systems and Organizations); NIST Special Publication 800-88 Revision 1 (Guidelines for Media Sanitization); Title 17, U.S. Code (Copyrights); Title 18, U.S. Code (Crimes and Criminal Procedure); 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. Authorizing Official (AO) will:

a. Ensure that cybersecurity is incorporated as an element of DoD information system life-cycle management processes.

b. Appoint the Program Information System Security ~~Assurance Program~~ Manager (P-ISSM) ~~(IAPM)~~ in writing, to include a statement of IA responsibilities, and that appointee receives appropriate IA training. Ensure the P-ISSM ~~IAPM~~, in addition to meeting all access requirements specified in Paragraph 4-8, DoD Directive 8500.1, (reference (a)), are U.S. citizens.

c. For DoD information systems or enclaves under his or her purview, ensure that all IA-related positions are assigned in writing, include a statement of IA responsibilities, and that appointees to positions receive appropriate IA training.

d. Ensure that all Information System Security ~~Assurance~~ Manager (ISSM) ~~(IAM)~~, in addition to meeting all access requirements specified in Paragraph 4-8, DoD Directive 8500.1, (reference (a)), are U.S. citizens.

e. Grant DoD information systems under his or her purview formal accreditation to operate according to the DoD RMF assess and authorize process (reference (a)).

f. Ensure that IA-related events or configuration changes that may impact accreditation are reported to affected parties, such as Information Owners and AOs of interconnected DoD information systems.

g. Meet position requirements defined by DoD 8570.01-M.

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

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

j. Oversee the command's formal Assess and Authorize (A&A) (formally Certification and Accreditation (C&A)) program. The AO is responsible for the following A&A actions:

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

(2) Issue a digitally signed approval after receiving/reviewing a recommendation from the Certifying Authority.

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

(4) Ensure when sensitive controlled but unclassified information (CUI) 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).

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

k. Ensure the establishment, administration, and coordination of security for USMEPCOM systems are conducted in accordance with Command IA procedures.

l. Ensure an incident reporting program is established and security incidents or events are reported to affected parties (i.e., interconnected systems, data owners, etc.).

m. Ensure USMEPCOM plans, budgets, allocates and spends resources to achieve and maintain an acceptable level of security and to remedy security deficiencies.

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

o. Complete training and certification.

2-3. Information System Security ~~Assurance~~ Program Manager (P-ISSM) ~~(IAPM)~~ will:

a. Meet position, training and certification requirements defined by DoD 8570.01-M.

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

c. Develop, manage and maintain a formal IA security program, ensuring the appointment of all IA workforce designees.

d. Develop and implement command-unique procedures as needed.

e. Implement and enforce Chairman, Joint Chiefs of Staff, DoD and IA policy.

f. Provide the supporting Regional Computer Emergency Response Team (RCERT) or Telecommunications Control Officer (TNOSC) with guidance and priorities regarding IA/Computer

TOC

Cybersecurity ~~Network Defense (CND)~~ to support to the command.

g. Ensure assigned 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.

i. Serve as the primary Point of Contact (POC) for IA-related actions.

j. Ensure the Department of Defense (DoD) Information Assurance Risk Management Framework (DIARMF) program is implemented.

k. Ensure the development of system A&A documentation.

l. Ensure approved procedures are in place for clearing, purging, and releasing system memory, media, output and devices.

m. Provide AO with system A&A documentation as required.

n. Ensure protective and corrective measures are implemented for vulnerabilities or incidents per direction of the Continental United States Regional Computer Emergency Response Team (CONUS RCERT).

o. Verify data ownership responsibilities (including accountability, access, and special handling requirements) for each information system (IS) or network.

p. Establish, conduct, and oversee a command program of announced and unannounced IA assessments.

q. Program, manage, execute, and report Information Technology Directorate Cyber Security ~~Risk Management and Compliance~~ Office (J-6/MEIT-CSO ~~RMO~~) IA budgets.

r. Provide technical and non-technical information to support the Information Operations Condition (INFOCON) program.

s. Ensure program controls are in place to verify validity of user access requests.

2-4. Information System Security ~~Assurance~~ Manager (ISSM) ~~(IAM)~~ will:

a. Meet position requirements defined by DoD 8570.01-M.

b. Complete the prescribed training and certification IAW DoD 8570.01-M.

c. Implement the IA program within their command and ensure all systems are accredited IAW the Risk Management Framework (RMF) and USMEPCOM A&A program.

d. Maintain a repository of all systems that have A&A documentation.

TOC

e. Inform the ~~IAPM~~ Program Information System Security Manager (P-ISSM) of any changes impacting the IA posture.

f. Conduct periodic reviews of the systems and networks under their jurisdiction to ensure changes have not occurred that affect security and negate the accreditation.

g. Review threat and vulnerability assessments to determine appropriate security measures are in place to manage the risk to systems and networks under their jurisdiction.

h. Provide information and guidance about the IA training and certification program within USMEPCOM.

i. Enforce the established policy for review of weekly alerts, bulletins and advisories as received.

j. Assess the impact to security and comply as prescribed in the J-6/MEIT Incident Response Plan based on reports from the DoD Computer Emergency Response Team (CERT) or service.

k. Oversee a program to review the systems and networks audit trails, and maintain an archive of all required audit records. Audit records will be retained under Record Number 25-1lll/400B, "ITS Administrative Reports". Keep in office file until no longer needed for conducting business, not to exceed 6 years, then destroy.

l. Mitigate ~~to~~ Information Assurance Vulnerability Alerts (IAVA) and other vulnerabilities identified within the Cybersecurity scan engine, Security Technical Implementation Guides (STIGs), and RMF security controls.

(1) Ensure the integrity of the USMEPCOM Enterprise.

(2) Review access request documents for completeness/correctness. Cyber Security ~~Risk Management and Compliance~~ Office (CSO ~~RMO~~) will maintain copies of this documentation for headquarters.

(3) Provide direction to users, as required, to maintain a coordinated overall system security program.

(4) Implement the enterprise IA program and act as the secondary POC for all IA related security matters.

2-5. Cybersecurity Defense Analyst (CSD-A) ~~IA Computer Network Defense (CND)~~ Role

a. Complete the prescribed training and certification as per DoD 8570.01-M.

b. Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.

c. Coordinate with enterprise staff to validate network alerts.

d. Perform analysis of log files from a variety of sources within the enterprise, to include individual

TOC

host logs, network traffic logs, firewall logs, and intrusion detection system logs.

e. Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.

f. Monitor external data sources (e.g. CSD-A ~~CND~~ vendor sites, CERT, SANS (SysAdmin, Audit, Networking, and Security), Security Focus) to maintain currency of CSD-A ~~CND~~ threat condition and determine which security issues may have an impact on the USMEPCOM enterprise.

g. Assist in the construction of signatures which can be implemented on CSD-A ~~CND~~ network tools in response to new or observed threats within the Network Environment (NE) or firewall (enclave).

h. Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.

i. Notify IA team members of suspected CSD-A ~~CND~~ incidents and articulate the event's history, status, and potential impact for further action.

j. Perform CSD-A ~~CND~~ incident triage to include determining scope, urgency, and potential impact; identify the specific vulnerability and make recommendations which enable expeditious remediation.

k. Provide incident reports, summaries, and other situational awareness information to ISSM/P-ISSM ~~IAM/IAPM~~.

2-6. Information System Security ~~Assurance~~ Officer (ISSO) ~~(IAO)~~ will:

a. Possess a valid 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 the information system is operated, used, maintained, and disposed of IAW current guidance.

d. Accreditation and/or certification support documentation will be retained under Record Number 25-2d1/400B, "Accreditation of Automated Systems". Keep in office file until no longer needed for conducting business, not to exceed 6 years, then destroy.

e. 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.

f. Maintain copies on all issued accounts for User Memorandum of Agreement (MOA) for the information systems or networks within their jurisdiction under Record Number 25/400B, "General Information Management Correspondence Files - User Memorandum of Agreement". Keep in office file not more than 2 years, then destroy.

g. Prepare, distribute, and maintain plans, instructions, guidance and standing operating procedures (SOPs) concerning the system operation security.

TOC

h. Enforce security policies and safeguards on all personnel having access to the information system for which the ISSO ~~IAO~~ is responsible.

i. Initiate protective or corrective measures to maintain security on information systems.

j. Verify warning banners are placed on all monitors and appear when a user accesses a system.

k. Notify the ISSM ~~IAM~~ when changes occur on information system(s) that might affect accreditation/certification.

l. Report security incidents to the ISSM ~~IAM~~ IAW Paragraph 2-7(f), 2-8(y) and Paragraph 6-2(b).

m. Conduct periodic reviews to ensure compliance with the accreditation or certification support documentation package.

n. Verify approved security patches are installed as directed.

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 the prescribed training and certification as per DoD 8570.01-M.

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 ISSO/ISSM ~~IAO/IAM~~ to ensure the information system or network is used securely.

f. Report security incidents to the ISSO/ISSM ~~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 (ISSM) ~~(IAM)~~ and ISSO ~~IAO~~ in development and maintenance of A&A support documentation package.

j. Conduct periodic reviews to ensure compliance with the A&A support documentation package.

k. Establish audit trails and conduct reviews weekly, and ensure, as directed by the ISSO ~~IAO~~ and (P-ISSM) ~~(IAPM)~~ that audit records are archived for future reference. Audit records will be retained under

TOC

Record Number 25-1lll/400B, “ITS Administrative Reports”. Keep in office file until no longer needed for conducting business, not to exceed 6 years, then destroy.

l. Provide backup of system operations.

m. Ensure IAVAs, IAVBs, and other vulnerability notifications are applied to appropriate operating systems.

n. Inform the MEIT-CSO ~~RMO~~ of odd, peculiar or strange security or integrity loopholes.

o. In coordination with the MEIT-CSO ~~RMO~~, administer user identification and authentication mechanism(s) of the information system or network.

p. Administer and protect SA passwords IAW current DoD guidance.

q. 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.

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 Acceptable Use Policy, see Appendix I.

b. Complete the Current USMEPCOM ~~IA~~ cybersecurity training requirements before gaining access to a USMEPCOM network or information system. Complete annual training as directed.

c. Verify accuracy of personal information on a DD Form 2875 to request a new system or network account.

d. Complete an automated USMEPCOM Acceptable Use Policy (AUP). A logon feature is enabled which will prompt each user for a response after inserting their Common Access Card (CAC) and entering their PIN. The prompt will open the AUP for review and require the user to select Yes or No. The login prompts will reoccur annually from the original date of record. If the user selects “Yes”, their agreement will be digitally recorded. If the user selects “No”, the login attempt will be aborted. This process will repeat annually.

e. Safeguard information and information systems from unauthorized or inadvertent modification, disclosure, destruction, or use.

f. Use DoD information systems only for official use and authorized purposes IAW Department of Defense Instruction (DoDI) 8530.01, (Cybersecurity Activities Support to DoD Information Network Operations), and DoD Directive (DoDD) 5500.7-R (Joint Ethics Regulation (JER)).

g. Only access data or use operating systems or programs as authorized.

h. 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.

TOC

i. Not use a non-government email account (e.g., Yahoo, Hotmail, etc.) for USMEPCOM-related business.

j. Use US Government acquired hardware and software for USMEPCOM-related business. Limited personal use of certain Government property as long as it occurs on non-duty time, does not interfere with official business, is not a commercial gain activity or is otherwise prohibited, and the expense to the Government is negligible. Managers may place additional restrictions on the use of Government property for personal purposes only for instances of abuse of this policy or in order to meet management needs and mission objectives.

k. Use of personally owned hardware, software, shareware, or public domain software (such as peer-to-peer software) is prohibited unless approved by J-6/MEIT-CSO ~~RMO~~.

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 IAW current DoD guidance.

o. Submit a waiver request to the J-6/MEIT-CSO ~~RMO~~ 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. Lock the workstation when leaving the immediate work area. Log off the workstation at the end of each working day (do not shut-down).

r. Will not load any executable or program files (e.g., .exe, .com, .vbs, or .bat) onto USMEPCOM information systems. Any software needed for mission accomplishment will be routed via the IMENS process.

s. Will not engage in “streaming” content from audio, visual or data streaming media sources for non-mission related purposes. Such live stream use of the Internet could strain the Command's network and significantly slow communications, inhibiting employees from conducting business.

t. Will not use “push” technology on the Internet or other continuous data streams, unless they are directly associated with the employee's official duties and responsibilities. Push technology from the Internet means daily, hourly or continuous updates via the Internet; e.g., news, stock quotes, weather, and similar information. Continuous data streams could degrade the performance of the entire network.

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, CSO ~~RMO~~, or appropriate local law enforcement officials.

v. Not use USMEPCOM networks or equipment on the Internet for personal gain.

TOC

w. Not visit unauthorized Web sites (i.e., pornographic, gambling, or hate crime sites) while using USMEPCOM networks or equipment.

x. Not write or introduce malicious code (e.g., virus or Trojans) using USMEPCOM networks or equipment.

y. Report all security incidents immediately to their ITS or the J-6/MEIT-CSD-CSB-Service Desk.

z. Not upload any sensitive-but-unclassified or personally identifiable information (PII) data files to Common-shared drive folders on any USMEPCOM IT system.

aa. Will not affix any personal electronic equipment to government workstations, computers, laptops, monitors, or other equipment to power/recharge to non-government equipment such as smartphones. This includes, but not limited to USB connections.

bb. All reachable workstations and laptops will be restarted weekly, either manually by the individual user or automatically via a batch file build in Dameware. In order to ensure the highest success rate and gain compliance with Department of Defense and U.S. Army directives for vulnerability management, and technical controls.

2-9. Safeguarding Sensitive Personally Identifiable Information (PII)

a. Sensitive PII: Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

b. PII that is always sensitive:

(1) Even if NOT coupled with additional PII or contextual information:

(a) Complete (9-digit) SSN

(b) Biometric identifiers (e.g., fingerprint, iris scan, voice print)

(2) When grouped with the person's name or other unique identifier, such as address or phone number, or partial SSN:

(a) Citizenship or immigration status

(b) Medical information

(c) Driver's license number

(d) Passport number

(e) Full date of birth

(f) Mother's maiden name

TOC

(g) Passwords

(h) Financial information such as account numbers

c. Collection: Shall occur only as authorized, for official purposes only, and use must be compatible with notices, such as Privacy Act, System of Records Notice (SORN), Privacy Impact Assessment (PIA), and Privacy Act Statements provided to the individuals from whom the information was collected.

d. Dissemination:

(1) Share only as authorized.

(a) Internal share authorized if recipient's need is related to official duties (need to know).

(b) External sharing authorized if routine use is published in the applicable SORN.

(2) Limit storage of PII on shared drives and folders whenever possible.

(3) Storage on shared drives must be restricted to those with a need to know only.

e. Minimize Proliferation:

(1) Do not create unnecessary or duplicative collections.

(2) Delete or destroy when no longer needed.

(3) When printing, copying, or extracting from a larger dataset, target actions to obtain data only on the specific information and subjects required.

f. Securing:

(1) Ensure PII resides only on government furnished IT equipment.

(2) Ensure recipients have a ‘need to know’.

(3) Email containing Sensitive PII:

(a) Must be digitally signed and encrypted.

(b) Subject line must contain proper markings (For Official Use Only (FOUO) Privacy Sensitive).

(c) Verify recipient email addresses.

(4) Paper documents must be controlled or locked in a secure container when not in use.

(5) Do not mail or courier on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted.

TOC

(6) Do not return failed drives to vendor if the device was ever used to store or process Sensitive PII. Drives must be sanitized, degaussed, or destroyed.

(7) Do not pack laptops or electronic storage devices in checked baggage.

(8) Do not leave laptops or electronic storage devices in a car overnight or in plain sight in a parking lot.

(9) Do not take Sensitive PII home or to any non-USMEPCOM approved worksite unless appropriately secured.

(10) Electronic form must be encrypted when containing Sensitive PII.

(11) If received in an unprotected manner, you must secure it once received.

(12) Remove sensitive PII before forwarding an email unless all recipients have the need to know.

g. Printing and Faxing:

(1) Verify device location prior to sending a document containing PII to the printer.

(2) Pickup copies as soon as they are printed.

(3) Double check fax numbers.

(4) Protect against 'shoulder surfing', eavesdropping, or overhearing so that PII is not to extend beyond the records.

h. Retention: The retention of Sensitive PII is not to extend beyond the records retention schedule or as identified in the applicable SORN or PIA.

i. Disposal: User appropriate destruction techniques to dispose of Sensitive PII (shred, pulp, degauss, incinerate, sanitize).

j. Privacy Incident: A privacy incident is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons, other than authorized users and for an unauthorized purpose, have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both suspected and confirmed incidents, whether intentional or inadvertent, involving PII which raise a reasonable risk of harm.

k. Incident Reporting: Report a Privacy Incident to your Supervisor as soon as it is suspected or confirmed. If your supervisor is unavailable or if there is a potential conflict of interest, report the incident to your Information Assurance Program Manager or Privacy Officer.

(1) Document or maintain records of information and actions relevant to the incident, as it may be required in the privacy incident handling report

TOC

(2) Do not further compromise the information by forwarding when reporting. If/when the compromised PII is needed, you will be given instructions on whether the information needs to be forwarded to someone at USMEPCOM.

TOC

Chapter 3
Life-Cycle Management

3-1. Overview
In accordance with 10 USC 2337, the Command shall issue and maintain comprehensive guidance on life-cycle management and the development and implementation of product support strategies to maximize competition and make the best possible use of available Department of Defense and industry resources at the system, subsystem, and component levels; and maximize value to the Department of Defense by providing the best possible product support outcomes at the lowest operations and support cost. IMENS data will be archived and retained under Record Number 25-1ppp1/400B, "Life Cycle Management of Information Management Systems (Information Mission Elements Need Statement (IMENS))". Keep in local archive until no longer needed for conducting business, not to exceed 6 years. Records will then be placed on physical media and transferred to the Federal Records Center (FRC), the FRC will destroy the records after 25 years.

3-2. Requirement Identification

a. Planning for J-6/MEIT 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 HQ functional proponent, MEPS, or Sector ITS will submit the Automated IMENS form using the PTC ~~PCT~~ 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/MEIT will either approve or disapprove the request. The originator of an IMENS will receive an automated email response if the IMENS is disapproved. At any time 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/MEIT 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/MEIT, the functional proponent that submitted the IMENS may request a review of that decision by the CCSB or CCB.

3-4. Sharing J-6/MEIT Resources
Wherever possible, ITS will satisfy requirements with existing J-6/MEIT resources. To facilitate sharing, the CIO maintains a central record of the description, quantity, application, and location of all J-6/MEIT 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 MEPS, a command-wide buy will be initiated to approve the item for all Sectors and MEPS. J-6/MEIT-CSD 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/MEIT strategic plan.

3-6. Acquiring J-6/MEIT Hardware

a. DoD requirement contracts will satisfy requirements for J-6/MEIT hardware when practical. 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/MEIT-PRO 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/MEIT 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, servers or any other government owned devices.

c. Printers, communications devices (hubs, switches, routers, etc.), fax machines, copiers, telephones, and admin PCs, servers, and terminals will be procured by J-6/MEIT-PRO. The MEPS and Sectors ITSs will submit an Automated IMENS form (see appendix C) for procurement of hardware from the command approved hardware list. J-6/MEIT-PRO 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/MEOP-AD within the automated approval process. J-3/MEOP-AD will analyze the functional requirement supporting the request and, if approved, will recommend approval for processing to J-6/MEIT-PRO.

e. With prior approval from J-6/MEIT-PRO, Sectors, Battalions, and MEPS may locally purchase hardware devices (i.e., A/B switch boxes, cables, and speakers), which are on the J-6/MEIT Approved Hardware List, that are compatible with the operating system of the workstation ~~PC~~; as long as the device does not adversely affect the performance or security of the computer and the network. There will be no local procurements that will change the command approved hardware list or network capabilities of the J-6/MEIT systems in Sectors or MEPS. All hardware device procurements for USMEPCOM will be processed by J-6/MEIT.

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

3-7. Acquiring J-6/MEIT Software

a. The command software manager maintains the official maintains a ~~five~~ four-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.

TOC

(1) Part I: Mandatory COTS software that will be installed on all admin computers in the command.

(2) Part II: COTS and GOTS standard software that can be installed on any admin computer after an IMENS has been approved by J-6/MEIT-PRO.

(3) Part III: Approved software for USMIRS computers.

~~(4) Part IV: Approved software for Meal Check computers.~~

(4) Part IV: Approved software for the EFCS computers.

b. 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/MEIT-PRO 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 MEPS will be processed by J-6/MEIT.

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

d. Each MEPS will submit an automated IMENS form to J-6/MEIT-PRO 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/MEIT-PRO prior to procurement. Depending on funding availability, the COTS software will be purchased and shipped to J-6/MEIT-PRO and then redistributed to the MEPS. A copy of DD Form 250 (Material Inspection and Receiving Report) will be emailed to POC in J-6/MEIT-PRO, not later than 14 working days after receipt of COTS software.

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

3-8. Maintenance Considerations
MEPS and Sectors ITSs will promote preventive maintenance practices for J-6/MEIT (e.g., keeping equipment dust-free, removing debris which accumulates inside printers, ensuring fans are not blocked, etc.) as recommended/required by the manufacturer.

3-9. Excess Hardware and Software

a. Hardware. Identify and report excess hardware resources to J-4/MEFA. ~~IAW INFO-11-08AUG-232 (Logistics Policies and Procedures for Property Accountability Operational Guide) UPDATE 1~~.

b. Software. Disposition of software is IAW AR 25-2, Paragraph 4-18.

3-10. Media Sanitization:
To ensure that all documents, equipment, and machine-readable media containing sensitive data are cleared and sanitized before being released outside of the Department of Defense.

a. Sectors, Battalions, and MEPS shall implement a local media sanitization policy. The policy must

TOC

include a formal process with proper recordkeeping, using the USMEPCOM Form 25-1-7-E USMEPCOM Sanitization Validation Form. USMEPCOM Form 25-1-7-E will be retained under Record Number 25/400B, "General Information Management Correspondence Files - USMEPCOM Form 25-1-7-E". Keep in office file for 2 years, then destroy.

b. Hard Copy (i.e. paper copies) containing sensitive data, not physically transferred to the gaining service as part of the accession packet will be shredded using a security level 4 cross cut shredder.

c. Soft Copy Data (i.e. electronic information) can be contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, phones, mobile computing devices, office equipment, etc. A complete list is provided in National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization (NIST Special Publication 800-88 Revision 1 Guidelines for Media Sanitization). Any media sanitization plan implemented locally must comply with the guidance in NIST Guidelines for Media Sanitization or National Security Agency (NSA) Information Assurance Mitigation Guidance, NSA media destruction guidance.

d. Clear, purge, or destroy media using NIST Guidelines for Media Sanitization or NSA media destruction guidance. These steps must be performed prior to reuse or turn-in.

~~(1) Overwriting - The Universal Purge Tool has been approved and distributed to all MEPS. Use of this program is limited to personnel with proper training.~~

(1) Degaussing - Tapes may be degaussed using a National Security Agency/Central Security Service (NSA/CSS) approved degausser. A degausser designed for magnetic tapes is preferred, however, any degausser able to purge data enough to prevent playback is acceptable.

(2) Incineration - If a MEPS is able to access a licensed incinerator, this meets all destruction requirements. Preparatory steps, such as removing tape from reel or cassette prior to destruction is not mandatory. The service facility may have such requirements.

(3) Shredding- Sensitive information handled by USMEPCOM requires a security level 4 cross-cut shredder. This method meets all destruction requirements. Strip shredders are not authorized for this process. A shredding service facility may have additional requirements.

3-11. Information Technology Asset Management (ITAM)

ITAM satisfies the need for visibility and situational awareness of those IT assets, whether purchased, leased, or developed. ITAM captures standard network operations capabilities, data regarding systems and applications on Army networks, down to individual computers, printers, copiers, workstations, and software licensing. It differs from Property Accountability, in that it documents all IT assets to include databases and applications. Hardware ITAM Workflows are outlined in Figure 3-1; Software ITAM Workflows outlined in Figure 3-2.

a. Office automation. Office equipment includes thin client workstations, desktop personal computers (PCs), servers, notebook computers, hand-held computers, and personal digital assistants (PDAs), copiers and multi-function devices. Peripheral devices include any device designed for use with PCs to facilitate data input, output, and storage, transfer, or support functions such as power, security, or diagnostics.

TOC

b. Network equipment: Network equipment includes chassis, switches, line cards, supervisor engines, routers, firewalls, power supplies, and other components necessary to facilitate data transmission and exchange.

c. System software: System software includes software required for PCs or thin client operations (for example, operating systems). Office automation applications include word processing, spreadsheets, email, task management, graphics, and databases that do not require the greater computational power of special-purpose workstations. System software includes both Commercial off the Shelf (COTS) and Government off the Shelf (GOTS) solutions utilized with USMEPCOM.

d. Enterprise software licenses: The Defense Federal Acquisition Regulation Supplement (DFARS), subpart 208.74, requires DoD components to purchase from the DoD inventory before buying the product from another source. When an activity requires a COTS product, the supporting Chief Information Officer (CIO) will determine if it is available from Computer Hardware Enterprise Software Solution (CHESS), the Army's representative for the DoD Enterprise Software Initiative (ESI). Per DA Pam 25-1-1, Enterprise Software Agreements (ESAs) negotiated with specific software publishers or their agents provide the best available prices, terms, and conditions. USMEPCOM will capture all enterprise software licenses and versioning in its' ITAM program.

e. Leasing IT assets. Requirements for leasing hardware and software will be handled using the same approval and validation procedures as other acquisition strategies.

TOC

Figure 3-1. Hardware ITAM Workflows

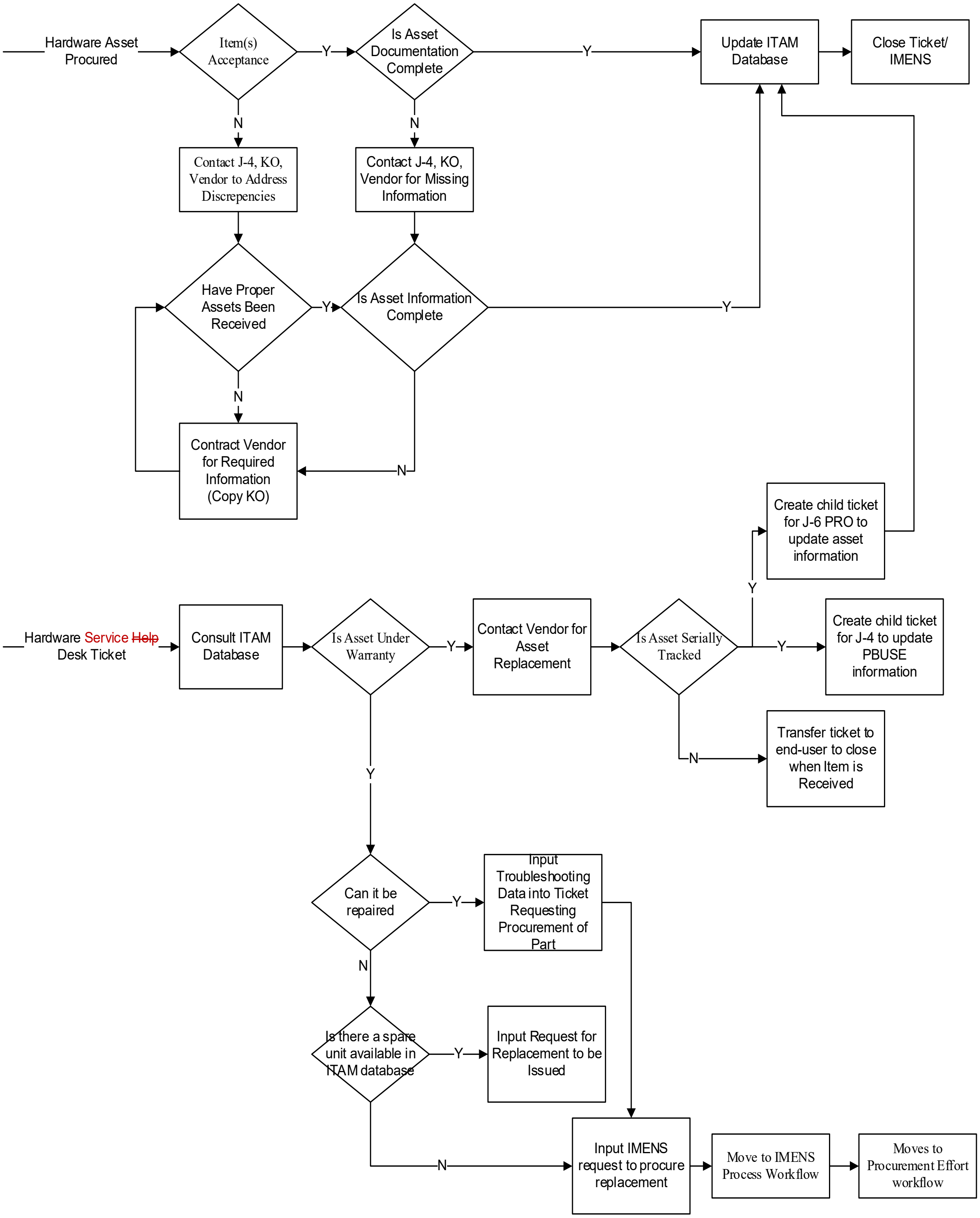

Hardware Asset Procured
Item(s) Acceptance
Y
Is Asset Documentation Complete
Y
Update ITAM Database
Close Ticket/ IMENS
N
Contact J-4, KO, Vendor to Address Discrepencies
N
Contact J-4, KO, Vendor for Missing Information
Have Proper Assets Been Received
Y
Is Asset Information Complete
Y
N
Contract Vendor for Required Information (Copy KO)
N
Create child ticket for J-6 PRO to update asset information
Y
Hardware Service ~~Help~~ Desk Ticket
Consult ITAM Database
Is Asset Under Warranty
Y
Contact Vendor for Asset Replacement
Is Asset Serially Tracked
Y
Create child ticket for J-4 to update PBUSE information
N
Transfer ticket to end-user to close when Item is Received
Y
Can it be repaired
Y
Input Troubleshooting Data into Ticket Requesting Procurement of Part
N
Is there a spare unit available in ITAM database
Y
Input Request for Replacement to be Issued
N
Input IMENS request to procure replacement
Move to IMENS Process Workflow
Moves to Procurement Effort workflow

Figure 3-1. Hardware ITAM Workflows

TOC

Figure 3-2. Software ITAM Workflows

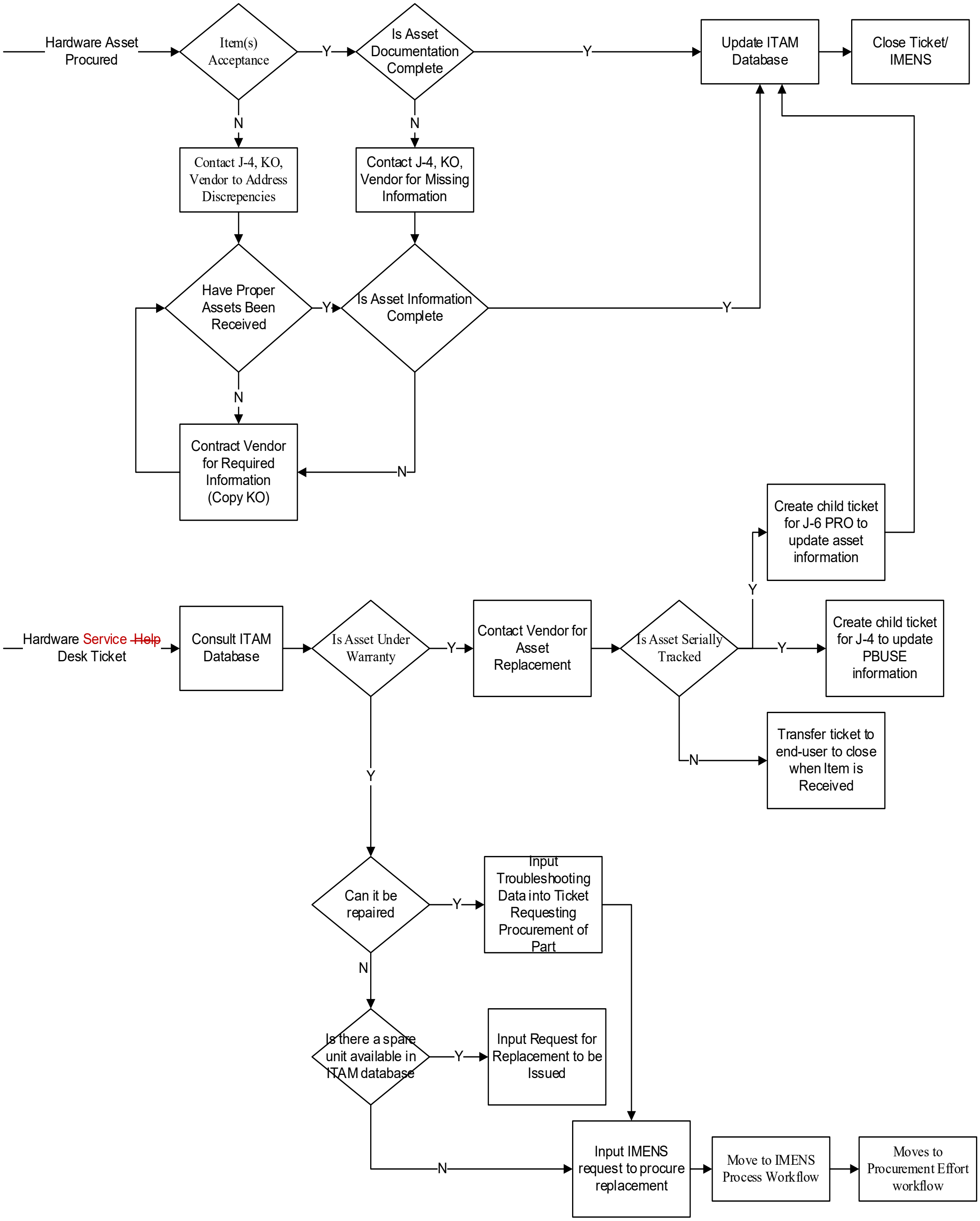

Hardware Asset Procured
Item(s) Acceptance
Y
N
Is Asset Documentation Complete
Y
N
Update ITAM Database
Close Ticket/ IMENS
Contact J-4, KO, Vendor to Address Discrepencies
Contact J-4, KO, Vendor for Missing Information
Have Proper Assets Been Received
Y
N
Is Asset Information Complete
Y
N
Contract Vendor for Required Information (Copy KO)
Create child ticket for J-6 PRO to update asset information
Y
Hardware Service ~~Help~~ Desk Ticket
Consult ITAM Database
Is Asset Under Warranty
Y
Contact Vendor for Asset Replacement
Is Asset Serially Tracked
Y
Create child ticket for J-4 to update PBUSE information
N
Transfer ticket to end-user to close when Item is Received
Y
Can it be repaired
Y
Input Troubleshooting Data into Ticket Requesting Procurement of Part
N
Is there a spare unit available in ITAM database
Y
Input Request for Replacement to be Issued
N
Input IMENS request to procure replacement
Move to IMENS Process Workflow
Moves to Procurement Effort workflow

Figure 3-2. Software ITAM Workflows

TOC

3-12. COR/ACOR Duties and Responsibilities

Contracting Officer Representatives (COR) serve as the eyes and ears of the Contracting Officer (KO) at the contractual place of performance or as otherwise designated by the KO. Alternate Contracting Officer Representative (ACOR) will be assigned in writing by the KO and perform the duties of the COR duties in the COR's absence. Within J-6/MEIT the CORs/ACORs have additional responsibilities beyond those delegated by KO. Standard J-6/MEIT COR/ACOR responsibilities include:

a. Contract Planning (Pre-Award and Solicitation)

(1) Lead requirements definition/acquisition planning and contract formation processes.

(2) Coordinate with J-4 IAW UMR 715-6 as soon as requirement has been assigned.

(3) Populate and maintain Acquisition schedule utilizing standardized J-6/MEIT-PRO Gantt chart to track progress of planning and document creation.

(4) Document any schedule delays or issues and notify management within two (2) business days.

(5) Schedule bi-weekly (at a minimum) requirement development sessions with Division/Branch Chiefs to accurately capture information necessary to draft tasks and deliverables.

(6) Coordinate with Division/Branch Chiefs to identify means and frequency for task/deliverable evaluation criteria.

(7) Coordinate with Division/Branch Chiefs to identify potential skill sets/labor categories and expected workload associated with each task and deliverable.

(8) Create Independent Government Cost Estimate In Accordance With (IAW) standard format identified by servicing Contracting Office.

(9) Perform market research IAW DoD and Army guidelines to identify potential sources for service support.

(10) COR is responsible for completion of all documents listed under the Components of Acquisition Package identified in the document.

(11) Maintain required COR training/COR refresher training to ensure · required training is current.

(12) Provide documented training certifications to external organizations as necessary to obtain/retain COR status

(13) Immediately notify the KO and appropriate COR management if a potential or actual conflict of interest subsequently arises.

(14) Provide documented proof of training completion to the KO before the COR appointment letter is issued.

(15) Maintain file for each contract assigned.

b. Contract Formation (Evaluation and Award)

(1) CORs shall monitor acquisition packages throughout the Contracting Office's timeline through either use of Acquisition Milestone Agreement (AMA) or Contracting Office bi-weekly contract status report.

(a) CORs will notify J-6 leadership within two business days upon determining an AMA milestone has been exceeded.

(b) CORs will notify J-6 leadership within two business days of any changes in acquisition timelines reported in the bi-weekly contract status report.

(2) CORs shall provide support to Contracting Officers and/or Contract Specialist throughout the Contract Formulation phase.

(3) CORs shall respond to Contracting Office correspondence within two business days; at the minimum this response will be acknowledging receipt of the correspondence and will include the date for a complete response to the request.

(4) CORs shall support the establishment of source selection team members and assist the Contracting Office as needed in the source selection process.

(5) CORs shall ensure Office Chief is notified when a follow-on acquisition package has not been awarded 30-days prior the end of the existing period of performance.

(6) Ensure vendors or vendor employees do not have access to information on a particular acquisition before such information is available to the business community at large.

c. Contract Management (Contract Administration: Actions following contract award).

(1) Perform contract surveillance oversight of the contractor's compliance with contract requirements and provide information regarding compliance to the KO.

(2) COR will monitor contract performance IAW applicable Quality Assurance Surveillance Plans (QASP).

(3) Contract issues will be documented in the J-6 Contract Issues log database and management notified whenever a new issue is identified or status of an existing issue changes.

(4) COR shall upload documents into Army Virtual Contracting Enterprise (VCE) per schedule required by Contracting Office or period not to exceed monthly in junction with the monthly report.

(5) The monthly report will be completed and uploaded NLT the 20th of each month.

d. The COR is responsible for obtaining the information necessary to create the Performance Work Statement (PWS), QASP, and other acquisition package documents. The following information must be provided by the operational units whether a current contract exists or an entirely new effort is being undertaken:

TOC

(1) Requirements Definition -What services or products does J-6 need to achieve a successful contracting action?

(2) Acceptable Performance Levels -How well must the vendor perform a specified task?

(3) Historical Manpower Requirements - How many hours has it historically taken to complete a task by complexity level, how many times was each task completed during a given time period?

(4) Expected Manpower Requirements (Level of Effort) - How many times does J-6 expect each task to be performed and associated level of complexity? This will include minimum:

(a) Historical workload per task identified by man-hours expended.

(b) Estimated workload per task identified by man-hour expected.

e. COR/ACOR Training:
A Complete list of training requirement can be found in complete the listed in Army Contracting Command (ACC) Pamphlet 70-1.

(1) The following must complete before the KO issues a letter of appointment.

(a) Overview of Acquisition Ethics (Defense Acquisition University (DAU) course number CLM 003)

(b) COR with a Mission Focus (DAU course number CLC 106)

(c) Contracting Officer Representatives (COR) Training (DAU course number CLC 222)

(d) Invoicing, Receipt, Acceptance and Property Transfer system (iRAPT) (formerly Wide Area Workflow) - https://wawftraining.eb.mil/wawfwbt/

(e) Mission and Installation Contracting Command (MICC) provide Enhanced COR Training (J4 schedules training, typically 2-3 times a year). CORs/ACORs need to be assigned the role and complete the other necessary training first.

(2) Type training requirements listed in ACC Pamphlet 70-1will be allowed 6 months from the issue date of this policy to complete the training.

3-13. Quality Assurance Evaluator (QAE)
The majority of J-6 contracts cross several functional Branches. As such, the corresponding Division/Branch Chief, or designated representative, within J-6 perform the role of QAE.

a. The QAE monitors contractor performance supporting the respective branch is in compliance with contractual requirements, evaluates and documents contractor performance and provides documented acceptance or rejection of deliverables to the COR. Issues with vendor performance shall be submitted to the COR as soon as issues are realized.

b. QAEs shall be nominated by the Division/Branch Chief and the COR will forward QAE nomination to the KO for approval/designation.

TOC

c. The QAE shall notify the COR in writing within two (2) business day of any contractor performance issues.

d. The QAE shall review deliverables IAW applicable QASP and document acceptance or rejection, to include detailed justification to the COR within (3) business days.

3-14. Contract Administration and Monitoring Process (CAMP)

All J-6 personnel involved in the acquisition process for service and support contracts must adhere to CAMP. This includes, but is not limited to, the Contracting Officer Representatives (COR) and Division/Branch/Office Chiefs; as well as any USMEPCOM Headquarters, Sector, Battalion, or MEPS employees who are assigned to provide input into development of contracting requirements. The CAMP is derived from processes outlined in UMR 715-6.

a. Contract Administration

(1) The Federal Acquisition Regulation (FAR) states that the Contracting Officer (KO) is responsible for ensuring performance of all necessary actions for effective contracting, ensuring compliance with the terms of the contract, and safeguarding the interests of the United States in its contractual relationships. To perform these responsibilities, KOs are afforded wide latitude to exercise sound business judgment. The FAR recognizes that the KO may need advice and assistance in areas of audit, law, engineering, information security, transportation, and other fields, as appropriate.

(2) The required organization prescribes contract quality requirements that the contracting office includes in contracts. As experts on the contract requirement, members of the organization are often delegated specific authority from the KO to conduct contract surveillance and to verify that the contractor is fulfilling .contract delivery, quality requirements, and to document performance for the contract record. The organization that coordinates with the contracting office is responsible in developing contract quality assurance, surveillance and performance assessment plans.

(3) The CORs function as the eyes and ears of the KO and liaison between the Government and contractor when executing surveillance responsibilities. However, contract surveillance is not solely the responsibility of the KO and COR. Others may have designated surveillance responsibilities under Parts 42, 45, or 46 of the FAR.

(4) The Defense Federal Acquisition Regulation Supplement (DFARS) 252.201- 7000 defines a COR as "an individual designated in accordance with subsection 201.602-2 of the DFARS and authorized in writing by the KO to perform specific technical and administrative functions".

(5) Contracting is usually carried out in three stages-contract planning (Pre-Award and Solicitation), contract formation (Evaluation and Award), and contract management (Contract Administration). The COR or the COR nominee will be involved in all stages of this process.

(6) Contract administration comprises the activities performed by Government officials after a contract is awarded. It encompasses all dealings between the Government and the contractor, from the award of the contract until the work is completed and accepted by the government, payment is made, any disputes are resolved, and the contract is closed out.

(7) The focus of contract administration is on obtaining supplies and services of the required

TOC

quality, on time and within the expected cost. Although the contract's legal requirements take precedence, the skill and judgment of the KO and COR often are required to protect the government's interests during the contract administration process.

(8) To ensure that the COR performs contract surveillance, it is Department of Defense (DoD) policy that COR management participate in nominating CORs and assessing their performance of COR responsibilities. COR management must also affirm that the COR will be afforded necessary resources (time, equipment, opportunity) to perform designated COR responsibilities.

(9) During the pre-award phase, the COR candidate works with the contracting team in requirements development, preparing the Independent Government Cost Estimate (IGCE), developing the Performance Work Statement (PWS), developing Quality Assurance Surveillance Plans (QASPs), etc. During the post-award phase, the COR shall monitor and assess contractor performance and perform other responsibilities as assigned by the KO. Again, the COR functions as the eyes and ears of the KO.

b. Army Virtual Contracting Enterprise (VCE) Tool

(1) The Army Virtual Contracting Enterprise (VCE) is a web-based capability for the appointment and management of CORs. VCE provides for the collection of COR training certificates and the posting of monthly status reports. VCE provides built in workflows for the nomination process to include email alerts/status reminders for monthly status report due-ins and delinquencies. The VCE tool provides contracting personnel and requiring activities/COR management the means to track and manage COR assignments across multiple contracts DoD-wide. This tool allows a prospective COR, COR management and KO to electronically process the nomination and appointment of CORs for one or multiple contracts.

(2) The VCE Tool is CAC enabled and is available to all DoD personnel with an Army Knowledge Online (AKO) or Defense Knowledge Online (DKO) account.

(3) Your CAC must be registered with AKO/DKO before access to the DoD VCE Tool can be obtained. Files retained by VCE are considered to be the "OFFICIAL" contract file of record.

c. Acquisition Requirements Package Components

(1) Requirements Road map (over $1M)

(2) Performance Work Statement (PWS)

(3) Quality Assurance Surveillance Plan (QASP)

(4) Market Research

(5) Independent Government Cost Estimate (IGCE)

(6) Independent Government Cost Estimate (IGCE) memo

(7) UMF 715-6-1 Acquisition Requirements Checklist

(8) Service Contract Approval (SCA) (over $100k)

(9) Contract Action Justification (CAJ)

(a) Signed by the USMEPCOM Chief of Staff for service requirements up to $100k

(b) Signed by Army G-1 General Officer or equivalent for service requirements over $100k

(10) Copy of the J-1/MEHR Antiterrorism Officer (ATO) or Operations Security (OPSEC) Officer Anti-terrorism Work sheet (J-4 forwards to J-1)

(11) Source Justification Documents (Limited, Sole, Name Brand)

(12) Title 10 U.S.C. Section 2222 statement

(13) Executive Summary (IT Service Contracts over $100k)

(14) Procurement Memo

(15) Minimum two (2) vendor quotes if Computer Hardware Enterprise Software Solutions (CHESS) Request for Quote (RFQ) is available

(16) Minimum three (3) CHESS or GSA vendor quotes are needed if using the Special Purpose “$25K” Government Purchase Card (GPC)

(17) COR Nomination Letter (over $150k) or as determined by the KO

(18) Alternate Contracting Officer's Representative (ACOR) Nomination Letter (as required)

(19) Copies of all COR training certificates

(20) Additional Supporting Documents/Approvals

(a) CHESS Statement of Non-Availability (SONA) if not available from a CHESS vendor

(b) Army G-6 Goal 1 Waiver is required for IT requirements from alternative sources

3-15. COR Contract File

a. VCE and the documents uploaded to the system shall be considered the OFFICIAL COR file. This allows the KO and COR to review the contract, order, and modification documents as needed.

b. The file will be used as a repository for all documents created throughout the entire acquisition process from initiation to closeout.

c. Electronic Contract File Records Management. An electronic contract file will be created for each contract effort. The file will be housed on the J-6 PRO shared drive. A folder "Contracts" will be the mandatory file storage location for all documents relating to each contract effort. The overarching folder structure for each contract will follow the prescribed format approved by the Chief, Plans and Resource Office. At a minimum, a sub-folder will match the reporting requirements listed in the VCE. This electronic file comprises the primary contract support record maintained by J-6. Each COR will ensure

TOC

contracts under their oversight contain complete documentation as prescribed by DoD, Army, and USMEPCOM regulations.

d. Each J-6 COR shall maintain a separate folder for each contract as prescribed below.

(1) Contract

(2) Contract modifications

(3) Invoices

(4) Copies of Deliverables

(5) All correspondence with the Vendor

(6) All correspondence with the Contracting Office

(7) Minutes from Post-award conference and any meetings with the contractor identifying persons present, dates, matters discussed, and actions taken

(8) Approved and accepted plans signed by the KO and/or functional area office

(9) Installation security requirements and vendor employee DD2875 and record of background investigation

(10) All system access requests (authorization and termination of access)

(11) Contractor employee changes

(12) Records of meetings and briefings

(13) Synopses of telephone conversations with the contractor

(14) Documentation of on-site visits

(15) Data, reports, and other documentation furnished by the contractor, including COR's inspection, analysis, and action taken

(16) Interim and final technical reports or other products

(17) Documentation of acceptability/unacceptability of deliverables

(18) QASP information regarding specific performance requirements and the corresponding surveillance methods to assure that they are timely, effective and are delivering the results specified in the contract or task order

(19) Progress schedules approved by the KO

(20) Progress reports submitted by the contractor

TOC

(21) Delinquency Reports

(22) Track projections of funding requirements and costs three months in advance to avoid Anti-Deficiency Act issues

(23) Maintain payment register/payment log that tracks all payments by the Government to ensure that expenditures do not exceed money available

(24) Ensure that payment register balances and the COR file match those in the contracting office file

(25) Maintain copies of all contractor invoices/receipt documents are in the proper format

(26) Maintain an inventory list of all government owned property, validated at least annually

(27) Contractor Performance Assessment Reporting System (CPARS)

TOC

Chapter 4
IT Business Services Division ~~System Development~~

4-1. Overview

J-6/MEIT-IT Business Services Division (J-6/MEIT-BSD) 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/MEIT-BSD-SDB systems analysts, (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/MEIT-BSD-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/MEIT-BSD is responsible for establishing, monitoring and enforcing software-programming standards.

a. New software development requests and changes to existing applications will be submitted as an SCP using the automated PTC ~~PCT~~ tool. See Appendix C for instructions.

b. J-6/MEIT-BSD 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. All IT development projects must follow the appropriate IT Governance processes as established by the USMEPCOM Information Technology Working Group Configuration Control Board (ITWG-CCB), Senior Leader Council (SLC) SOPs and Enterprise Review Board (ERB) Charter. ~~and Enterprise Portfolio Management Board (EPMB)Charter.~~ Development of applications, systems, programs, or any other software coding outside of the approved J-6/MEIT, ITWG-CCB, SLC ~~EPMB~~, or ERB processes is not authorized. Software applications or updates not approved by the ITWG-CCB, SLC ~~EPMB~~, or ERB are not authorized to be loaded to any computer connected to the USMEPCOM network and will be reported to J-6/MEIT-CSO. ~~RMO~~ These systems may constitute or introduce violations of the Certificate of Authority to Operate for all of USMIRS and related subsystems; and may damage the IT Enterprise by not accounting and properly implementing the more than 160 Application Security Technical Implementation Guides (STIGs).

(1) All changes must be presented to, and approved by, the ERB before development can proceed.

(2) Changes that impact USMEPCOM external Service Partners must be submitted 120 days prior to the implementation date and must be approved by the ERB before development can proceed.

(3) Emergency/Urgent changes must be approved by the ERB before development can proceed.

TOC

c. Application Changes will be implemented on the following quarterly schedule. The actual implementation date will be on USMEPCOM established training days when possible.

Figure 4-1. Routine Software Release Schedule

Quarter	**Months**	**Release Month**
1	January – March	March
2	April – June	June
3	July – September	August
4	October – December	December

Figure 4-1. Routine Software Release Schedule

d. Changes implemented outside of the dictated quarterly schedule must be presented to the IT Governance Board for approval for Emergency Release. Emergency/Urgent Releases must be coordinated using the J-6/MEIT Change and Release Management policy and process.

e. Changes that are not considered an emergency and do not meet the requirements to be released will be scheduled for the next Quarterly Release.

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/MEIT-BSD 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, operational field testing, regression testing, performance testing and integration/system testing phases. A controlled test environment is maintained by the J-6/MEIT-BSD-Quality Assurance Branch (J-6/MEIT-BSD-QAB). This reflects the MEPS environment for both hardware and software.

a. Testing of requirement documentation is essential and used to ensure that the requirement documentation is testable.

b. Test planning is the activity that is used to document and communicate to stakeholders, vendors and management with who, what, where and how the testing effort will be conducted. The test plan also includes identifying risk and dependencies associated with the testing effort.

c. Test environment setup review involves verifying that the baseline software is the correct software installed and that all other components are available. The environment setup review also involves ensuring that all software testing tools are installed and properly configured, the test bed is installed and configured and network connectivity is established.

d. Test design techniques are contributors to the success of the testing effort. A good test design can result in efficient test coverage.

TOC

(1) Use of a Requirements Traceability Matrix document is a main stay and is used to document and trace actual requirements to actual test cases. This activity ensures that the requirements are addressed by test cases, this is a component of test coverage.

(2) Test scenario identification and test case preparation is conducted.

(3) Test data identification and preparation is conducted. This activity associates the appropriate test data that will be used during the testing effort.

(4) Peer review of test cases are conducted to ensure that test cases and overall test coverage is complete in form and content. Stakeholders use the Fagan Inspection method to determine whether or not test cases should be approved.

(5) Approved test cases are entered into the test management tool repository.

e. Test execution is conducted and when the test results are captured, reviewed and analyzed. Test results are entered into the defect tracking management repository. If a fail result was encountered the defect tracking management process is initiated, when the test analyst documents a “fail” result by creating and completing a defect template.

f. Defect tracking management process is used to track and documents test cases that when executed do not meet the requirements.

(1) The test analyst collects the completed defect template and enters the information into the defect tracking management tool. The tool assigns a unique defect ID number which is used to track each defect.

(2) Collection of the completed defect template from the test analyst. The completed defect template is updated with the unique defect ID number and submitted to the development or appropriate support team for their review and resolution via email.

(3) The updated defect template information is transferred to a defect tracking log that contains the defect ID number, severity of the defect, initial priority, status of the defect, test case number, summary of the defect, defect detected date, test analyst who discovered the defect, actual requirement associated with the test case, responsible organization, expected resolution date and comments.

(4) Defect tracking meetings are scheduled to discuss and track the status of each defect with the stakeholders, developers, appropriate support team and functional users (J3 and J7). For vendors that are not on site, they are telephonically conference in.

(5) Appropriate defect statuses are open (non-resolved defects), rejected (defects deemed not to be actual defects), closed (resolved defects with a “pass” test result) and hold (defects awaiting a system change proposal to be created).

(6) Appropriate defect severities are severity 1 (show stopper); severity 2 (no workaround is available); severity 3 (work around is available) and severity 4 (cosmetic defect).

(7) System, integration, acceptance and operational field testing efforts must meet the established exit criteria prior to progressing to the next software development lifecycle phase. There must be no open severity 1 defects; no open severity 2 defects; less than 3% of severity 3 defects and less than 4% of severity 4 defects.

(8) Testing reports are created along with the collection of testing metrics.

g. During the acceptance and operational field testing efforts the system/integration testers support those testing efforts by conducting the defect management process and validating whether a defect is an actual defect.

4-5. Release Management

Release Management is the responsibility of J-6/MEIT-BSD. Release management coordinates the many sources involved with a significant release of hardware, software and associated documentation across a distributed environment. Release Management is responsible for planning the rollout of software and hardware, designing and implementing procedures for the distribution and installation of software and hardware components, communicating and managing expectations of the release,

a. Release Planning is the process is used to define the scope and content of Releases. Based on this information, the Release Planning process also develops a schedule for building, testing and deploying the Release. A Release Plan is the document used to provide an overview of the release and identifies components of the release such as the role of stakeholders and participants, communications and schedule dependencies

b. Release Build and Test is the process that is responsible for collecting and assembling release package items based upon the results from the testing effort of each release package item.

c. The Release Package Build is the process used to build the actual package for release, the package contains items such as a summary of the test results, artifacts of the release, documentation including deployment instructions, messaging and communications.

d. Review and reconciliation of the release schedule is conducted with the assistance of Change Management personnel.

e. Release Meeting is conducted in order to determine available release dates, the J6/MEIT Change Management and Release Calendar is consulted and a dateline is proposed, deployment roles are communicated, durations and a deployment timeline is created and a “Go/No Go” decision is made to continue to plan the deployment effort.

f. The Change Management process is initiated when the request for change is submitted along with the collected release information.

g. J6/MEIT Pre-Release Meeting is conducted within 10 days of the scheduled release in order to confirm that the deployment checklist is correct and acceptable, deployment timeline is accepted and that the release communication plan and the release message are reviewed and accepted. This meeting is attended by only J6/MEIT stakeholders. The stakeholders attending this meeting will make a “Go/No Go” decision to continue the release process. If a “No Go” decision is made, the discrepancy that caused the decision is corrected then another meeting is conducted.

TOC

h. ALCON Release Meeting is conducted within 10 days of the scheduled release in order to confirm that the deployment checklist is correct and acceptable, deployment timeline is accepted and that the release communication plan and the release message are reviewed and accepted. This meeting is attended by an expanded group of stakeholders such as J6/MEIT Division Leadership, the Functional user, J3 and J7, Sector ITS and other external stakeholders, as appropriate. The stakeholders attending this meeting will make a “Go/No Go” decision to continue the release process. If a “No Go” decision is made, the discrepancy that caused the decision is corrected then another meeting is conducted.

i. The deployment effort uses a deployment checklist and the instructions contained within the Release Package, to deploy the change into the J6/MEIT enterprise.

(1) Depending on the deployment characteristics, CM and/or SSB will be the lead in the deployment activities.

(2) The deployment activities are validated and the test results are communicated via voice and email.

(3) If the results of the deployment validation procedure indicates a failure the deployment is rolled back (the environment is restored to the state prior to the attempted and failed deployment) after the approval from senior management. Using the rollback instructions contained in the Release Package. The roll back is validated and the test results are communicated via voice and email.

(4) Publishing of the release and deployment activities. According to the Release Communication Plan, RM broadcasts the results of the deployment to the J6 Management, J-6/MEIT-CSD-CSB-Service Desk, J3-MOC, Functional Users (J3 & J7) and external stakeholders.

j. Release categories are:

(1) Major software releases and major hardware upgrades, normally containing large amounts of new functionality, some of which may make intervening fixes to problems redundant. A major upgrade or release usually supersedes all preceding minor upgrades, releases and emergency fixes.

(2) Minor software releases and hardware upgrades, normally containing small enhancements and fixes, some of which may have already been issued as emergency fixes. A minor upgrade or release usually supersedes all preceding emergency fixes.

(3) Emergency software and hardware fixes, normally containing the corrections to a small number of known problems.

4-6. Software Change Management

Software Change Management is the responsibility of J-6/MEIT-BSD. The Software Change Management Process controls all changes made to the USMEPCOM IT Enterprise through standardized and repeatable procedures. This includes confirming there is a business reason behind each change, identifying specific configuration items (CI’s) and identifying production services affected by the change, planning the change, testing the change, and having a back out plan should the change result in an unexpected state to J6/MEIT enterprise.

a. A Change Order is submitted whenever an addition, modification or removal of any network, server, desktop, application and system software occurs. A modification of a production application and

TOC

system software entails actions such as addition of a new application and system software , scheduled maintenance to a network component, server or application software, addition or modification of a network component, server, desktop and printer or retirement of a production network component, server, desktop and printer.

b. A Service Request is defined as a user initiated request for the provision of a new service that is not classed as a change to an existing application or supporting infrastructure. An incident is defined as an unplanned interruption to an IT service or reduction in the quality of an IT service. If an interruption or degradation of service occurs it should be managed in accordance of the vendor's Service Level Agreements (SLA).

c. Problem Reports (PR) are generated when there is an issue with application or process. The PR is assigned to analysis and investigated to resolve the problem. If the PR has a solution the analyst will recommend the generation of a Software Change Proposal (SCP). PRs and SCPs are released on a Quarterly basis.

d. PRs and SCPs Change Orders are entered by the Change Manager upon receipt of the Quarterly Release Development Plan.

(1) The Change Order Deployment Package must be completed.

(2) Configuration Management (CM) will update/upload the Production Release Package to the Change Order. This indicates that the Change has passed SIT and UAT testing and is ready for coordination and release into production.

(3) Supporting documentation must be attached to the Change Order such as the Release Package completed in its entirety, Final Software Submission Form, Test Scripts and resolved defects

e. Change Types defines the level, risk and potential impact of the change request. A risk is measured by the probability of a threat or the vulnerability to the J6/MEIT Enterprise.

(1) Change Type Level 1 represents an Emergency Change. This change indicates that Business Operations may be interrupted or delayed, resulting in financial impact or significant mission to the business.

(2) Change Type Level 2 represents an Urgent Change. This change indicates that Business Operations may be interrupted or delayed, which affects commitments.

(3) Change Type Level 3 represents a Scheduled Change. This change is scheduled within the agreed change window at least 7 days Business Operations may be interrupted or delayed with little impact to commitments.

f. The Change Management Procedure applies to all types of changes related to J6/MEIT. The following is a description of each of the categories of changes that can take place within the J6/MEIT enterprise.

(1) Changes to any application code that is running on or linked to by any hardware or software in the IT environment. These changes are typically made to enhance the function or performance of or to fix a known error in the IT application environment.

TOC

(2) Hardware additions, deletions, reconfigurations, relocations, or preventative or emergency maintenance.

(3) Software product releases, versions, table changes, tuning, alterations to libraries, catalogs, monitors, traps, or changes to priority mechanisms, service packs, security patches, configuration changes such as business rules, and new installations.

(4) Environmental related items such as power maintenance/outages, MEPS relocations or upgrades, UPS system, generators, air conditioning, electrical work, facility maintenance, security systems, fire control systems.

(5) Telecommunications related items such as telephonic upgrades, VOIP, installs, uninstalls, and maintenance.

(6) Network related items such as additions, modifications, lines, routers, network access, controllers, servers, protocol converters, software components either distributed or centralized, rack maintenance, Bitnet tables, and router software.

(7) Operational items such as changes in equipment downtime schedules, planned system outages, changes in delivering services, database maintenance, storage or changes to service levels.

(8) Workstations and Public Clusters items such as Changes in hours of availability, hardware configurations, operating systems, desktop images, utilities, applications including release levels or versions, installations or de-installations of systems.

(9) Security processes covering security policy improvements, such authentications, Security Technical Implementation Guides (STIGs), Information Assurance Vulnerability Alert (IAVAs), DoD and/or Army Mandates.

g. Tier I (J-6/MEIT-CSD-CSB-Service Desk and Monitoring) provides initial Point of Contact for IT related issues providing support to HQ and each of the USMEPCOM 65 MEPS. Resolves issues if possible, if not the issue (s) are escalated to Tier II or III. Which includes MEPS ITS.

(1) Tier I provides basic application software and/or hardware support to callers.

(2) Register and classify received Incidents and to undertake an immediate effort in order to restore a failed IT Service as quickly as possible.

(3) If no ad-hoc solution can be achieved, Tier I will transfer the Incident to expert Technical Support Groups Tier II.

(4) Processes Service Requests and keeps users informed about their Incidents' statuses at set or agreed intervals.

h. Tier II (Operations and Technical Delivery) provides day-to-day operations, maintenance, vulnerabilities management remediation, and limited break/fix solutions.

TOC

(1) Provides more complex support on application software and/or hardware and is usually an escalation of the call from Tier I.

(2) Takes over Incidents which cannot be solved immediately with the means of Tier I.

(3) If necessary, it will request external support, e.g. from software or hardware vendors

(4) The aim is to restore a failed IT Service as quickly as possible.

(5) If no solution can be found, the Tier II representative transfers the Incident to Tier III.

i. Tier III (Engineering and Critical Problem Resolution) is the backend support and final escalation level. Tier III consists of teams comprised of Subject Matter Experts, Senior Engineers and Developers. This tier provides comprehensive research for new issues where know solution do not exist, plan upgrades, migrations and design new implementations

(1) Provides support on complex hardware and operating system software and usually involves certified systems engineers.

(2) Its services are requested by Tier II if required for solving an Incident, typically problems are then generated at this level to continue an ongoing investigation of the incident.

(3) If necessary, it will request external support, e.g. from software or hardware vendors.

(4) The aim is to restore a failed IT Service as quickly as possible.

j. The Change Advisory Broad (CAB) Member attends a mandatory scheduled meeting or sends a representative, and is empowered to make decisions on behalf of the area he or she represents. The CAB may ask participants to take on responsibilities such as a change technical reviewer — a CAB member who provides technical guidance during CAB assessment and authorization stages of one or more change orders. The attendance will be recorded for every meeting.

(1) Participants are CSD Division Chief, BSD Division Chief, CSO ~~RMO~~ Branch Chief (Advisory Member);

(2) All MEIT Branch and Office Chiefs or a qualified representative, excluding Division Chiefs and CSO ~~RMO~~ Branch Chief (Advisory Members);

(3) Eastern Sector & Western Sector ITS Representative; any other MEIT technical representative Subject Matter Experts (SME) () to help clarify a change.

4-7. Process and Product Quality Assurance (PPQA)
PPQA is the responsibility of J-6/MEIT-BSD. This procedure has the responsibility to objectively evaluate processes and work products against actual processes utilized and work products delivered. The team documents non-compliance issues, provide feedback to project staff and management of the results of the evaluation and ensure non-compliance issues are addressed.

a. The PPQA Group develops and documents the PPQA plan in the project plan or as a standalone PPQA Plan.

TOC

b. The PPQA Group establishes and maintains the procedures, checklists, and work aids that describe how PPQA is to be performed.

c. The PPQA Group ensures that resources (tools, databases, work stations, etc.,) for performing the PPQA Process, developing the work products and providing PPQA services are adequate. Tools required to perform the PPQA tasks are identified based on project requirements.

d. The PPQA Group performs the tasks as defined in the project or PPQA Plan. Problems or non-conformances with requirements and standards are documented and reported to the Project Manager or appropriate authority. The PPQA Group communicates the results of PPQA activities to relevant stakeholders for resolution. Senior management addresses non-compliance issues that cannot be resolved within the project.

e. The PPQA Group monitors and controls the day-to-day PPQA activities against the PPQA Plan, schedule and budget. Identify and evaluate the effects of risks on, and significant deviations from, the PPQA plan, schedule and budget. Take corrective action when requirements and objectives are not being satisfied or when progress differs significantly from the plan.

f. The PPQA Group places completed PPQA work products under Software Configuration Management (SCM) in accordance with the project Configuration Management Plan.

g. An objective verifier evaluates the PPQA Group to provide credible assurance that the PPQA Process is implemented as planned, and adheres to its process description, standards and procedures.

h. PPQA activities, status and results are reviewed with the stakeholders, Project Manager and senior management on a periodic and event-driven basis as designated in the PPQA Plan. The PPQA Group escalates unresolved or non-compliance issues and resolves them as necessary.

4-8. 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 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 8320.02 (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.

4-9. 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/MEIT-BSD developed or supported electronic data transfer requirements and provides technical expertise in support of the J-6/MEIT-CSD-CSB-Service Desk and all users of J-6/MEIT-BSD systems. It implements all completed software systems/changes, software configuration management for all J-6/MEIT-BSD developed/maintained software, and provides one-time special ad-hoc reporting requirements technical support, that cannot be supported by J-5/Strategic Planning & Transformation (MEPT) using USMEPCOM Business Intelligence System (UBIS).

TOC

4-10. Documentation

Software application developers will document changes within the code following Application Development and User Interface Standards. Change documents will be developed for all USMIRS application releases. User manual documentation or online help will be updated and available for all applications to assist the user in using applications.

4-11. Software Configuration Management (SCM)

SCM is the responsibility of J-6/MEIT-BSD. These procedures ensure proper maintenance and effective tracking of the configuration management process of base-line applications software for all systems/platforms. This function includes version identification, development and production software library maintenance. Users at HQ USMEPCOM, Sectors, or MEPS will utilize PR submitted to SCM, via automated Software Configuration Management System (SCMS) tool, for fielded software problems identified. In addition, SCM will be utilized for SCP submissions. SCM establishes and maintains the integrity of the products of a project throughout the project life cycle. SCM involves identifying the configuration of products that are delivered to the customer and used in development, systematically controlling changes to the configuration, and maintaining the traceability of configuration items.

a. The SCM Group documents the Software Configuration Management Plan (SCMP) as part of the Project Plan or as a standalone Configuration Management Plan. The plan includes the purpose of SCM; governing standards; SCM organization, roles, and responsibilities; Configuration Items (CIs); control boards; and CM functions, activities, tools, and procedures.

b. The SCM Group is responsible for the implementation of the Software Configuration Management Plan by developing the procedures and performing the SCM activities detailed in the SCMP including the resolution of SCM deficiency issues.

c. The SCM Group places configuration items and applicable technical artifacts in CM libraries to maintain the integrity of the products throughout the life cycle. The CM group establishes baselines and delivers releases and associated changes to authorized baselines.

d. The SCM Group produces Configuration Status Accounting (CSA) reports to provide visibility into the status of baselines. CSA reports are developed periodically or in event-driven to address status and history of controlled products, approved identification numbers, library and baseline contents, CCB decisions, and SCM deficiencies.

e. The SCM Group performs Functional Configuration Audits (FCA) and Physical Configuration Audits (PCA).

(1) Functional Configuration Audit activities and processes to confirm that the resulting baselines and documentations are accurate, and record the audit results as appropriate.

(2) A Physical Configuration Audit is performed to verify that every delivery item (e.g., program input file, test software, or document) is as reported in the delivery documentation and release letter. Each item is checked to ensure that the item is present, is complete, is the correct version, is in the specified delivery format, and is correctly identified.

f. The SCM Group reviews and reports to higher-level management the activities, results, and overall status of this process.

TOC

4-12. Command Enterprise Web Development

J-6/MEIT-BSD will develop, maintain, and coordinate the command's Enterprise Web strategy and architecture ensuring it aligns with the J-6/MEIT Strategic Plan. Development and maintenance of the command's intranet (SPEAR) and internet sites will be done IAW AR 25-1, chapter 4.

4-13. 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.

~~4-14. Authorized Users~~

~~a. Only government civilian employees, military service members, and contract personnel shall have access to government automated resources. Applicants shall only be granted supervised access for the purpose of completing official processing functions (e.g. in CAT-ASVAB testing, Defense Language Proficiency Test (DLPT), Red Carpet Survey).~~

~~b. All Users will assure that USMEPCOM systems and data are safe and secure from unauthorized access that might lead to the alteration, damage, or destruction of automated resources and data, unintended release of data, and denial of service.~~

~~c Users will remove their CAC card from when the computer is left unattended.~~

~~d. The USMEPCOM J-6/MEIT-CSD-CSB-Service Desk serves as a focal point for incident reporting and subsequent resolution. All incidents will be handled in accordance with the J-6/MEIT Incident Response Plan located on the J-6 Risk Management & Compliance Office SPEAR page.~~

TOC

Chapter 5
USMEPCOM Data Communications Networks

5-1. Overview

J-6/MEIT-CSD-Enterprise Network Branch (ENB) will be responsible for all aspects of the network equipment/devices, ~~servers/appliances~~ the Local Area Networks (LANs), Wide Area Network (WAN), Unified Communication Platform (UC), and data communication connectivity between each MEPS, Sector, Battalion and HQ USMEPCOM. These networks are designed for Controlled Unclassified Information (CUI) 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/MEIT-CSD-ENB is also responsible for all network ~~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/MEIT-CSD-ENB and J-6/MEIT-CSO ~~RMO~~.

5-3. Network Design

J-6/MEIT-EA~~O~~, J-6/MEIT-CSD-ENB, and J-6/MEIT-CSD-EDC will be responsible for the design of the Networks used in MEPS, Sectors, Battalions and HQ USMEPCOM. Any changes to the design will be approved by J-6/MEIT-EA~~O,~~ J-6/MEIT-CSD-ENB, J-6/MEIT-CSD-EDC and J-6/MEIT-CSO ~~RMO~~.

5-4. Network Installation

J-6/MEIT-CSD-ENB will be responsible for the installation of network equipment including Enterprise switches, hubs, routers, servers, wireless equipment, UC devices, patch panels, and network drops. J-6/MEIT-CSD-ENB will approve anyone else installing any network equipment in MEPS, Sectors, and HQ USMEPCOM including other service contractors. Only devices authorized for use on a USMEPCOM network will be connected to the network.

5-5. Network Operations

J-6/MEIT-CSD-ENB will be responsible for the network operation in all MEPS, Sectors, and HQ USMEPCOM. J-6/MEIT-CSD-ENB may restrict or allow MEPS personnel to access certain network equipment. J-6/MEIT-CSD-ENB with J-6/MEIT-EA~~O~~ and J-6/MEIT-CSO ~~RMO~~ establishes guidelines, standards, policies, and procedures for effective LAN and WAN operations. J-6/MEIT-CSD-ENB controls and coordinates installation and maintenance of computer network resources. J-6/MEIT-CSD-ENB oversees the planning, installation, operation, and maintenance of command-wide data communications network servicing all levels of USMEPCOM. J-6/MEIT-BSD-QAB is responsible for configuration management, performance analysis, and fault analysis of all network components. J-6/MEIT-CSD-ENB with J-6/MEIT-EA~~O~~ and J-6/MEIT-CSO ~~RMO~~ 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. J-6/MEIT-CSD-ENB will ensure the security of the network by following Information Assurance Vulnerability Alert (IAVAs), Defense Information Systems Agency (DISA) Security Technical Implementation Guides, or "STIGs." Or any vulnerabilities directed from J-6/MEIT-CSO.

5-6. Network Management
J-6/MEIT-CSD-ENB will be responsible for managing all the USMEPCOM networks. J-6/MEIT-CSD-ENB 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; provide input for network administration policy and guidance; and architecture and standards policy to J-6/MEIT-CSO.

c. J-6/MEIT-CSD-ENB will be responsible for all integration efforts onto the communications backbones and departmental Virtual LANs (VLAN) 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.

5-7. Network Documentation
J-6/MEIT-CSD-ENB will be responsible for the overall network documentation and architectural plans. MEPS ITSs are required to maintain a Network Documentation will be retained under Record Number 25-1jjjj2/400B, "Enterprise Architecture Records". Keep in office file until no longer needed for conducting business, not to exceed 7 years, then destroy. Records may be transferred to the FRC after 5 years, the FRC will destroy the records after 7 years. Responsibilities will include, but is not limited to:

a. Create 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. Track Internet Protocol (IP) addresses used in the MEPS (in spreadsheet format):

Figure 5-1. Network Map Example:

Device Name	4th IP Octet	Location in MEPS	Additional Information
MEPCOM-PR-MIT26	xxx.xxx.xxx.123	HRA Office	Shared Printer
USMEPCOM-NB-IT215	xxx.xxx.xxx.456	Commander Office	Notebook

Figure 5-1. Network Map (Example)

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

TOC

5-8. 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/MEIT-CSD-ENB 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 email, USMIRS, CAT-ASVAB, or World-Wide Web (WWW) access will comply with the standards established by J-6/MEIT-CSD-ENB. 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.

5-9. Networks, Computer, and Peripheral Maintenance

J-6/MEIT-CSD-ENB 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/MEIT-CSD-CSB-Service Desk.

5-10. Equipment Warranties

J-6/MEIT-CSD-ENB 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 MEPS, 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/MEIT-CSD-ENB.

5-11. 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/MEIT-CSD-ENB will attempt to minimize unscheduled network equipment outages.

5-12. Access to USMEPCOM Networks, Devices, and Services

Each user requiring access to the network will have a signed DD 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 on page 3 of the DD Form 2875. J-6/MEIT-CSD-ENB will maintain access forms for USMEPCOM. Each year this form will be reviewed and updated. J-6/MEIT-CSD-ENB is responsible for the management of passwords, logins, and email accounts IAW Paragraph 2-7 and AR 25-2.

5-13. User and Information Technology Specialist's Responsibilities

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

5-14 Enterprise Email (DEE) USMEPCOM Email system

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

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

b. Users will not transmit classified information over the DEE or network. Any email or email attachment containing Personal Identifiable Information (PII), Personal Health Information (PHI), Internet Protocol (IP) addresses, hostnames, passwords, or other information which would provide an individual information to penetrate the infrastructure must be Digitally Signed and Encrypted prior to sending.

c. Users will only utilize the USMEPCOM provided email system to send and receive email on USMEPCOM provided computers or Mobile Devices ~~Blackberries~~.

d. User will not forward meeting invites or official email to a commercial service provider (Comcast, AOL, Gmail, Yahoo, etc.) or private email server or network.

e. All USMEPCOM employees and contractors will use the Standard Signature Block and disclaimer when sending all emails. The Standard Signature Block will be Times New Roman, 11 pt and will use the following in Figure 5-2. The only approved variance to the standard USMEPCOM disclaimer has been granted to the Inspector General Office.

Figure 5-2. USMEPCOM Standard Signature Block

Very Respectfully,

Name
Title (optional), Directorate/Branch, Office, MEPS, Sector, or Battalion
Email Address
Office Telephone Number
Government Cell or ~~Blackberry~~Mobile Device Number (if applicable)

DISCLAIMER:
The information contained in this communication is intended for the sole use of the named addressees/recipients to whom it is addressed. This communication may contain information that is exempt from disclosure under the Freedom of Information Act, 5 U.S.C. 552 and the Privacy Act, 5 U.S.C.552a.

Addressees/recipients are not to disseminate this communication to individuals other than those who have an official need to know. If you received this communication in error, please do not examine, review, print, copy, forward, disseminate, or otherwise use the information. Please immediately notify the sender and delete the copy received.

Figure 5-2. USMEPCOM Standard Signature Block

f. Employees will not add slogans, quotes, tag lines, special backgrounds, special stationeries, digital images, emoticons, or unusual fonts to the body of their electronic messages or signature blocks. When sending an email, use proper email etiquette and address recipients with appropriate courtesies based upon rank and position.

g. All messages should contain a complimentary Salutation (or greeting), e.g. “Dear”, “Good Morning”, etc.; and closings to messages, e.g., “Very Respectfully,” “Sincerely,” or “Regards,” etc. should be businesslike and professional in nature.

TOC

h. Employees shall refrain from including in any official email message a greeting, closing, or remark that a reasonable person might find offensive based on race, sex, color, national origin, religion, disability, sexual orientation, or age.

i. A User Guide to assist in creating a signature block in Outlook 2013 and on Blackberry devices can be obtained by contacting the USMEPCOM J-6/MEIT-CSD-CSB-Service Desk.

j. Emails will be digitally signed using an approved DoD PKI certificate to a .mil address recipient when:

(1) An active (embedded) hyperlink is inserted, or

(2) The email contains an attachment

k. Emails will be digitally signed and encrypted using an approved DoD PKI certificate to a .mil address recipient when:

(1) Enclosing Personal Identifiable Information (PII), or

(2) Enclosing sensitive IP addresses, host names, passwords, or other information which should provide an individual information to penetrate the infrastructure.

l. Mobile Device ~~Blackberry~~ Users shall not send messages which require a digital signature unless configured for PureBred. ~~using a DISA approved CAC Sled or soft certificate~~

m. Users may configure systems to automatically digitally sign or encrypt email.

5-15. Nongovernmental email System

Email services such as "Hotmail," "Yahoo mail," "Excite mail," "AOL," etc., are not to be used for official government email. These email services are not approved methods for transmitting work-related email and will not be supported. These systems are outside the control of HQ USMEPCOM, Sectors, Battalions, and MEPS personnel and security measures which do not provide proper security, virus scanning, and backup capabilities.

5-16. Assistance and Problem Resolution

HQ USMEPCOM, Sectors, Battalions, and MEPS 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/MEIT-CSD-CSB-Service 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 Service owned equipment should contact their respective recruiting service for instructions.

5-17. Other Networks

a. J-6/MEIT-CSD-ENB is responsible for coordinating access and providing appropriate security for other networks including access to the Internet and USMEPCOM Intranet and Extranets.

b. Army funds may not be used to acquire non-government Internet access and Wi-Fi. Funding for non-government Internet access and wireless is managed by Morale, Welfare and Recreation (MWR). Television cable contracts will not be utilized to attempt to provide "free" Internet access through the use of bundling or a bill showing no charge for Internet. Prior to installation, a request for approval to install MWR or non-appropriated funded wireless service must be made, in writing, through the HQ USMEPCOM J-6/MEIT-CSO ~~RMO~~ (Cyber Security ~~Risk Management and Compliance~~ Office) by completing the questionnaire located at Appendix H. A copy of the request, signed by the USMEPCOM Designated Approval Authority (DAA), will be kept on file.

c. The following procedures must be followed for non-government use of a commercial Internet connection and wireless access:

(1) A request for approval to install MWR or non-appropriated funded wireless service must be made through the HQ USMEPCOM J-6/MEIT- Cyber Security ~~Risk Management and Compliance~~ Office (CSO ~~RMO~~) by completing the attached questionnaire and:

(a) The request must include documentation from the MEPS ITS describing the architecture and equipment utilized to provide wireless Internet access.

(b) The request must be approved by the MEPS, Battalion, and Sector Commanders prior to submission to J-6/MEIT-CSO ~~RMO~~.

(2) The utilization of Wi-Fi at the MEPS for non-government use must be approved by the USMEPCOM Authorizing Official prior to installation of non-appropriated funds Wi-Fi.

5-18. Additional Network Services

All USMEPCOM employees, MEPS Service Liaisons, Government Contractors, and guest users accessing the USMEPCOM enterprise network will follow the below procedures for requesting additional USMEPCOM and non-USMEPCOM IT network services.

a. All requests for USMEPCOM IT network services over and above standard, already installed, USMEPCOM/MEPS network services shall be requested via J-6/MEIT. No work such as installation, implementation, activation, porting of phones, or any other related work may commence without clear authorization and direction from the Chain of Command. This includes, but is not limited to, wireless networks, hot spots, network equipment, routers, switches, telephones, or new data connections from a non-USMEPCOM source.

b. Requests must be initiated and submitted by the local MEPS Information Technology Specialist to the J-6/MEIT Service Desk via the Service Desk ticketing system. Once J-6/MEIT receives the request, technical staff(s) will perform appropriate analysis to determine feasibility, IT security, infrastructure impact, architecture impact, support requirements, and financial impact. Any further coordination action by J-6/MEIT with the requestor's Chain of Command will be based upon nature of the request.

5-19. Internet Access and Monitoring

a. J-6/MEIT-CSD-ENB is responsible for coordinating and monitoring access to the Internet including access to the military portion known as the NIPRNET.

b. J-6/MEIT-CSO ~~RMO~~ may gather information IAW AR 25-2, if an employee's usage of the Internet is questioned. USMEPCOM, Sectors, Battalions, or MEPS 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/MEIT-CSO ~~RMO~~ will direct requests for monitoring to the Staff Judge Advocate/MEJA 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. User access and website logs will be retained under Record Number 25-1ggggg/400B, "Website and User Access Logs". Keep in office file for 3 years, then destroy.

5-20. Intranets and Extranets

J-6/MEIT-CSD-ENB is responsible for maintaining Web servers that are accessed across the Internet. SPEAR is the current USMEPCOM intranet site. J-6/MEIT-CSD-ENB is responsible for USMEPCOM extranets.

5-21. External Accesses to USMEPCOM Network

J-6/MEIT-CSD-ENB 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 (ISSM) ~~(IAM)~~.

5-22. Portable Electronic Device (PED) and Commercial Mobile Device (CMD)

Portable Electronic Devices (PEDs) and Commercial Mobile Devices (CMDs) are defined in DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG) and AR 25-2 as portable Information Systems (IS) or government owned and issued ("Government") PEDs, as well as personally owned ("personal") devices with the capability of wireless or LAN connectivity. PEDs include CMDs and devices with photographic, audio/video recording, and/or are web enabled. These include, but are not limited to: cellular/personal communication system devices, audio/video/data recording or playback devices, scanning devices, remote sensors, messaging devices, Personal Digital Assistants (PDAs) (for example, Blackberries, Palm Pilots, Pocket PCs), two-way radios, cameras, web cameras, and tablets. Failure to comply may lead to disciplinary action under the Uniform Code of Military Justice (UCMJ) or AR 690-700, Personnel Relations and Services (General), Chapter 751, Table 1 -1: "Table of Penalties for Various Offenses", as appropriate.

a. Authorized Devices: Only government PEDs may be used to process, store and transmit government business. PEDs issued and approved by USMEPCOM shall have documentation that the PED is approved by the Cyber Security ~~Risk Management~~ Office (CSO ~~RMO~~).

(1) Non-Enterprise-Connected Devices: A non-enterprise-connected device is defined as a PED that does not connect to a DoD network and is only authorized to store publicly releasable information.

(2) Lost/Stolen Devices: Individuals arc to report lost or stolen government PEDs to both their supervisor and the CSO ~~RMO~~ immediately. Supervisors must initiate appropriate property accountability actions in accordance with USMEPCOM Property Book Standard Operating Procedures (SOP).

(3) Authorized Use: USMEPCOM Acceptable Use Policy, as well as the rules in DoDD 5500.7 and UMR 27-2, Legal Services Ethics, regarding use of government communication systems, apply to government PEDs. Misuse shall be reported to an individual's supervisor and local Information Assurance Support Officer or the CSO ~~RMO~~.

b. Personally Owned Devices: Use of personal PEDs for official USMEPCOM business must be requested through their supervisory chain and approved by the CSO ~~RMO~~. Employees should not expect reimbursement for the use of PEDs for government business. Employees must also comply with the rules

TOC

set forth in DoDD 5500.7 and UMR 27-2, Ethics regarding conducting personal business while at work or on government time with respect to their personal PED use.

c. Restricted Areas: Testing rooms and medical exam rooms, due to sensitive operations and protection of individual's privacy, are defined as restricted areas. Bathrooms are also considered restricted areas when being used to conduct urinalysis testing. Personal and government PEDs are not authorized to enter into restricted areas.

(1) Only government devices approved by MEMD/J-7 and the MEIT/J-6 CSO ~~RMO~~ used by the MEPS medical staff for the purpose of capturing dermatology photographs (i.e. tattoos, scars, etc.) are exempt.

(2) The Director and staff of the Facilities and Acquisitions Directorate MEFA/J-4, may use government portable electronic devices (PEDs) in all areas of the MEPS for documenting items of legitimate interest. This exception specifically allows government PED use in testing and medical examination rooms when applicants are not present.

d. Restricted Use: Due to operations and privacy, it is USMEPCOM policy that:

(l) At no time may non-enterprise-connected devices and personally owned PEDs be used to process, store or transmit "For Official Use Only" (FOUO) or Personally Identifiable Information (PII) or Protected Health Information.

(2) At no time may PEDs be in use by the operator of a Government Owned Vehicle (POV), unless the vehicle is safely parked or a hands-free device is being used.

5-23. Social Media

Use of Social Media for official purposes is governed by MEDC-PA and is addressed in UMR 360-1 and its associated policy memoranda.

5-24. Wireless Local Area Network (WLAN)

a. Wireless Local Area Networks (WLAN) are to be implemented, managed, configured, and utilized throughout the USMEPCOM Network Infrastructure or DAN in a secure manner in accordance with DoDI 8420.01, DoDD 8100.02, DoDI 8510.01, NIST-SP 800-53, and NIST-SP 800-53A in order to be authorized for use while connected to the Department of Defense Information Network (DoDIN).

b. WLAN Installation.

(1) During installation, the Wireless Access Points (APs) must be configured to ensure radio frequency does not impede other wireless devices or leave the authorized area.

(2) Radio frequencies must not extend into classified areas.

(3) Wireless APs and authorized areas must be clearly defined and documented for each facility, floor, and room through active and passive site surveys.

TOC

(4) Wireless APs must be installed in a secure area, to avoid tampering, reconfiguration, or reset of existing configurations. For example, this can be achieved by securing within a lock box, installation in a secured building or facility where access is permitted only by authorized personnel.

(5) Wireless APs, appliances, and switches must be logically separated from other data paths IAW NIST-SP 800-53.

(6) Wireless APs shall be installed in accordance with building and safety codes.

c. WLAN Configuration

(1) All wireless must be configured with Federal Information Processing Standards (FIPS)-140-2 encryption IAW DoDI 8420.01.

(2) Operating systems must be updated IAW NIST-SP 800-53.

(3) Service Set Identifier (SSID)s shall be configured in accordance with DISA STIGs and configured not to broadcast its network name.

(4) Wireless APs shall be configured to permit only authorized devices, which constitutes a pre-authorized list of government furnished mobile devices, such as laptops, tablets, and phones. Non-government laptops, tablets, and phones are not authorized to connect to the government Wireless AP.

TOC

Chapter 6
Service Desk

6-1. Service Desk

Provides a single POC for all J-6/MEIT supported services and equipment within USMEPCOM. This encompasses all technical assistance and problem resolution for systems and software applications, including service interfaces, computers, email, Web, LAN, WAN and components of the communications infrastructure. J-6/MEIT-CSD-CSB-Service Desk processes all requests received from MEPS, Battalions, Sectors and HQ USMEPCOM and facilitates J-6/MEIT-CSD-CSB-Service Desk problem determination and resolution.

6-2. Service Desk Operations

J-6/MEIT-CSD-CSB-Service Desk operational hours and procedures are based on USMEPCOM priorities and resources. Requirements for additional support should be emailed to the Director, J-6/MEIT ~~CSD-CSB-Service Desk~~ at least one week in advance. Current hours of operation are 0330 – 1800, Monday – Friday, excluding Federal holidays. In the event of a Saturday processing day (“Saturday Opening”) the Service Desk will be manned during coordinated processing hours. These hours may be adjusted to accommodate exceptional circumstances or to facilitate changes in support requirements. USMEPCOM functional experts are available ON CALL, for software problem resolution and additional assistance on mission days. On call support hours are subject to change to accommodate exceptional circumstances such as furloughs. Credit, Compensatory, Over Time for the Service Desk is not authorized without the prior approval of the Director, J-6/MEIT.

a. J-6/MEIT-CSD-CSB-Service 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/MEIT-CSD-CSB-Service 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/MEIT-CSD-CSB-Service Desk personnel after a trouble ticket has been submitted. No equipment will be moved or replaced without coordination and the approval of J-4/MEFA-Logistics Branch (ADL).

(2) Technical assistance for J-6/MEIT systems/applications (e.g., workstations ~~PC~~, applications, USMIRS and the USMIRS Family of systems (CAT-ASVAB, Personal Digital Assistant (PDAs) used to generate ASVAB QuickScores, Electronic Fingerprint Capture System (EFCS), eSecurity, HIV/DAT, Travel Orders, Meal Check, etc.)

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

(4) Email issues.

(5) RSN outages reported and status tracked with United States Army Human Resources Command (HRC).

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

TOC

(7) Functional or policy inquiries will be directed to J-3/Operations Directorate-Operations Center ("MOC" J-3/MEOP-COO).

6-3. Requests for Assistance and Reporting Problems

The ITS will notify J-6/MEIT-CSD-CSB-Service 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/MEIT-CSD-CSB-Service Desk management system is used to log all entries and provide reports. The user or the ITS will submit a CA ticket for all issues.

6-4. Managing Assistance and Problems

Each ITS will assist the J-6/MEIT-CSD-CSB-Service Desk personnel in resolving problems and notify the J-6/MEIT-CSD-CSB-Service 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/MEIT-CSD-CSB-Service Desk provides inaccurate information to decision makers and wastes USMEPCOM resources.

TOC

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 IAW DA Pamphlet 25-1-1, chapter 2-9.

7-2. Command Software Manager
J-6/MEIT-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 Computers
Software, whether COTS, GOTS, USMEPCOM-unique applications or programs, residing on USMEPCOM-owned computers require an approved IMENS submission prior to software installation. USMEPCOM-owned computers will be subject to annual audits. Contracted personnel employed by USMEPCOM may install or retain on government computers (both workstations and laptops) software purchased or supplied by the sponsor company only after obtaining written permission from J-6/MEIT. In the situation of software being mailed or delivered to USMEPCOM in the contractor's name, J-6/MEIT-PRO will be advised prior to delivery.

7-4. Screensavers
Screensaver programs other than those that come with the computer's operating system, 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 an ITS, 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 20 MB (megabytes) 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 Sector, Battalion and MEPS ITS will secure all original software media.

TOC

7-8. End-User Training

J-6/MEIT-CSD, in coordination with the J-1/Human Resources Directorate-Workforce Development, Training, and Conferences ~~Training Development~~ Division (J-1/MEHR-WTC ~~TR~~), is responsible for coordinating and providing initial computer training for end-users. Users are encouraged to view the tutorials provided with the computer, as well as COTS software manuals. Before using J-6/MEIT hardware, personnel will receive introductory training to ensure users properly and safely operate their system. The MEPS and Sectors ITS will provide initial introductory computer training at their level. Follow-up training will be accomplished as priorities and requirements in the command change. USMIRS Users are responsible for reviewing the Training Standardization Job Task Sheets associated with their position located on the J-1/MEHR-WTC ~~TR~~ SPEAR page.

TOC

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/MEIT-PRO and J-6/MEIT-CSD-ENB 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/MEIT-CSD-ENB no later than 7 working days following the appointment. The TCCO is responsible for the administration of the telecommunications program within Sectors, Battalions and MEPS.

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. Personal calls made during duty hours must not adversely affect the performance of an employee's official duties or the organization's work performance, and must be of reasonable duration and frequency.

8-4. Request for Telecommunications Services

Requests for telecommunications services and facsimile (FAX) machines, outlined in Appendix D, will be processed through the local TCCO. The TCCO in turn will submit their requirements through their respective Sector to J-6/MEIT-CSD-CSB-Service 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/MEIT-CSD-CSB-Service 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/MEIT-CSD-ENB are authorized to issue the DD Form 1367 (Commercial Communications Work Order) and requests for Communications Service Authorizations (CSAs) for HQ USMEPCOM, Sectors, and MEPS. 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 J-6/MEIT- PRO. 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 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

a. MEPS receive telecommunication service from either the Hosting Installation or a USMEPCOM-procured contract. Telephone bills received at MEPS are informational only, may differ from contractual agreements, or invoiced costs, and are not to be paid by the MEPS. HQ USMEPCOM personnel are responsible for inspecting and accepting phone company invoices for payment which must be submitted through Wide-Area-Work Flow (WAWF). The contracted costs shall be considered as total allowable billing by the vendor.

b. The J-6/MEIT-PRO Contracting Officer Representative (COR) shall be notified if unauthorized services were received. Phone calls must be for official purposes only. HQ USMEPCOM J6 MEIT personnel may work with telecommunications providers to verify services provided, and identify unauthorized use of telephone services. The purpose of verification is to collect payment from those personnel making unauthorized calls.

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 Verizon Communications or other competitively awarded government contract through General Services Administration (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. Multi-Functional Devices (MFDs)
HQ USMEPCOM, Sectors, and MEPS have Multi-Functional devices which allow 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.

TOC

8-13. Headquarters Public Branch Exchange Phone Systems
All additions, changes, and deletions to HQ USMEPCOM, Sectors, Battalions and MEPS public branch exchange (PBX) telephone systems will be submitted to J-6/MEIT-CSD-CSB-Service Desk either by generating an in-house service desk ~~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

a. Mobile devices will be used only when conventional telephones are not available, or use of the mobile device is more cost effective for the Government (i.e., local toll areas are already included in the wireless communications contract). Mobile devices 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 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/MERM in coordination with J-6/MEIT-PRO and J-6/MEIT-CSD-ENB. The use of a J-6/MEIT calling card or its number is a much more cost effective method and saves the command dollars.

b. USMEPCOM provides wireless communications services in support of Mission related activities. Wireless communications usage should be based upon operational need that supports USMEPCOM's Mission and complies with government rules and regulations. Mobile wireless devices are intended for official Government business only.

(1) Individual Responsibilities:

(a) Compliance with applicable regulations, ethics, procedures, DoD, and USMEPCOM policies.

(b) All users are required to maintain proper security, control, handling, and storage of classified and unclassified information.

(c) Users will not use the Internet for personal gain at any time. Do not visit unauthorized websites (i.e., pornographic, gambling, or hate crime sites). Acceptable use only. (See Appendix I: USMEPCOM Acceptable Use Policy)

(d) The ~~air card/~~hotspot is considered the employee's "personal responsibility" as set forth in AR 735-5. It is Government property and all persons entrusted with a ~~air card/~~hotspot are responsible for its proper use, care, maintenance, and security.

(e) Immediately report loss of a mobile wireless device to the supervisor and the J-6/MEIT-CSD-CSB-Service Desk to cut off service. Please include as much specific information as possible to help expedite the replacement (e.g., serial number, ESN, device type, wireless carrier, etc.).

(f) Report loss and/or theft of the mobile wireless devices in accordance with USMEPCOM Regulation 380-1, USMEPCOM Security Program.~~710-2 by filling out Financial Liability Investigation of Property Loss (DD Form 200)~~.

TOC

(2) The Enterprise Network Branch (J-6/MEIT-CSD-ENB) roles and responsibilities:

(a) Purchase mobile wireless devices, setup the service provider, and distribute devices to the Directorates, Sectors, MEPS, and MET sites for use.

(b) Maintain records of which Directorates, Sectors, MEPS, and MET sites are issued wireless devices under Record Number 710-2c/700A, "Hand Receipts". Upon turn-in or superseded by a new hand receipt, keep in office file until no longer needed for conducting business, not to exceed 6 years, then destroy. Note: Individuals may request and receive the cancelled hand receipt for their own records. In such case, the hand receipt is not required to be retained as an official record.

(c) Provide remote access to the USMEPCOM networks for authorized personnel. Report unauthorized access as a security violation to the USMEPCOM Cyber Security ~~Risk Management~~ Office (CSO ~~RMO~~).

(3) Directors, Special Staff Officers, Sector, and MEPS Commanders will:

(a) Be responsible for accountability and hand receipt of all air cards/hotspots to users.

(b) Submit an Information Mission Elements Need Statement (IMENS) if additional air card/hotspot is required.

(4) Any user requiring USMEPCOM VPN access must submit an Authorization Access Request form, located on the SPEAR, through the user's supervisor to J-6/MEIT-CSO ~~RMO~~ prior to VPN software being installed.

(a) Desktop Support will perform software installation for Headquarters and Sector personnel.

(b) MEPS ITS will perform software installation for MEPS and MET Site personnel.

(5) Disciplinary Guidance:

(a) In accordance with USMEPCOM Acceptable Use Policy (AUP) (Appendix I), government equipment and property shall be used by employees, military personnel, and contractors for official Government purposes only. All authorized users have the duty to protect and conserve government property and shall not use such property, or allow it use by others, for any reason other than authorized purposes.

(b) Improper, fraudulent, abusive, or negligent use of a Government ~~air card/~~hotspot is strictly prohibited. Authorized users who misuse a Government air card/hotspot in violation of this policy or other applicable regulations are subject to disciplinary action in accordance with AR 680-700, Chapter 751, the Uniform Code of Military Justice (UCMJ), or Title 18 of the United States Code, as appropriate. Supervisors shall take appropriate corrective action against any authorized user who has engaged in any fraud, misuse, or abuse of an air card/hotspot.

c. The use of personal or non-Government hotspots is not authorized within the USMEPCOM network or facilities.

TOC

8-15. Mobile Telephone Use Overseas

a. Employees traveling overseas (i.e. outside the United States, Puerto Rico, or U.S. Territories) on official business with a government issued electronic device will submit a Service Desk ticket a minimum of 2 weeks prior to the start of their overseas travel and contain the mobile telephone number, the location(s) of international travel, and the first and last dates of travel.

b. All requests for overseas service will go through Sectors to include justification and that Sectors will put in the CA ticket in the "J6.ClientHardware.iPhone" request area if approved by Sector Commander/Deputy. For HQ, should be Director/Deputy approval. Government phones and data are not to be utilized overseas unless approved in advance, failure to comply will result in the user being responsible for all additional charges. Government furnished equipment, i.e. laptops and mobile phones, are not authorized to be used to access non-U.S. owned Wi-Fi networks.

TOC

Chapter 9
Enterprise Data Center (EDC)

9-1. Overview

The EDC is available to support HQ USMEPCOM, Sectors, Battalions, and MEPS processing and system requirements.

9-2. Operating Hours and System Availability

The EDC is staffed 0330-1800, Monday through Friday on processing days excluding Federal holidays. In the event of a Saturday processing day ("Saturday Opening") the J-6/MEIT-CSD-CSB-Service Desk will be manned during coordinated processing hours. These hours may be adjusted to accommodate exceptional circumstances or to facilitate changes in support requirements. Most functions are accessible 24x7. Changes to hours of operation will be requested through the Director, J-6/MEIT. 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." The computer room is operated as a "closed shop" (i.e., personnel not directly involved in computer operations will obtain permission to gain access). Access is granted only to personnel with a proper security credentials and valid requirement. EDC visitors will be escorted at all times while in the EDC. Security of the Enterprise is discussed in Chapter 1.

9-4. Technical Support

Technical support is provided for Enterprise application programmers and users by submitting a J-6/MEIT-CSD-CSB-Service Desk ticket. The J-6/MEIT-CSD-CSB-Service Desk ticket system can be accessed from the SPEAR main page.

9-5. EDC Telecommunications Services

Enterprise Network Connectivity services will be routed through J-6/MEIT-CSD-ENB.

9-6. Billing and Accounting (Chargeback)

USMEPCOM may charge a fee for services in some cases IAW the Support Agreement and Service Level Agreement between USMEPCOM and the other party.

9-7. Application Approval

HQ USMEPCOM, Sectors, Battalions, and MEPS requests for approval of new application systems will be submitted in writing by functional proponents to J-6/MEIT-ESB.

9-8. Users Working Group

There are several work groups which are made of USMEPCOM, the Accession Community of Interest (ACOI), and DoD and non-DoD agencies. The working groups focus on establishing better communication throughput, applicant data reliability, and increased support for ensuring the security of government data.

9-9. Requests for Special Print Forms

a. Request for or changes to USMEPCOM and MEPS specific forms and special reports printed with USMEPCOM equipment will be submitted in writing to J-3/MEOP-AD and J-1/MEHR-SD-MSS ~~SSS~~.

TOC

b. The MEPS will not produce large quantities of documents, forms or flyers on MEPS printers/copiers/MFDs without obtaining prior authorization from J-6/MEIT-PRO.

9-10. Backup and Recovery

J-6/MEIT-CSD-CSB provides for backup and off-site storage and subsequent retrieval of the USMEPCOM Enterprise system and 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 Servers environments in the event of a major catastrophe.

9-11. EDC Continuity of Operations Plan

J-6/MEIT-PRO maintains an Enterprise Continuity of Operations Plan (COOP) to ensure a viable COOP site is available with properly configured servers and appropriate environment and security for processing the USMEPCOM critical workload.

9-12. Temporary Issuing Equipment, Computers, and Peripherals

J-6/MEIT-CSD-CSB may temporarily issue network equipment, computers, laptops, or peripherals after the user submits a J-6/MEIT-CSD-CSB-Service Desk ticket. All requests for network equipment, computers, laptops, and peripherals should be made at least 7 work days in advance. This type of transaction needs to be coordinated with J-4/MEFA-ADL for temporary hand receipting process using a DA Form 2062 (Hand Receipt/Annex Number) in accordance with DA Pamphlet 710-2-1.

TOC

Chapter 10
USMEPCOM Enterprise Architecture Team for Information Technology (MEIT-EA) ~~Enterprise Systems Architecture & Integration Office~~

10-1. Overview

The USMEPCOM Enterprise Architecture Team for Information Technology (MEIT-EA) ~~Enterprise Systems Architecture & Integration Office (EAO)~~ provides IT architecture and systems engineering for USMEPCOM. MEIT-EA ~~EAO~~ researches, evaluates and recommends IT solutions. MEIT-EA ~~EAO~~ provides advisory services as technical leads on technology trends and their application to meet business challenges. MEIT-EA ~~EAO~~ maintains As-Is architecture and high level designs and develops the To-Be architectures and high level designs through the use of ontology and methodology frameworks and tools. A key MEIT-EA ~~EAO~~ goal is to directly assist USMEPCOM in the analysis, design, acquisition, development deployment and integration of all technology systems in the command through compliance with Federal, Department of Defense (DoD) and Department of the Army (DA) regulations, directives, guidelines and initiatives.

10-2. Responsibilities

a. Maintain the USMEPCOM Enterprise System Architecture (ESA): As-Is, To-Be and transition plans for the Data Architectures, Application Architectures, and Technology Architectures of USMEPCOM's IT systems.

(1) Providing input to IT strategic planning.

(2) Coordinating with all appropriate groups when there is a change in strategy or requests for exceptions to the ESA, and when oversight of a project's design-related decisions is necessary.

(3) Serving as reviewers and advisors for IT projects as a part of IT governance and ensuring compliance with Federal, Department of Defense and Department of the Army regulations, directives, guidelines and initiatives.

(4) Assisting in project planning and management as required.

(5) Providing technical leadership and assurance that IT projects are in alignment with the To-Be ESA.

(6) Serving to arbitrate design disputes across projects or systems.

(7) Creating and sustaining DoD Architecture Framework (DoDAF), an associated Federal, DoD and DA frameworks, ontologies, viewpoints, models and artifacts.

b. Establish and maintain the evolving technical blueprints, technical diagrams, artifacts and accompanying guidelines for the IT To-Be ESA and roadmap to manage the integration and interoperability of information technology across the command.

(1) Identifying and specifying USMEPCOM baseline through the use of framework tools, design standards, integration and interoperability and services used across the accessions community.

(2) Promoting Business Enterprise Architecture (BEA) Semantic Ontology initiatives and Service Oriented Architecture (SOA) principles to maximize the benefits of functionality reuse and systems

TOC

integration. Generally, establishing a net-centric technology vision to support USMEPCOM mission and Federal, DoD and DA initiatives.

(3) Maintaining compliance with security technical implementation guides (STIGs) by researching STIGs for To-Be ESA components and applying STIGs IAW DOI 8500 series of IA directives and instructions to components being added to J-6/MEIT IT systems.

(4) Proactively researching GOTS/COTS hardware and software in order to optimize accession processing solutions. Researching GOTS/COTS in the areas of information models, semantic Web and Ontology development, applications, middleware, Data Base Management System (DBMS), operating systems, servers, LAN and WAN networking systems, virtualization technologies, medical equipment, e-tablets, application/user/client security technology, etc.

(5) Researching DoD and DA initiatives impact on J-6/MEIT accession processing systems - initiatives and programs from accession partner application, Global Information Grid (GIG), Installation Information Infrastructure Modernization Program (I3MP), BEA, Defense Information Systems Agency (DISA), etc.

c. Establish and maintain a Technology Evaluation Program (TEP) as the ESA Assurance program and process. The TEP process is used to evaluate any proposed changes to the USMEPCOM ESA.

(1) The TEP process is used for chartered projects, SCPs, PRs, and new technology evaluations as required or needed.

(2) Performing solution alternatives analysis to assure quality software and/or system delivery is based on informed technical design choices.

(3) Identifying project technical risks and propose risk mitigation strategies.

d. Provide guidance for components of USMEPCOM information systems including Technology, Data Management, System Application, and Infrastructure in order to support future USMEPCOM initiatives through information systems engineering and provide a more agile business environment responsive to immediate change.

(1) Assure alignment of technical solutions and business models. Facilitate and support continuous engagements with functional and technical members of architecture working group across J-staff. This includes continuous development, integration, and sustainment of the full range of business and technical architectures required at USMEPCOM to enable fully integrated planning, analysis, and engineering across the Future Year's Defense Program for the USMEPCOM enterprise and to strengthen architecture-driven communications with major stakeholders in the DoD Accession Enterprise.

(2) Identify types of resources required to sustain internally and externally developed products.

(3) Review IMENS impact and risk on the enterprise architecture and compliance with As-Is and To-Be ESA and validating compliance with Federal, DoD and DA regulations, directives, guidelines and initiatives.

(4) Provide other required technical consultation and assistance to USMEPCOM functional and accessions partners.

TOC

Chapter 11
Web Infrastructure

11-1. Overview
J-6/MEIT-BSD-SDB is responsible for 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 (MEDC-PA) following procedures outlined on Web page. Requests for additions and changes to the intranet site are performed by HQ USMEPCOM Directorate/Special Staff Office content managers by contacting MEDC-PA.

11-2. USMEPCOM Internet Web Site
The goal of the Internet site is to provide outside agencies and the public with basic USMEPCOM information. MEDC-PA is the proponent and releasing authority for the site. J-6/MEIT-BSD-SDB is the functional manager and responsible for creating, maintaining, securing, and monitoring the Web site.

11-3. USMEPCOM Intranet Web Site
The SPEAR is a secure private intranet site provided to USMEPCOM employees. The SPEAR (https://spear) provides USMEPCOM specific information such as publications, calendars, budget information, and briefings. It 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/MEIT-BSD-SDB is the functional proponent for the intranet site and is responsible for creating, maintaining, securing, and monitoring the Web site.

11-4. USMEPCOM Internet Item Implementation Process
Request for changes or additions to the current Web site are submitted via an email to USMEPCOM MEDC-PA. MEDC-PA will create and forward updates to J-6/MEIT-BSD-SDB who will verify the technical feasibility and publication approved changes.

11-5. 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.

11-6. Web Technical Design, Development, Security, Operations, and Maintenance
J-6/MEIT-BSD-SDB is responsible for all Web infrastructure, technical design, development, security, operations and system maintenance.

TOC

Chapter 12
Copier Usage

12-1. Printing and Self-Service Copying

The USMEPCOM, Command Print Service Manager (CPS) serves as the POC for all matters relating to USMEPCOM copier and printing requirements.

12-2. Multifunctional Devices (MFD)

Sectors, Battalions and MEPS are responsible for ensuring compliance with policies concerning printing, duplication, and MFDs. MEPS commanders will implement an aggressive program for conserving resources and will ensure adherence to the policies outlined in AR 25-30, chapter 5. 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.

12-3. Key Operators (MEPS Level)

The MEPS Information Technology Specialist (ITS) shall be designated as the Key Operator of Leased MFDs. Key Operator will assist with paper jams, ensure MFD paper and supplies are available, and report malfunctions to HQ J-6/MEIT-CSD-CSB-Service Desk to schedule a service call. Each MEPS is responsible for ensuring the ITS performs the following roles and responsibilities as the Key Operator for MFDs:

a. ITS will ensure that only consumables (i.e., toner and fuser) authorized by the manufacture or Defense Logistics Agency (DLA) Document Services approved are used.

b. ITS will ensure MFD Hard Drives are removed/degaussed prior to release from HQ USMEPCOM control IAW AR 25-2 and AR 25-1, as applicable.

c. ITS will ensure the CPS Manager shall obtain documentation from the Key Operators confirming removal/degauss of Hard Drives when applicable.

d. ITS will ensure no vendor has access to the MFD(s) and/or printer(s) without notification/notifying Headquarters.

e. ITS will assist Headquarters and vendor(s) in the configuration, updating and restoration of MFD(s) and printer(s).

f. ITS will require all vendors to provide documentation for any and all services performed on MFD(s) or printer(s).

g. ITS will report any malfunctions, request for service, and consumables by entering a J-6/MEIT-CSD-CSB-Service Desk ticket.

h. ITS will report any malfunctions, delays in services, security risks/threats/opportunities that influence the operation and function of the MFD(s) and printer(s) immediately to the CPS Manager via email.

i. ITS is responsible for requesting and submitting "DLA Document Services Machine Relocation Request" form for all MFD(s) moves/relocations at least 60 days in advance of desired move/relocation CPS Manager.

TOC

j. ITS and their officially documented alternate are the only USMEPCOM personnel at the MEPS level authorized to request/report the relocation, service and maintenance, request consumables, facilitate updating and configuration of MFDs.

12-4. Key Operator (HQ Level)

a. The Key Operator and alternate at the Headquarters level are assigned by their respective Directorate; the HQ Key Operator and alternate are responsible for requesting moves/relocations, consumables, service and maintenance as needed or required.

b. HQ Key Operator is responsible for requesting and submitting "DLA Document Services Machine Relocation Request" form for all MFD(s) moves/relocations at least 60 days in advance of desired move/relocation to the CPS Manager.

c. HQ Key Operator will assist with paper jams, ensure MFD paper and supplies are available, and report malfunctions to HQ J-6/MEIT-CSD-CSB-Service Desk to schedule a service call.

d. HQ Key Operator will report any malfunctions, request for service, and consumables by entering a J-6/MEIT-CSD-CSB-Service Desk ticket.

e. HQ Key Operator will report any malfunctions, delays in services, security risks/threats/opportunities that influence the operation and function of the MFD(s) and printer(s) immediately to the CPS Manager via email.

f. Only J-6/MEIT-CSD-CSB personnel, or MFD contracting authorized agent, are authorized to perform updates of MFD firmware and/or software at the Headquarters level.

12-5. Liaison support

Under the guidance of ~~AR 601-270~~ Department of Defense Manual DoDM 1145.02 (Military Entrance Processing Station (MEPS)), USMEPCOM is responsible for providing copier support to all Service liaisons and guidance counselors physically located at each MEPS.

TOC

Appendix A
References

Section I
Publications referenced in or related to this publication

ACC Pamphlet 70-1
Contracting Officer's Representative Policy Guide

AR 11-2
Managers' Internal Control Program

AR 25-1
Army Knowledge Management and Information Technology.

AR 25-2
Information Assurance.

AR 70-13
Management and Oversight of Service Acquisitions

AR 190-13 (Restricted – FOUO)
The Army Physical Security Program.

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

AR 340-21
The Army Privacy Program**.**

AR 690-700
Personnel Relations and Services (General)

AR 735-5
Property Accountability Policies

Army (G-6) Information Assurance Best Business Practice (IA BBP) 05-PR-M-0002
Information Assurance (IA) Training and Certification

DA Pamphlet 25-1-1
Army Information Technology Implementation Instructions

DA Pamphlet 710-2-1
Using Unit Supply System (Manual Procedures)

Defense Acquisition Guidebook
https://www.dau.mil/tools/t/Defense-Acquisition-Guidebook

TOC

DFAR 208.74
Defense Federal Acquisition Regulation (Enterprise Software Agreements-Acquisition Procedures)

DFARS 252.201-7000
Defense Federal Acquisition Regulation Supplement

Directive-Type Memorandum (DTM) 09-012, Interim Policy
Guidance for DoD Physical Access Control

DoD COR Handbook

DoD Directive 5000.01
The Defense Acquisition System

DoD Directive 8000.1
Management of DoD Information Resources and Information Technology

DoD Directive 8100.02
Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

DoD Guidebook for the Acquisition of Services

DoDI 1000.13
Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals

DoDI 5000.02
Operation of the Defense Acquisition System

DoDI 8320.02
Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense

DoDI 8420.01
Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies

DoDI 8500.01
Cybersecurity.

DoDI 8510.01
Risk Management Framework (RMF) for DoD Information Technology (IT)

DoDI 8530.01
Cybersecurity Activities Support to DoD Information Network Operations

DoD JTA
Department of Defense Joint Technical Architecture Volume II Version 6.0

TOC

DoD Regulation 5500.7-R
The Joint Ethics Regulation (JER).

DoD 8570.01-M
Information Assurance Workforce Improvement Program

FAR
Federal Acquisition Regulation

Homeland Security Presidential Directive 12
Policy for a Common Identification Standard for Federal Employees and Contractors.

ITE-BOI
Information Technology Equipment (ITE) Basis of Issue (BOI)

NIST Special Publication 800-12.
An Introduction to Computer Security: The NIST Handbook.

NIST Special Publication 800-53 Rev 4
Security and Privacy Controls for Federal Information Systems and Organizations

NIST-SP 800-53A
Guide for Assessing the Security Controls in Federal Information Systems and Organizations

NIST Special Publication 800-88
Guidelines for Media Sanitization

NSA Information Assurance Mitigation Guidance
Media Destruction Guidance

OMB Circular A-130.
Managing Federal Information as a Strategic Resource

Public Law 93-579.
Privacy Act of 1974,

Public Law 99-474
Computer Fraud and Abuse Act of 1986

Public Law 100-235
Computer Security Act of 1987

Public Law 104-106 (Clinger-Cohen Act)
Information Technology Management Reform Act

Public Law 104-294
Economic Espionage Act of 1996
-- Title II—National Information Infrastructure Protection Act Of 1996

TOC

Public Law 107-347, sec 301-305
E-Government Act of 2002
-- Title III - - Federal Information Security Management Act of 2002 (FISMA)

Title 17, United States Code
Copyrights.

Title 18, United States Code
Crimes and Criminal Procedure

Uniform Code of Military Justice (UCMJ)
Uniform Code of Military Justice

USMEPCOM Regulation 10-1
United States Military Entrance Processing Command

USMEPCOM Regulation 27-2
Legal Services Ethics

USMEPCOM Regulation 360-1
Command Information (CI), Public Information (PI), and Community Relations (CR)

USMEPCOM Regulation 380-1
USMEPCOM Security Program

USMEPCOM Regulation 715-6
Acquisition Planning/Contract Management

10 U.S. Code, Subsection 2222
Defense Business Systems: Business Process Reengineering; Enterprise Architecture; Management

10 U.S. Code, Subsection 2337
Life-Cycle Management and Product Support

Section II
Forms referenced in or related to this publication

DA Form 11-2
Internal Control Evaluation Certification

DA Form 2062
Hand Receipt / Annex Number

DD Form 200
Financial Liability Investigation of Property Loss

DD Form 250
Material Inspection and Receiving Report

TOC

DD Form 1367
Commercial Communication Work Order

DD Form 2875
System Authorization Access Request (SAAR)

USMEPCOM Form 25-1-7
USMEPCOM Sanitization Validation Form

USMEPCOM VPN Form
USMEPCOM VPN Authorization Access Request

USMEPCOM IMENS Form
Information Mission Elements Need Statement (IMENS)

DLA Document Services Machine Relocation Request Form
MFD Relocation Request

Section III
Recordkeeping Requirements

RN 25-1ppp1/400B: "Life Cycle Management of Information Management Systems (Information Mission Elements Need Statement (IMENS))"
PA: N/A
Keep in local archive until no longer needed for conducting business, not to exceed 6 years. Records will then be placed on physical media and transferred to the Federal Records Center (FRC), the FRC will destroy the records after 25 years.
(Referenced in Paragraph 3-1)

RN 25-1lll/400B: "ITS Administrative Reports"
PA: N/A
Keep in office file until no longer needed for conducting business, not longer than 6 years, then destroy.
(Referenced in Paragraphs 2-4k, 2-7k)

RN 25-2d1/400B: "Accreditation of Automated Systems"
PA: N/A
Keep in office file until no longer needed for conducting business, not longer than 6 years, then destroy.
(Referenced in Paragraph 2-6d)

RN 25/400B: "General Information Management Correspondence Files - *User Memorandum of Agreement*"
PA: N/A
Keep in office file not more than 2 years, then destroy.
(Referenced in Paragraph 2-6f)

RN 25/400B: "General Information Management Correspondence Files - *USMEPCOM Form 25-1-7-E*"
PA: N/A
Keep in office file not more than 2 years, then destroy.
(Referenced in Paragraph 3-10)

TOC

RN 25-1jjjj2/400B: "Enterprise Architecture Records"
PA: N/A
Keep in office file until no longer needed for conducting business, not to exceed 7 years, then destroy. Records may be transferred to the FRC after 5 years, the FRC will destroy the records after 7 years.
(Referenced in Paragraph 5-7)

RN 25-1ggggg/400B: "Website and User Access Logs"
PA: N/A
Keep in office file for 3 years, then destroy.
(Referenced in Paragraph 5-19b)

RN 710-2c/700A: "Hand Receipts"
PA: A0710-2bDALO
Upon turn-in or superseded by a new hand receipt, keep in office file until no longer needed for conducting business, not to exceed 6 years, then destroy. **Note:** Individuals may request and receive the cancelled hand receipt for their own records. In such case, the hand receipt is not required to be retained as an official record.
(Referenced in Paragraph 8-14b(2)(b))

RN 25-1ccc/400B: "Telephone Equipment and Service Control Files – BOI Exceptions"
PA: N/A
Keep in office file until no longer needed for conducting business, not to exceed 6 years, then destroy.
(Referenced in Appendix D-1)

TOC

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 PTC ~~PCT~~ (formally MKS) system? (UMR 25-1, Paragraph(s) 1-4f(3), 1-4g(2), 1-4l(7), 1-4m(5) 1-4n(12), 3-2b, 3-6, 3-7b, 3-7d, 4-3a, 7-3, 7-5 and Appendix C

(2) Does each piece of accountable ADP hardware have an approved IMENS processed through PTC ~~PCT~~ (formerly MKS) system? (UMR 25-1, Paragraph. 3-2b and Paragraph 3-6d)

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 IMENS? (UMR 25-1, Paragraph 7-3)

(2) Are the original media (CD-ROM and/or diskettes) and manuals secured by the command software manager? (UMR 25-1, Paragraph 7-7)

(3) Has the command software manager conducted the annual audit of the non-MIRS computer hard drives to ensure no copyright violations exist? (UMR 25-1, Paragraphs 1-4n(16) and 7-3)

(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)? (UMR 25-1, Paragraph. 3-7)

TOC

(5) Does the command software manager have the correct and updated command approved software list that corresponds to the IMENS? (UMR 25-1, Paragraph. 3-7)

(6) Has a back-up for the ITS been assigned? (UMR 25-1, Paragraph 1-4m(8) and Appendix G)

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? (UMR 25-1, Paragraph. 1-4n(18) and 5-7)

(2) Are all network connected devices authorized for use on a USMEPCOM network? (UMR 25-1, Paragraph. 5-4)

(3) Is there a USMEPCOM Designated Approval Authority (DAA) signed request to use Wi-Fi in the MEPS request on file? (UMR 25-1, Paragraph 5-17b)

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 a~~n informal~~ memorandum? (UMR 25-1, Paragraph. 8-2)

(2) Is the TCCO aware of his or her duties and responsibilities? (UMR 25-1, Paragraph. 8-2)

(3) Are the telephone lines and instruments in accordance with the basis of issue authorization? (UMR 25-1, Appendix D-2)

(4) Are personnel aware of restrictions regarding making personal telephone calls using government telephones? (UMR 25-1, Paragraph. 8-3)

(5) Are persons making unauthorized long distance calls paying for them? (UMR 25-1, Paragraph. 8-7)

(6) Are mobile telephones being used outside of the United States, this includes Puerto Rico? (UMR 25-1, Paragraph 8-15)

f. Cyber Security Risk ~~Management and Compliance~~ 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 UMR 25-1, 5 June 2017.

B-6. Comments

Submit comments on this inspection program through your Sector ITS to HQ USMEPCOM, J-6/MEIT.

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

Use DA Form 11-2 to document management control evaluations.

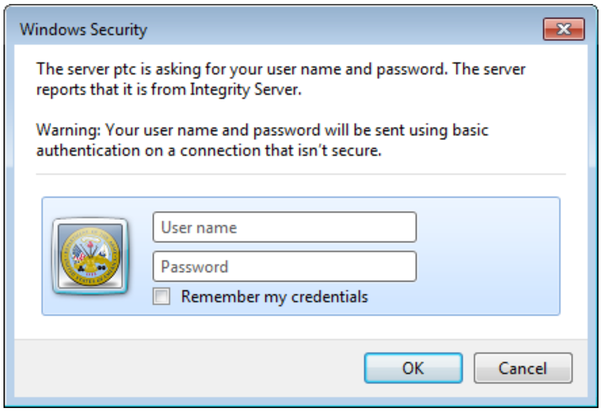
TOC

Appendix C
Instructions for Completion of a Problem Reporting (PR) and System Change Proposal (SCP) and Information Mission Elements Need Statement (IMENS)

The PTC ~~PCT~~ software is used to create Problem Reporting (PR) and System Change Proposal (SCP) and Information Mission Elements Need Statement (IMENS). To gain access to the PTC ~~PCT~~ Software, the requester's supervisor submits an email to J-6/MEIT-BSD-QAB requesting access for the user. Once the account has been established, J-6/MEIT-BSD-QAB will return an encrypted email to the user with the user's account information and password.

All PRs, SCPs, and IMENS must be submitted electronically.

Log into http://ptc:7001/im and enter appropriate information



Windows Security

The server ptc is asking for your user name and password. The server reports that it is from Integrity Server.

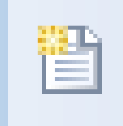
Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

User name

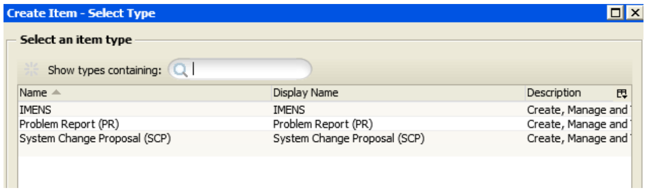
Password

□ Remember my credentials

Select the Create New Item icon from the left side of the webpage.



Choose which items to create.



Create Item - Select Type

Select an item type

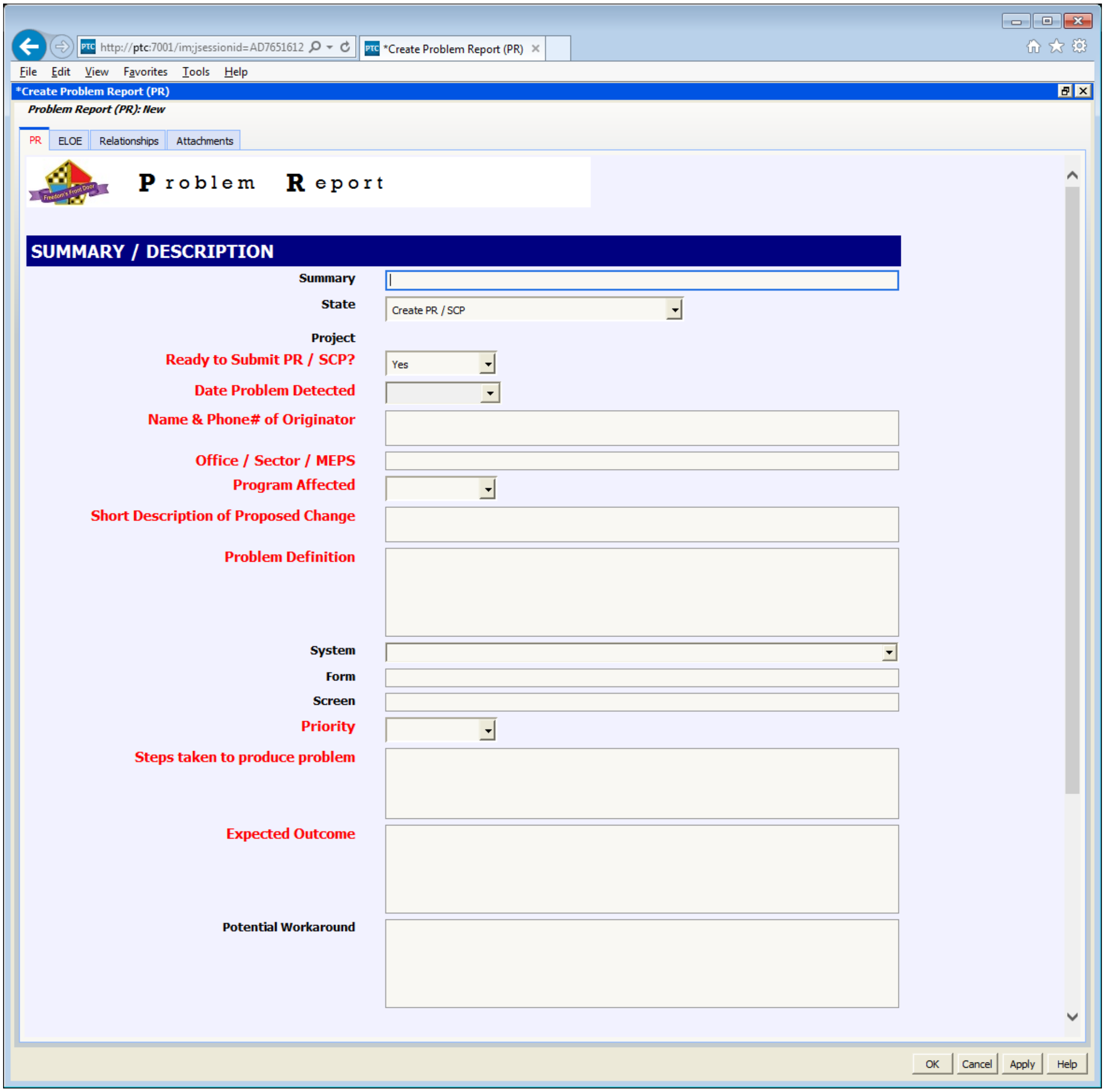
Show types containing:

Name	Display Name	Description
IMENS	IMENS	Create, Manage and
Problem Report (PR)	Problem Report (PR)	Create, Manage and
System Change Proposal (SCP)	System Change Proposal (SCP)	Create, Manage and

After a PR or SCP or IMENS is created, the requester will receive an email notification with a reference number which can be used to update and track the request. At any time the requester can log into the PTC ~~PCT~~ system and check the status of a request using the reference number.

TOC

Problem Report (PR). The requestor will complete Section 1.

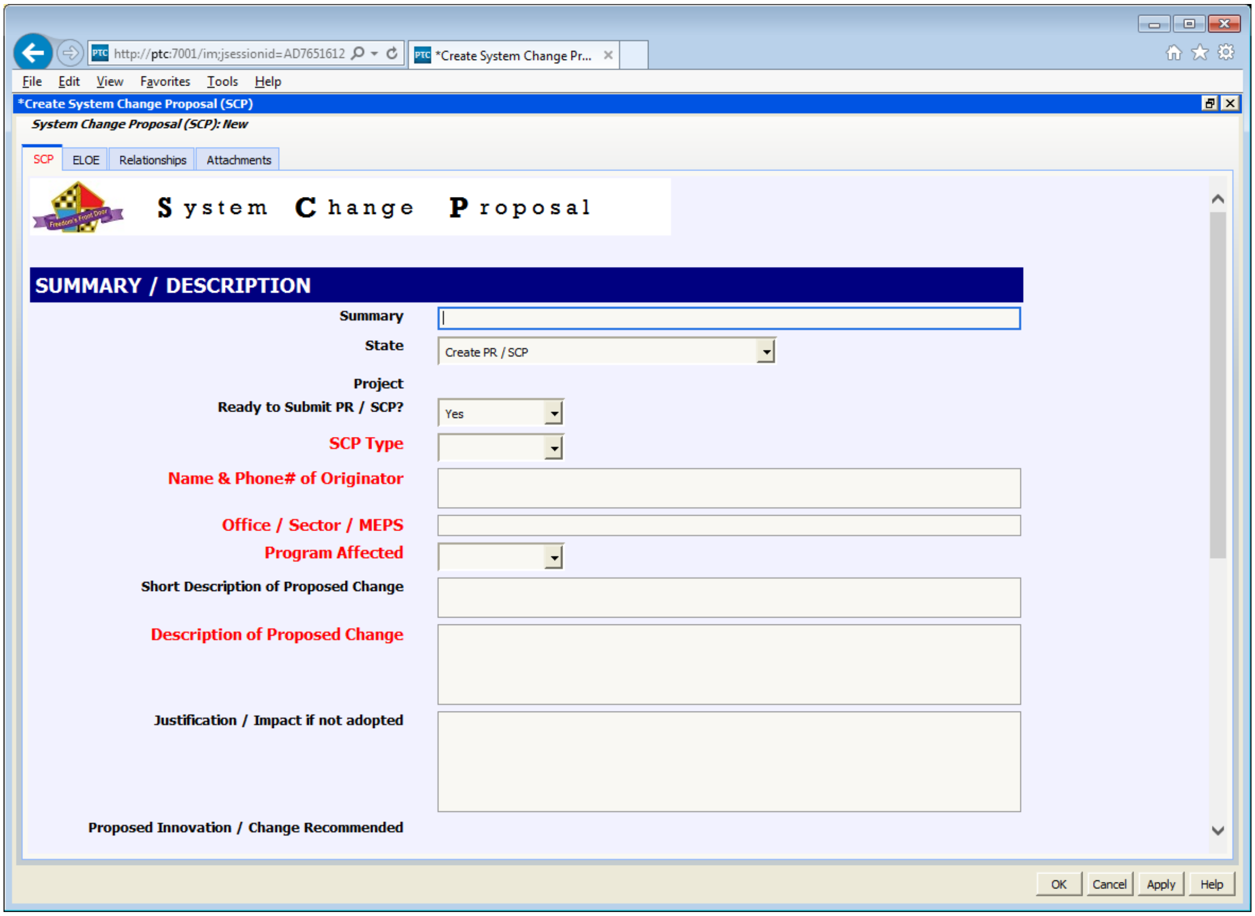


SUMMARY / DESCRIPTION

Summary	
State	Create PR / SCP
Project	
Ready to Submit PR / SCP?	Yes
Date Problem Detected	
Name & Phone# of Originator	
Office / Sector / MEPS	
Program Affected	
Short Description of Proposed Change	
Problem Definition	
System	
Form	
Screen	
Priority	
Steps taken to produce problem	
Expected Outcome	
Potential Workaround	

TOC

System Change Proposal (SCP). The requestor will complete Section 1.



*Create System Change Proposal (SCP)

System Change Proposal (SCP): New

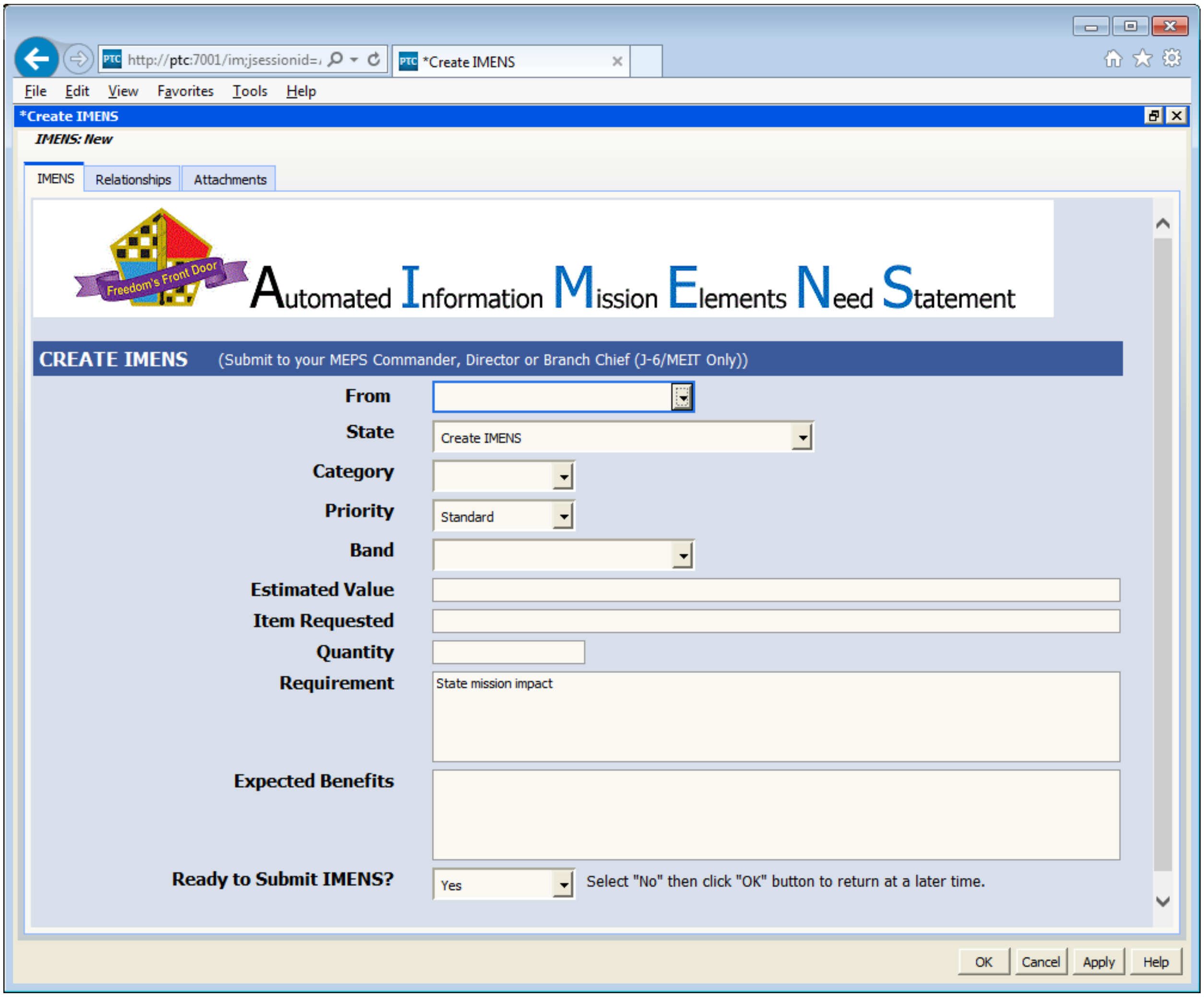
System Change Proposal

SUMMARY / DESCRIPTION

Summary	
State	Create PR / SCP
Project	
Ready to Submit PR / SCP?	Yes
SCP Type	
Name & Phone# of Originator	
Office / Sector / MEPS	
Program Affected	
Short Description of Proposed Change	
Description of Proposed Change	
Justification / Impact if not adopted	
Proposed Innovation / Change Recommended	

TOC

Information Mission Elements Need Statement (IMENS). The requestor will complete Section 1.


http://ptc:7001/im;jsessionid=
*Create IMENS
File Edit View Favorites Tools Help
IMENS Relationships Attachments
Freedom's Front Door
OK Cancel Apply Help

*Create IMENS

IMENS: New

Automated Information Mission Elements Need Statement

CREATE IMENS (Submit to your MEPS Commander, Director or Branch Chief (J-6/MEIT Only))

From	
State	Create IMENS
Category	
Priority	Standard
Band	
Estimated Value	
Item Requested	
Quantity	
Requirement	State mission impact
Expected Benefits	
Ready to Submit IMENS?	Yes Select "No" then click "OK" button to return at a later time.

TOC

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/MEIT-CSD-CSB-Service Desk.
A copy of all approved exceptions to the BOI will be maintained at the Sector and MEPS (when applicable) under Record Number 25-1ccc/400B, “Telephone Equipment and Service Control Files – BOI Exceptions”. Keep in office file until no longer needed for conducting business, not to exceed 6 years, then destroy.

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, Battalions and MEPS will be determined by J-6/MEIT-CSD-ENB.

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) 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.

TOC

Appendix E
Format to Request Telecommunications Service

(Appropriate Letterhead)

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

MEMORANDUM THRU (Appropriate Sector)

FOR Director, J-6/MEIT-Plans and Resource Office, North Chicago, Illinois

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

IAW USMEPCOM Regulation 25-1, 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 D (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.)

TOC

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)

TOC

Appendix F:
Format for Appointment of MEPS ITS

(Appropriate Letterhead)

Office Symbol

MEMORANDUM FOR RECORD

SUBJECT: Appointment of an Information Assurance Technical Level I (IAT), <Location> MEPS

1. References:

a. Army Regulation 25-2, October 24, 2007.

b. Department of Defense 8570.01-M, Information Assurance Workforce Improvement Program, Incorporating Change 4, 10 November, 2015.

2. Effective immediately, the below individual is appointed to perform duties/function for <Location> MEPS, USMEPCOM as the IA Technical Level I & IA Support Officer.

(FOUO)
Name: First Name Last Name
Grade/Rank: GS-9
Civilian Job Specialty Code: 2210 IT Specialist (INFOSEC)
Person Security Standards (IAW AR 25-2, Paragraph 4-14): ITII
IA Category Level And Level (IAW DoD 8570.01-M): IAT I

3. Purpose: To perform IA functions/duties per AR 25-2, chapter 3 and DoD 8570.01-M.

4. Period: Until officially relieved or released from appointment, or upon transfer, termination, reassignment, retirement or discharge.

5. Special Instructions:

a. Complete required IA training and certification for category/level per the Army's IA Training and Certification Best Business Practice.

b. Register in the Army Training and Certification Tracking System (https://atc.us.army.mil) and enter training and certification completions as outlined in the Army's IA Training and Certification Best Business Practice.

c. Upload duty appointment orders and privilege access agreement (if applicable).

6. The point of contact is the undersigned.

(SIGNATURE BLOCK)

Appendix G
Format for Appointment of MEPS Auxiliary ITS

(Appropriate Letterhead)

Office Symbol

MEMORANDUM FOR RECORD

SUBJECT: Appointment of an Auxiliary Information Assurance Technical Level 1 (IAT), <Location> MEPS

1. References:

a. Army Regulation 25-2, October 24, 2007.

b. Department of Defense 8570.01-M, Information Assurance Workforce Improvement Program, Incorporating Change 4, 10 November, 2015.

2. Effective immediately, the below individual is appointed to perform duties/function for <Location> MEPS, USMEPCOM as the Auxiliary IA Technical Level I & IA Support Officer.

(FOUO)
Name: First Name Last Name
Grade/Rank: GS-9
Civilian Job Specialty Code: 2210 IT Specialist (INFOSEC)
Person Security Standards (IAW AR 25-2, Paragraph 4-14): ITII
IA Category Level And Level (IAW DoD 8570.01-M): IAT I

3. Purpose: To perform IA functions/duties per AR 25-2, chapter 3 and DoD 8570.01-M.

4. Period: Until officially relieved or released from appointment, or upon transfer, termination, reassignment, retirement or discharge.

5. Special Instructions:

a. Complete required IA training and certification for category/level per the Army's IA Training and Certification Best Business Practice.

b. Register in the Army Training and Certification Tracking System (https://atc.us.army.mil) and enter training and certification completions as outlined in the Army's IA Training and Certification Best Business Practice.

c. Upload duty appointment orders and privilege access agreement (if applicable).

6. The point of contact is the undersigned.

(SIGNATURE BLOCK)

TOC

Appendix H
Format to Request to Install MWR or Non-Appropriated Funded Wireless Service

(Appropriate Letterhead)

Office Symbol

MEMORANDUM FOR Headquarters, USMEPCOM Information Technology Cyber Security Office (J-6/MEIT-CSO)

THRU <MEPS Battalion> Battalion Commander
<Eastern/Western> Sector Commander
HQ, USMEPCOM J-6/MEIT-CSO
HQ, USMEPCOM DAA

SUBJECT: Request to install MWR (or Non-Appropriated Funded) Wireless Service, <Location> MEPS

1. References:

a. Army Regulation 25-2, October 24, 2007.

b. Department of Defense 8570.01-M, Information Assurance Workforce Improvement Program, Incorporating Change 4, 10 November, 2015.

c. USMEPCOM Regulation 25-1

2. The <Location> MEPS, USMEPCOM requests the installation of a non-secure Wi-Fi Wireless network. The following information is provided.

a. Who is providing the Wi-Fi Service?

b. Equipment list –

c. What is the intended security for the main equipment?

d. Equipment installation locations (waiting area, game room, etc.).

e. What are the hours the Wi-Fi will be providing service?

f. What internet security software will be used (net-nanny, etc.)?

g. How will the MEPS identify the service provided is unofficial to the users?

h. How will the MEPS identify/enforce Rules of Behavior/Acceptable Use?

i. Who will support the equipment/wireless and how?

j. How will access be monitored to identify/prevent abuse?

TOC

3. I affirm that I have read reference c., USMEPCOM Regulation (UMR) 25-1, chapter 5-17 Other Networks.) , Acquisition and Use of Commercial Internet Service Providers (ISP) and Wireless Fidelity (Wi-Fi) in a United States Military Entrance Processing Command (USMEPCOM) Facility Policy.

4. The point of contact is the undersigned.

(SIGNATURE BLOCK)

TOC

Appendix I
USMEPCOM Acceptable Use Policy

The following is an excerpt from the USMEPCOM Acceptable Use Policy. Each user of the USMEPCOM Enterprise must electronically sign a copy of the Acceptable Use Policy at first logon and on, or about, the anniversary of the user's first logon.

1. Understanding. I understand that I have the primary responsibility to safeguard the information contained within the USMEPCOM Network from unauthorized or inadvertent modification disclosure, destruction, denial of service, and use.

2. Access. Access to this network is for official use and authorized purposes as set forth in DoD Regulation 5500.7-R (Joint Ethics Regulation) or as further limited by this policy.

3. Revocation. Access to USMEPCOM resources is a revocable privilege and is subject to content monitoring and security testing.

4. Classified information processing. The USMEPCOM Network is not authorized for any processing of classified information.

5. Unclassified information processing. The IT Network is the primary unclassified system for USMEPCOM. User must be a U.S. citizen to access USMEPCOM's Network.

a. The IT Network provides unclassified communication to external DoD and other United States Government organizations. Primarily this is done via electronic mail and Internet networking protocols such as Web and ftp (File Transfer Protocol).

b. Controlled Unclassified Information (CUI) per DoDI 5200.01, volume 4 DoD Information Security Program: Controlled Unclassified Information (CUI).

c. Email and attachments are vulnerable to interception as they traverse the Non-secure Internet Protocol Routing Network (NIPRNET) and Internet.

6. Minimum security rules and requirements. As an IT Network user, the following minimum security requirements apply:

a. Personnel are not permitted to access the IT Network unless in complete compliance with the USMEPCOM personnel security requirements for operating in an UNCLASSIFIED but sensitive environment.

b. I have completed user security awareness-training. I will participate in all training programs as required (including threat identification, physical security, acceptable use policies, malicious content and logic identification, and nonstandard threats such as social engineering) before receiving system access.

c. I will generate and protect passwords and pass-phrases. Passwords will consist of 14 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. I will not use as my user ID, common names, birthday, telephone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.

d. I will use only authorized hardware and software. I will not install or use any personally-owned hardware, software, shareware, or public domain software.

e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk.

f. I will not attempt to access or process data exceeding the authorized Information System (IS) classification level.

g. I will not alter or change the configuration or use operating systems or programs, except as specifically authorized.

h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code.

i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know.

j. I will not utilize USMEPCOM or DoD-provided ISs for commercial financial gain or illegal activities.

k. I will comply with all security guidance from USMEPCOM Information Assurance Personnel.

l. Maintenance will be performed by J-6 information technology specialists (ITSs) only.

m. I will use screen locks, actively lock workstation, log off, and remove my Common Access Card from the workstation when departing the area of my workstation. If I am going to vacate my workstation for an extended period to include at the end of the workday, I will log off completely.

n. I will immediately report any suspicious output, files, shortcuts, or system problems to the MEPS or Sector ITS or USMEPCOM MIT Service Desk and cease all activities on the system.

o. I will address any question regarding policies, responsibilities, and duties to the MEPS or Sector ITS or USMEPCOM MIT Service Desk.

p. I understand each IS is the property of USMEPCOM and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

q. Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

r. Ensure that display or output of sensitive information in human-readable form is positioned to deter individuals from reading the information or obtain a privacy screen for your monitor.

TOC

s. Inform the supervisor when access to a particular DoD information system or enclave is no longer required.

t. Personal use of the information system is authorized as long as the following conditions are met:

(1) Does not adversely affect the performance of official duties

(2) Is made during employee's personal time

(3) Does not reflect adversely on the Federal Government

(4) Does not interfere with communications or network system functionality

(5) Does not create any significant additional cost to DoD

u. Personal use of the information system is not authorized for the following:

(1) To solicit, advertise, or engage in selling activities in support of a private business enterprise,

(2) To promote fundraising activities

(3) To send chain letters

(4) To send harassing email

v. I understand that monitoring of the IT Network will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities define unacceptable uses of USMEPCOM Information Systems:

(1) Storage of personal files obtained via the Internet may not be stored on Government workstation hard drives or on local area network (LAN) servers.

(2) Downloading of video or voice files except where serving an approved official USMEPCOM function.

(3) Use of programs intended to scan networks and systems, such as port scanners and vulnerability scanners, unless authorized by the Cyber Security Risk Office.

(4) Use of network sniffing tools used to collect user information and passwords, unless authorized by the Cyber Security Risk Office.

(5) Use of Unauthorized user IDs. This includes attempting to impersonate another user.

(6) Use of authorized user IDs. This includes attempting to impersonate another user.

(7) Use of the IT Network without proper training and a valid USMEPCOM Acceptable Use Policy signed.

TOC

(8) Failure to follow existing security policies and procedures in the use of Internet services. Inclusive in this restriction is any action that might jeopardize the USMEPCOM Network and associated computer systems and data files (to include, but not limited to virus attacks when downloading files from the Internet).

(9) Disclosure of Privacy Act material, copyrighted materials, and procurement of sensitive material without the appropriate clearances.

(10) Use of the USMEPCOM Network while in violation of any USMEPCOM and Department of Defense Policies and Regulations, and the current license agreements.

(11) Viewing, storage, or distribution of pornography or pornographic or obscene (adult or child) material.

(12) Installation of unauthorized games on any USMEPCOM computer.

Note: Activity in any of the above can lead to criminal prosecution.

Acknowledgment: I have read the above regulations. I understand that the information below will be used to identify me and may be disclosed to law enforcement authorities for investigation or prosecuting violations. I understand my responsibilities regarding these systems and the information contained in them.

TOC

Appendix J
Glossary

Section I
Glossary

A&A
Assess and Authorize

ACC
Army Contracting Command

ACL
Access Control List

ACOR
Alternate Contracting Officer Representative

ACTEDS
Army Civilian Training, Education and Development System

ADP
Automated Data Processing

ADL
Acquisition Logistics Branch

ACOI
Accession Community of Interest

AD
Accessions Division

ADL
Logistics Branch

AKO
Army Knowledge Online

AMA
Acquisition Milestone Agreement

AO
Authorizing Official

AOL
America On Line (email)

TOC

AP
Access Points (wireless)

APMS
Army Portfolio Management System

AR
Army Regulation

ARIMS
Army Records Information Management System

AST
Administrative Service(s) Technician

BEA
Business Enterprise Architecture

BBP
Best Business Practice

BOI
Basis Of Issue

BPR
Business Processing Reengineering

BSD
Business Services Divisions

C&A
Certification and Accreditation

CAB
Change Advisory Broad

CAC
Common Access Card

CAJ
Contract Action Justification

CAMP
Contract Administration and Monitoring Process

CAT-ASVAB
Computer Adaptive Testing-Armed Services Vocational Aptitude Battery

TOC

CCB
Configuration Control Board

CCSB
Configuration Control Sub-Board

CD
Compact Disk

CE
Computing Equipment

CERT
Computer Emergency Response Team

CHESS
Computer Hardware Enterprise Software Solution

CI
Configuration items

CIO
Chief Information Officer

CM
Configuration Management

CMD
Commercial Mobile Devices

CND
Computer Network Defense / Command Network Device

CONUS RCERT
Continental United States Regional Computer Emergency Response Team

COO
Operations Center

COOP
Continuity of Operations Plan

COR
Contracting Officer Representative

COTS
Commercial-Off-The-Shelf

TOC

CP
Career Program

CPM
Career Program Manager

CPS
Command Print Service Manager

CSA
Configuration Status Accounting

CSAs
Communication Service Authorizations

CSD
Core Services Division

CSD-A
Cybersecurity Defense Analyst

CSO
Cyber Security Office

CSS
Central Security Service

CUI
Controlled Unclassified Information

DA
Department of the Army

DAT
Drug Alcohol Test

DD
Department of Defense

DAR
Data At Risk/Data At Rest

DAU
Defense Acquisition University

DBMS
Data Base Management System

TOC

DBS
Defense Business System

DCIO
Deputy Chief Information Officer

DD
Defense Department

DEE
DISA Enterprise Email

DISA
Defense Information Systems Agency

DKO
Defense Knowledge Online

DLA
Defense Logistics Agency

DLPT
Defense Language Proficiency Test

DIARMF
DoD Information Assurance Risk Management Framework

DoD
Department Of Defense

DoDAF
DoD Architecture Framework

DoDIN
Department of Defense Information Network

DoDM
Department of Defense Manual

DOIT
Director of Information Technology

DTM
Directive Type Memorandum

EAB
Enterprise Application Branch

TOC

EAO
Enterprise Systems Architecture and Integration Office

EDC
Enterprise Data Center

EFCS
Electronic Fingerprint Capture System

email
Electronic Mail

ENB
Enterprise Network Branch

EPMB
Enterprise Portfolio Management Board

ERB
Enterprise Review Board

ES
Eastern Sector, USMEPCOM

ESA
Enterprise Systems Architecture

ESI
Enterprise Software Initiative

FAR
Federal Acquisition Regulation

FAX
Facsimile

FCA
Functional Configuration Audits

FIPS
Federal Information Processing Standards

FOUO
For Official Use Only

GIG
Global Information Grid

TOC

GOTS
Government-Off-The-Shelf

GOV
Government Owned Vehicle

GSA
General Services Administration

HBSS
Host Based Security System

HIV
Human Immunodeficiency Virus

HQ
Headquarters

HRC
Human Resources Command

I3MP
Installation Information Infrastructure Modernization Program

IA
Information Assurance

IAM
Information Assurance Manager

IAPM
Information Assurance Program Manager

IASO
Information Assurance Support Officer

IAT
Information Assurance Technical

IAVA
Information Assurance Vulnerability Alert

IAVB
Information Assurance Vulnerability Bulletin

IAW
In Accordance With

TOC

ID
Identification

IG
Inspector General

IGCE
Independent Government Cost Estimate

IMENS
Information Mission Elements Needs Statement

INFOSEC
Information Systems Security

IP
Internet Protocol

IS
Information System

ISSM
Information System Security Manager

ISSO
Information System Security Officer

IT
Information Technology

ITAM
Information Technology Asset Management

ITM
Information Technology Management

ITE
Information Technology Equipment

ITS
Information Technology Specialist

ITWG
Information Technology Working Group

JTA
Joint Technical Architecture

TOC

KO
Contracting Officer

LAN
Local Area Network

LANWarNET
Local Area Network War Network

MB
Megabytes

MEDC-PA
USMEPCOM Public Affairs Office

MEFA
USMEPCOM Facilities and Acquisition Directorate (J-4)

MEHR
USMEPCOM Human Resources Directorate (J-1)

MEIT
USMEPCOM Information Technology Directorate (J-6)

MEIT-EA
USMEPCOM Enterprise Architecture Team for Information Technology

MEOP
USMEPCOM Operations Directorate (J-3)

MEMD
USMEPCOM Medical Plans and Policy Directorate (J-7)

MEPS
Military Entrance Processing Station

MEPT
USMEPCOM Strategic Planning & Transformation (J-5)

MERM
USMEPCOM Resource Management (J-8)

MET
Military Entrance Test

MFD
Multifunctional Device

TOC

MICC
Mission and Installation Contracting Command

MKS
Mortice Kern System

MOA
Memorandum of Agreement

MOC
USMEPCOM Operations Center

MWR
Morale, Welfare and Recreation

NE
Network Environment

NETCOM
Network Enterprise Technology Command

NIPRNET
Non-secure Internet Protocol Router Network

NIST
National Institute Of Standards And Technology

NSA
National Security Agency

OMB
Office of Management And Budget

P-ISSM
Program Information System Security Manager

PA
Public Affairs

PBO
Property Book Officer

PBUSE
Property Book Unit Supply Enhanced

PBX
Public Branch Exchange

TOC

PC
Personal Computer

PCA
Physical Configuration Audits

PTC
Parametric Technology Corporation

PCM
Production Change Management

PDA
Personal Digital Assistant

PDS
Protected Distribution Systems

PED
Portable Electronic Device

PHI
Protected Health Information

PIA
Privacy Impact Assessment

PII
Personally Identifiable Information

PKI
Public Key Infrastructure

PL
Public Law

POC
Point Of Contact

PPQA
Process and Product Quality Assurance

PR
Problem Report

PRO
Plans and Resources Office

TOC

PWS
Performance Work Statement

QASP
Quality Assurance Surveillance Plans

QAE
Quality Assurance Evaluator

QBA
Quality Assurance Branch

RAM
Random Access Memory

RCERT
Regional Computer Emergency Response Team

RFQ
Request for Quote

RMF
Risk Management Framework

ROM
Read-Only Memory

RSN
Recruiting Services Network

SA
System Administrator

SAAR
System Authorization Access Request

SANS
SysAdmin, Audit, Networking, and Security

SCA
Service Contract Approval

SCIFs
Sensitive Compartmented Information Facilities

SCM
Software Configuration Management

TOC

SCMP
Software Configuration Management Plan

SCMS
Software Configuration Management System

SCP
System Change Proposal

SDB
System Development Division

SLC
Senior Leader Council

SLA
Service Level Agreements

SME
Subject Matter Expert

SOA
Service Oriented Architecture

SONA
Statement of Non-Availability

SOP
Standing Operating Procedures

SORN
System of Records Notice (SORN), Privacy

SPEAR
Sharing Policy Experience And Resources

SSID
Service Set Identifier

SSS
Selective Service System

STIG
Security Technical Implementation Guides

TCCO
Telecommunications Control Officer

TCOO
Telecommunications Ordering Officers

TDA
Tables Of Distribution And Allowances

TEP
Technology Evaluation Program

TNOSC
Theater Network Operations and Security Center

UMF
USMEPCOM Form

UMR
USMEPCOM Regulation

UBIS
USMEPCOM Business Intelligence System

USC
United States Code

USB
Universal Serial Bus

USMEPCOM
United States Military Entrance Processing Command

USMIRS
USMEPCOM Integrated Resource System

VCE
Virtual Contracting Enterprise, Army

VoIP
Voice over Internet Protocol

VPN
Virtual Private Network

WAN
Wide Area Network

WAWF
Wide-Area-Work Flow

TOC

Wi-Fi
Wireless Fidelity (Wireless Network)

WLAN
Wireless Local Area Networks

WS
Western Sector, USMEPCOM

WTC
Workforce Development, Training and Conference Division (J-1)

WWW
World Wide Web

TOC

Section II
Terms

Acquisition
Purchasing by contract with appropriate funds for supplies and services to include construction by and for the use of the Federal Government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

Acquisition Planning
Means the process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency need in a timely manner and at a reasonable cost. It includes ·developing the overall strategy for managing the acquisition.

Acquisition Streamlining
Means any effort that results in more efficient and effective use of resources to design and develop, or produce, quality systems.

AFARS
Army Federal Acquisition Regulation Supplement is the Army's supplemental guidance to the FAR and DFARS.

Air Card
A device that adds wireless connectivity to a laptop for cellular data.

Bona Fide Need
The balance of an appropriation or fund limited for obligation to a definite period is available for payment of expenses properly incurred during the period of availability.

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.

Computer Hardware Enterprise Software Solution (CHESS)
The Army’s designated primary source for commercial Information Technology (IT). CHESS provides a no-fee, flexible procurement strategy through which an Army user may obtain Commercial Off-the-Shelf (COTS) IT hardware, software, and services contract vehicles via the CHESS IT e-mart (https://chess.army.mil).

Clinger-Cohen Act
Public Law 104-106.

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

TOC

Configuration status accounting (CSA)
Reports to provide visibility into the status of baselines.

Communications Service Authorizations (CSAs)
A contract issued by 7th Signal Command to J-6/MEIT-CSD-ENB Telephone Operations, Sectors, Battalions, MEPS, and vendors. The CSAs are used as authorization to pay telephone invoices and order telephone services.

Contract Action Justification Form
Service contract requirements in excess of $100k require approval at the designated General Officer/Senior Executive Service level. The USMEPCOM commander signifies completion of the initial review and approval of the requirement or Chief of Staff signing the form Army G-1 CAJ form before submission to Army G-1.

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.

Contracting Officer's Representative
Is an individual designated IAW DFARS subsection 201.602-2 and authorized in writing by the KO to perform specific technical and administrative functions (DFAR Clause 252.201-7000)? Alternates are also appointed in writing designating specific responsibilities, authorities, and limitations.

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.

DFARS
Defense Federal Acquisition Regulation Supplement is the source for regulations, which include the implementation of statutes and DoD-wide contracting policies, authorities, and delegations.

DFARS Procedures Guidance and Information
DFARS PGI is a companion resource to the DFARS. The PGI is a web-based tool for simply and rapidly accessing guidance and information relevant to FAR and DFARS topics. The PGI contains both mandatory and non-mandatory internal DoD procedures, guidance, and supplemental information.

DoD Enterprise Software Initiative (ESI)
A joint initiative sponsored by the DoD Chief Information Officer to save time and money on commercial software, IT hardware, and services. Knowledgeable and experienced Component team members identify and consolidate DoD-wide IT requirements to establish enterprise agreements with IT providers. Impacts include lower procurement costs, more efficient acquisition processes, and greater visibility into IT assets across the entire department.

TOC

DoD FMR
The DoD FMR directs statutory and regulatory financial management requirements, systems, and functions for all appropriated and non-appropriated, working capital, revolving, and trust fund activities.

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.

FAR
Federal Acquisition Regulation is the primary regulation that governs all federal acquisitions.

Gantt Chart
A graphical depiction of a project schedule. A type of bar chart that shows the start and finish dates of several elements of a project that include resources, milestones, tasks and dependencies.

Government-wide Acquisition Contract
A GWAC is a type of Indefinite-delivery contract that has been awarded by another agency. The rules of FAR 16.505 apply. Other agencies can use the contract IAW its terms and conditions, but often a fee is associated with usage. If there are multiple awardees on the contract, they must be given a fair opportunity to be considered for the order. Proper Use of Non-DoD Agency documentation may be required depending on who awarded the contract.

Hotspot
A wireless LAN (local area network) node that provides Internet connection and virtual private network (VPN) access from a given location (also see Air Card).

Information Technology Services
Means the performance of any work related to IT and the operation of IT, including national security Systems. This includes work outsourced IT-based business processes, outsourced information technology, and outsourced information functions.

Internal Control
The organization policies and procedures that help program and financial managers achieve results and safeguard the integrity of their programs by reducing the risk of adverse activities. They are techniques and devices employed by managers to ensure that what should occur in their daily operations does occur on a continuing basis.

Invoicing Receipt Acceptance and Property Transfer
iRAPT is the system that allows DoD to reach its e-invoicing goals and reduce interest penalties due to lost or misplaced documents. iRAPT was known as WAWF until release
5.6.0 in 2014 when the name was changed.

Leads
Person assigned by command elements to lead acquisition efforts and teams through the process. Some terms used to identify leads are PM, Action Officer, or End Users.

Managers' Internal Control Program
Managers Internal Control Program (MCIP) serves as an overarching program under which the DoD complies with a host of laws and regulatory requirements with the primary three being the Federal Managers

TOC

Financial Integrity Act of 1982, the Federal Financial Management Improvement Act of 1996, and the Government Performance and Results Act.

Market Research
Collecting and analyzing information about capabilities within a market to satisfy agency needs and comply with FAR requirements.

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

Procurement Administrative Lead Time
The estimated amount of time required to award a contract action once a requirements package has been accepted by a supporting contracting agency. The standard PALT for contract actions reflects the amount of time generally required to process procurements in accordance with FAR, DFARS, AFARS and is affected by acquisition strategy, program dollar value, complexity, risk, and the authority level for approving acquisition documents.

Performance Requirements Summary
The document used to capture the desired outcomes, performance objectives, performance standards, and Acceptable Quality Levels (AQL) that measure contractor performance. The PRS serves as the baseline for the PWS. It should be brief and capture the critical elements of the requirement. In the actual PWS, the acquisition team will elaborate on and describe the requirement in detail. The ultimate goal is to describe the requirement in a way that allows an offer or to understand fully what will be necessary to accomplish it.

Personal Services
A personal service is characterized by the employer-employee relationship it creates between the government and the contractor's personnel. The government is normally required to obtain its employees by direct hire under competitive appointment or other procedures required by the civil service laws. Obtaining personal services by contract, rather than by direct hire, circumvents those laws unless Congress has specifically authorized acquisition of the services by contract as indicated in FAR 37.104. In a personal services contract, the contractor is considered to be, and is treated as, an employee of the government. In this type of relationship, a government officer or employee directly supervises and controls the contractor's personnel on a continuing basis. Personal service contracts require specific authorization.

Performance Work Statement
The PWS should state requirements in general terms of what (result) is to be done, rather than how (method) it is done. The PWS gives the contractor maximum flexibility to devise the best method to accomplish the required result. The PWS must ensure that all offerors can compete equally. The U.S. Government must remove any features that could restrict a potential offeror. However, the PWS must also be descriptive and specific enough to protect the interests of the U.S. Government and to promote competition. The clarity and explicitness of the requirements in the PWS will invariably enhance the quality of the proposals submitted. A definitive PWS is likely to produce definitive proposals, thus reducing the time needed to evaluate proposals

QASP
The QASP describes what the Government will do to ensure that contractor performance is executed in accordance with the contract requirements and performance standards.

TOC

Quality Assurance Surveillance Plan
The key Government-developed surveillance process document that is applied to Performance-Based Service Contracting (PBSC) and is used to manage contractor performance assessment by ensuring that systematic quality assurance methods are utilized to validate that the contractor's quality control efforts are timely, effective, and are delivering the results specified in the contract or task order. The QASP directly corresponds to the performance objectives and standards (i.e., quality, quantity, timeliness) specified in the PWS and details how, when and by whom the Government will survey, observe, test, sample, evaluate, and document contractor performance results to determine whether the contractor has met the required standards for each objective in the PWS.

Request for Service Contract Approval
Army Federal Acquisition Regulation Supplement (AFARS) Subpart 5107.503(e) requires the completion of the Request for services Contract Approval (RSCA) form. KOs must ensure that requiring officials provide a copy of a RSCA signed by an appropriate General Officer or member of the Senior Executive Service. KOs shall not issue a solicitation for a service requirement or award any service contract or order, modify a service contract or order to add new work, or exercise an option under a service contract or order, without an approved certification. The KO shall include the approval and completed worksheets in the official contract file. The general officer or senior executive may delegate certification authority for requirements valued less than $1,000,000 in accordance with Command Policy. KOs shall document the contract file with a copy of the Command Policy before accepting a service approval that has a signature below the General Officer/Senior Executive level. An RSCA is also referred to as a SCA.

Requiring Activity
The organization that receives the benefits of a goods or services contract, or the entity responsible for making contractual provisions for requirements in order to meet mission objectives.

Services
For purposes of this regulation, the term "service" means the engagement of the time and effort of a contractor whose primary purpose is to perform an identifiable task, or tasks, rather than to furnish an end item of supply.

Select & Native Programming Data Input System -- Information Technology
SNaP-IT is the authoritative DoD database used for publishing the DoD IT Budget Estimates to Congress, the Circular A-11 Section 53 and Section 300 exhibits to the Office of Management and Budget (OMB), and for monthly IT performance reporting to the Federal IT dashboard. Snap-IT is operated by the Assistant Secretary of Defense for Networks and Integration/DoD Chief Information Officer (ASD (NII)/DoD CIO). Additional Snap-IT guidance can be located within Management Regulation (7000.14-R, Volume 2B, Chapter 18) or within annual budget guidance issued by OUSD(C), D, CAPE, and DoD CIO.

SourceAmerica
Non-profit agency that participates in the Ability One Program (formerly known as NISH).

Source Selection Evaluation Board
A group of military and/or government civilian personnel, representing functional and technical disciplines, that is charged with evaluating proposals and developing summary facts and findings during source selection.

TOC

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

Supplies
Supplies mean all property except land or interest in land. It includes (but is not limited to) public works, buildings, and facilities; ships, floating equipment, and vessels of every character, type, and description, together with parts and accessories; aircraft and aircraft parts, accessories, and equipment; machine tools; and the alteration or installation of any of the foregoing.

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.

Timely Manner
A timely manner means planning and initiating procurement requirements to ensure services and supplies are available when required to meet organizational needs. This requires backwards planning to factor in the time necessary to complete the internal process, and adhere to the procurement acquisition lead-time established by the supporting contracting agency.

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/MEIT-CSD-ENB telephone operations for further processing.