DEPARTMENT OF THE ARMY
WASHINGTON, DC 20310

20 JUL 2005

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Knowledge Management (AKM) Guidance Memorandum – Capabilities-Based Information Technology (IT) Portfolio Governance

1. The enclosures establish governance structures and processes to effectively identify and manage the Army's IT-based capabilities and associated investments.

2. Army Mission Areas and subordinate Domain Leads are specified and assigned responsibilities for IT investment decisions in enclosures 1 and 2. IT investments must support the Army's strategic goals, mission, and interrelated strategies. Investments in duplicative or stove-piped systems, or systems not in compliance with Army and DoD standards, will be terminated.

3. Our goal is to reduce redundant and stove-piped IT investments by 80% by the end of Fiscal Year 2007. Failure to vet IT investments through Mission Area and Domain Leads will result in the withdrawal of funds from the sponsoring organization until the IT investment is adjudicated by the Mission Area and Domain Leads.

4. The Chief Information Officer/G-6, in coordination with Mission Area and Domain Leads, will issue portfolio management implementing instructions within 60 days. The Mission Area and Domain Leads will identify other domains and sub-domains as appropriate, and assign their leads within 60 days.

5. The CIO/G-6 is the proponent for this memorandum.

Peter J. Schoomaker
General, US Army
Chief of Staff

Francis J. Harvey
Secretary of the Army

4 Encls
1-2. as
3. References
4. Definitions

SUBJECT: Army Knowledge Management (AKM) Guidance Memorandum – Capabilities-Based Information Technology (IT) Portfolio Governance

DISTRIBUTION:
ASSISTANT SECRETARY OF THE ARMY FOR ACQUISITION, LOGISTICS, AND TECHNOLOGY
ASSISTANT SECRETARY OF THE ARMY FOR CIVIL WORKS
ASSISTANT SECRETARY OF THE ARMY FOR FINANCIAL MANAGEMENT & COMPTROLLER
ASSISTANT SECRETARY OF THE ARMY FOR INSTALLATIONS AND ENVIRONMENT
ASSISTANT SECRETARY OF THE ARMY FOR MANPOWER AND RESERVE AFFAIRS
GENERAL COUNSEL
ADMINISTRATIVE ASSISTANT TO THE SECRETARY OF THE ARMY
CHIEF INFORMATION OFFICER/G-6
THE INSPECTOR GENERAL
THE AUDITOR GENERAL
DEPUTY UNDER SECRETARY OF THE ARMY (OPERATIONS RESEARCH)
CHIEF OF PUBLIC AFFAIRS
DIRECTOR, ARMY STAFF
DEPUTY CHIEF OF STAFF FOR PERSONNEL/G-1
DEPUTY CHIEF OF STAFF FOR INTELLIGENCE/G-2
DEPUTY CHIEF OF STAFF FOR OPERATIONS AND PLANS/G-3/5/7
DEPUTY CHIEF OF STAFF FOR LOGISTICS/G-4
DEPUTY CHIEF OF STAFF FOR PROGRAMS/G-8
ASSISTANT CHIEF OF STAFF FOR INSTALLATION MANAGEMENT
THE SURGEON GENERAL
CHIEF, NATIONAL GUARD BUREAU
CHIEF OF ARMY RESERVE
THE JUDGE ADVOCATE GENERAL
CHIEF OF CHAPLAINS

COMMANDER:
U.S. ARMY EUROPE, AND SEVENTH ARMY
EIGHTH U.S. ARMY
U.S. ARMY FORCES COMMAND
U.S. ARMY TRAINING AND DOCTRINE COMMAND
U.S. ARMY MATERIEL COMMAND
U.S. ARMY CORPS OF ENGINEERS
U.S. ARMY SPECIAL OPERATIONS COMMAND
U.S. ARMY PACIFIC
U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
MILITARY SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND
U.S. ARMY CRIMINAL INVESTIGATION COMMAND

SUBJECT: Army Knowledge Management (AKM) Guidance Memorandum – Capabilities-Based Information Technology (IT) Portfolio Governance

DISTRIBUTION (CONT'D)
U.S. ARMY MEDICAL COMMAND
COMMANDER
U.S. ARMY MILITARY DISTRICT OF WASHINGTON
U.S. ARMY SOUTH
U.S. ARMY TESTING AND EVALUATION COMMAND
U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND
SUPERINTENDENT, U.S. MILITARY ACADEMY

CF: PROGRAM EXECUTIVE OFFICER
COMMAND, CONTROL, AND COMMUNICATIONS TACTICAL (PEO C3T)
ENTERPRISE INFORMATION SYSTEMS (PEO-EIS)

SUBJECT: Army Knowledge Management (AKM) Guidance Memorandum – Capabilities-Based Information Technology (IT) Portfolio Governance

Enclosure 1 – Governance Structure

1. This enclosure identifies and maps Army functional proponents to DoD Mission Areas and Domains. It further delineates the four Global Information Grid (GIG) Enterprise Services (ES) Mission Areas (MA), the Army MA Leads and Domain Lead roles and responsibilities for managing capabilities-based Information Technology (IT) investments. Mission Area Leads may delegate these responsibilities to the supporting Army General Staff activity. In addition, Domain Leads may delegate to the supporting Army General Staff activity upon approval of the Mission Area Lead and in coordination with the CIO/G-6.

2. Listed are the four GIG ES MAs. The Army MA Leads are designated below.

Mission Areas	**DoD Leads**	**Army Leads**
Warfighting	Chairman, Joint Chiefs of Staff (CJCS)	Deputy Chief of Staff, G-3/5/7
Business	USD, (AT&L)	Under Secretary of the Army (USA)
Enterprise Information Environment	Assistant Secretary of Defense (Networks & Information Integration)/DoD Chief Information Officer (ASD(NII))	Chief Information Officer/ G-6 (CIO/G-6)
DoD Portion of National Intelligence	Under Secretary of Defense (Intelligence) (USD(I))	Deputy Chief of Staff, G-2

3. The Army Domain Leads within the MAs are designated below.

Mission Areas/Domains	**DoD Leads**	**Army Leads**
Warfighting Mission Area	**Chairman, Joint Chiefs of Staff (CJCS)**	**Deputy Chief of Staff, G-3/5/7**
Battlespace Awareness Domain	Vice Director of Intelligence; Joint Staff, J-2	Deputy Chief of Staff, G-2
Force Application Domain	Deputy Director for Joint Warfighting Capability Assessments; Joint Staff, J-8	Deputy Chief of Staff, G-8
Protection Domain	Deputy Director for Force Protection; Joint Staff, J-8	Deputy Chief of Staff, G-8
Focused Logistics Domain	Vice Director for Logistics, Joint Staff, J-4	Deputy Chief of Staff, G-4
Battlespace Communications Systems Domain	Vice Director for Command, Control, Communications and Computer Systems, Joint Staff, J-6	CIO/G-6

Mission Areas/ Domains	**OSD Leads**	**Army Leads**
DoD Portion of National Intelligence Mission Area	**USD(I)**	**Deputy Chief of Staff, G-2**
Business Mission Area	**USD, (AT&L)**	**USA**
Acquisition Domain	Under Secretary of Defense (Acquisition, Technology and Logistics) (USD(AT&L))	Assistant Secretary of the Army (Acquisition, Logistics & Technology) (ASA(AL&T))
Financial Management	Under Secretary of Defense (Comptroller) (USD(C)	Assistant Secretary of the Army (Financial Management & Comptroller) (ASA (FM&C))
Human Resources Management Domain	Under Secretary of Defense (Personnel and Readiness) (USD(P&R))	Assistant Secretary of the Army (Manpower & Reserve Affairs) (ASA(MR&A))
Logistics Domain	Deputy Under Secretary of Defense (Acquisition, Technology and Logistics) (USD(AT&L))	Assistant Secretary of the Army (Acquisition Logistics & Technology(ASA(AL&T))
Installations & Environment Domain	USD(AT&L)	Assistant Secretary of the Army (Installations and Environment)(ASA(I&E))
Civil Works	N/A	Assistant Secretary of the Army (Civil Works) ASA(CW)
Enterprise Information Environment Mission Area	**ASD(NII)**	**CIO/ G-6**
Communications Domain	Director, Wireless	CIO/G-6
Computing Infrastructure Domain	Director, Architecture and Interoperability	CIO/G-6
Core Enterprise Services Domain	Director, Information Management	CIO/G-6
Information Assurance Domain	Director, Information Assurance	CIO/G-6

4. The Army Mission Area/ Domain Leads will identify any additional Mission Area Domains, Sub-Domains and Leads within 60 days after this memorandum is published.

1. Responsibilities:

a. Mission Area Leads (Specific).

(1) The Under Secretary of the Army, or his designated representative, as the Army's Mission Area (MA) Lead for the Business Mission Area (BMA) will ensure generating force efforts are traceable to, and fully support, the required capabilities for DoD Warfighting, Intelligence, and EIE Mission Areas. Additionally, this MA Lead will ensure that a single integrated Architecture for the BMA efforts exists to support the Business Enterprise Architecture (BEA).

(2) The Chief Information Officer/G-6, as the Army's Mission Area Lead for Enterprise Information Environment (EIEMA), will support the DoD EIE Mission Lead and ensure EIE efforts are traceable to, and fully enable, the required capabilities for the Warfighting, Intelligence and Business Mission Areas.

(3) The Deputy Chief of Staff, G-3/5/7, as the Army's Mission Area Lead for Warfighting (WMA) will approve, prioritize, and synchronize all GIG capabilities, experimentation, concepts, and operational architecture development efforts for the WMA.

(4) The Deputy Chief of Staff, G-2, as the Army's Mission Area Lead for National Intelligence and National Intelligence Technology Infrastructure will ensure that intelligence efforts are traceable to, and fully support, the required capabilities for DoD Warfighting and EIE Mission Areas. Additionally, this MA Lead will ensure that a single integrated architecture for the National Geospatial-Intelligence Agency efforts exists to support the Battlespace Awareness Domain of the WMA.

b. Mission Area Leads (General).

(1) Establish direction and plans for MA GIG capabilities Enterprise Solutions, experimentation, concepts, and operational architecture development efforts.

(2) Establish key metrics and targets by which to track IT transformation.

(3) Will identify Domains and sub-Domain Leads and ensure linkages to existing DoD Domains.

(4) Establish MA Portfolio Management policies that comply with DoD and Army guidance. Implement the IT portfolio management process developed by DoD and the Army to define and justify planned IT expenditures as being consistent with IT enterprise solutions against needed capabilities.

(5) Require portfolio reviews to be conducted for each subordinate Domain, ensuring their IT capabilities are represented by appropriate resource needs and priorities. The CIO/G-6 is establishing a portfolio review process for managing IT investments as portfolios. Portfolio reviews will be briefed to the CIO/G-6 and this information will be used to provide quarterly updates to OSD. This will also clarify and standardize the review process, and assign accountability for follow-on actions.

(6) Develop outcome-oriented performance measures that are aligned with strategic guidance from the President, Secretary of Defense, Secretary of the Army, and strategic goals and objectives of the Mission Area, in coordination with CIO/G-6.

c. Domain Leads.

(1) Implement the IT portfolio management process developed by DoD and the Army to define and justify the portfolio planned IT expenditures consistent with strategic imperatives and operational requirements.

(2) Identify the Domain's technical infrastructure and IT enterprise solutions against needed capabilities.

(3) Utilize portfolio management tools to determine within Domains where redundancies exist and where integration of products and services might better support warfighter needs.

(4) Recommend opportunities for cross domain integration to continually improve delivery of IT-based capabilities in support of warfighter needs.

(5) Utilize existing Army processes to prioritize, synchronize and fund opportunities identified by portfolio management processes.

(6) Initially document the business case analysis for those planned IT expenditures that require USD, Comptroller approval before an obligation of funds in excess of $1M in a fiscal year can be incurred for system improvements. (The scope of this requirement will be changed when criteria/thresholds are established for reporting IT expenditures.)

(7) Ensure Domain investments focus on capabilities, and include the full life cycle of IT expenditures in their assigned Mission Area.

(8) Participate in enterprise governance forums led by the CIO/G-6 aimed at identifying opportunities for commonality in portfolio management techniques, and providing solutions that are in the best interest of the Enterprise.

(9) Ensure IT systems/initiatives are registered in the AITR.

(10) Establish and utilize outcome-oriented IT performance measures that are aligned with strategic guidance and the MA scorecard. Progress will be reviewed and reported through the governance structure.

(11) Implement the DoD Data Strategy by exposing Domain data to the enterprise (tagging and cataloging) and facilitating/supporting the formation of Communities of Interest.

(12) Coordinate with the G-3/5/7, and the G-8 to ensure issues of portfolio/system prioritization and funding are addressed during portfolio reviews.

(13) Provide a plan to collectively identify Army Enterprise-wide end-to-end processes and assignment of process owners.

d. G3/5/7.

(1) Serve as the ARSTAF focal point for organization, integration, decision-making, and execution of the spectrum of activities encompassing requirements definition, force development, force integration, force structuring, combat developments, training developments, resourcing, and prioritization.

(2) Serve as the focal point for prioritization, integration, and synchronization of capabilities and requirements made both on the ARSTAF and externally.

(3) Serve as the overall integrator of Army transformation.

e. G-8.

(1) Manage the programming phase of the Army Planning, Programming and Budgeting System (PPBES) to facilitate the development of the Army program and the transition to an Army Budget Estimate Submission (BES).

(2) Responsible for transitioning approved Army requirements from the planning to the programming phase.

(3) Responsible as principal advisor to the CSA on Joint materiel requirements, doctrine, training, leader development, organizations, and materiel - personnel and facilities (DTLOM-PF) integration, and materiel program execution over their life cycles.

f. CIO/G-6.

(1) Serve as the Executive Secretary to the Senior Review Group during the conduct of Information Technology Portfolio Management reviews.

(2) Provide IT Portfolio Management policy guidance and oversee implementation of Mission Area IT portfolios to ensure they are aligned with Army Enterprise Solutions.

(3) Serve as the single Army interface with the Office of the Secretary of Defense (OSD), GIG ES implementing organizations, and stakeholder organizations for all data calls and other IT investment-related actions.

(4) Review and revise the current process for maximizing the value, and assessing and managing the risks of Army IT investments across the enterprise, ensuring consistency with evolving DoD policy.

(5) Review and revise the Army IT Portfolio Management Process IAW evolving DoD guidance/policy, fully incorporating the DoD Mission Area/Domain construct and the necessary program review requirements. Ensure portfolio management processes are incorporated into, and integrated with, each of the principal decision support systems: Joint Capabilities Integration and Development System (JCIDS), PPBES, and the Defense Acquisition System.

(6) Establish enterprise level performance measures as an integral component of the transformation strategy, aligned with mission, vision, goals and objectives.

(7) Maintain the Army Information Technology Registry (AITR) as the official Army inventory of systems/initiatives, and investigate potential alternatives for a database that can integrate and enhance support to the portfolio management process.

(8) In conjunction with the Assistant Secretary of Defense (Networks and Information Integration) (ASD (NII)), integrate the architectures that support enterprise IT solutions.

(9) Provide Departmental level policy, guidance and direction in the definition, design, implementation and integration of enterprise solutions and business process improvements across the Army and between the Department of Defense, the Army and other external organizations.

g. The Senior Review Group (SRG) will serve as the overarching governance body for integration decisions between GIG ES Mission Areas pertaining to IT Portfolio Investments and establish a framework for resolving cross-Mission Area IT Portfolio issues. The SRG will:

(1) Resolve resource allocations and other issues;

(2) Monitor staff implementation of decisions;

(3) Recommend prioritization of programs unresolved at lower levels;

(4) Recommend resource alternatives;

(5) Establish strategic direction for Mission Areas; and,

(6) Establish key metrics and targets by which to track progress.

2. Follow-on actions.

a. The CIO/G-6 will:

(1) Develop implementing guidance in coordination with the ARSTAFF within 60 days after this memorandum is published.

(2) Incorporate this guidance into the next revision of Army Regulations 10-5 and 25-1.

(3) Track and measure progress of the capabilities provided by IT investments against the established performance criteria.

b. The Army Mission Area/ Domain Leads will (within 60 days after this memorandum is published):

(1) Identify any additional Mission Area Domains, Sub-Domains and Leads.

(2) Provide a plan to identify their Mission Area IT performance measures aligned with strategic guidance.

3. The CIO/G-6 will provide core criteria and metrics to track and measure capabilities provided by IT investments against the established performance criteria embedded in the Strategic Readiness System (SRS). Portfolio management and the governance structure outlined in this memorandum will serve to strengthen and reinforce the teamwork processes already in place throughout the Army to increase our warfighting effectiveness and efficiency.

References:

a. Goldwater-Nichols Act of 1986 (10 USC, Subtitle A, Part 1, Chapter 5).

b. Clinger Cohen Act (40 USC §§ 11312 & 11315).

c. OMB Circular No. A-130, Management of Federal Information Resources, Revised, November 28, 2000, (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html).

d. DepSecDef Memorandum, Information Technology Portfolio Management, March 22, 2004.

e. HQDA General Order 2002-03, Assignment of Functions and Responsibilities within Headquarters, Department of the Army, July 9, 2002.

f. CJCS Memorandum, Assignment of Warfighting Mission Area (WMA) Responsibilities to Support Global Information Grid Enterprises Services (GIG ES), September 8, 2004.

g. DoD CIO Memorandum, Enterprise Information Environment Mission Area (EIEMA) Domain Owner Designations, July 14, 2004.

h. The Ronald W. Reagan National Defense Authorization Act for Fiscal Year (FY) 2005, § 332: Defense Business Enterprise Architecture.

i. VCSA Memorandum, Global Information Grid Mission Area Roles, Responsibilities, and Development, October 8, 2004.

Definitions

Domain. An area of common operational and functional requirements.

Enterprise. The highest level in an organization; it includes all missions, tasks, and activities or functions.

Enterprise Information Environment (EIE). The common, integrated computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, or that assure, local area networks, campus area networks, tactical networks, operational area networks, metropolitan area networks, and wide area networks. The EIE is also composed of GIG organizational, regional, or global computing capabilities. The EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the GIG. The EIE includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, and delivery of information on the GIG.

Enterprise Process. Enterprise processes are those end-to-end groupings of integrated and interrelated functions across Domain and Mission Areas that provide mission-critical capabilities to the warfighter, and form the basis for the enterprise architecture.

Enterprise Process Owners. Key decision makers on Army Enterprise process issues; interface with the Mission Area and Domain Leads to conduct portfolio management of process enablers; approve end-to-end process scenarios to facilitate design and implementation of process capabilities; and champion the use of Enterprise Solutions as process enablers.

Global Information Grid (GIG). The globally connected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Governance. The process through which organizations make strategic decisions, determine whom they involve and demonstrate accountability for the results of their actions. The process of governance relies on a system or framework – to include Federal statutes; DOD and Army directives, policies or guidelines; steering committees or groups; and performance measures – to define how the process is supposed to function in a particular setting. Cultural traditions, accepted practices, and codes of conduct are also instrumental in influencing the governance process. Ideally, the governance process achieves agreement between differing interests to reach a broad consensus on what is in the best interest of the enterprise.

Enclosure 4 – Definitions

Information Technology (IT). 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 the DoD Component. The term "information technology" includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related sources.

Information Technology (IT) Portfolio. A grouping of IT capabilities, IT systems, IT services, IT system support services (e.g. IT required to support and maintain systems), management, and related investments required to accomplish a specific functional goal. Decisions to make, modify, or terminate IT investments shall be based on the GIG integrated architecture, Mission Area goals, risk tolerance levels, potential returns, outcome goals, and performance.

Initiative. Initiatives are IT systems, programs, projects, organizations, activities or family of systems.

Mission Area (MA). A defined area of responsibility with functions and processes that contribute to mission accomplishment.

National Security Systems (NSS). Any telecommunications or information system operated by the US Government, the function, operation, or uses of which 1) involves intelligence activities, 2) involves cryptologic activities related to national security, 3) involves command and control of military forces, 4) involves equipment that is an integral part of a weapon or weapons system, or 5) is critical to the direct fulfillment of military and intelligence missions (ref. the Clinger-Cohen Act of 1996)

Portfolio Management. The management of selected groupings of IT investments using integrated strategic planning, integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio investment strategies. The core activities associated with portfolio management are: analysis, selection, control, and evaluation.

System. An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. Within the context of the Army Enterprise Architecture, systems are people, machines, and methods organized to accomplish a set of specific functions; provide a capability or satisfy a stated need or objective; pr produce, use, transform, or exchange information. For the purpose of reporting to the Army Information Technology Registry (AITR), the term s "application" and "system" are used synonymously – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information (that is, the application of IT).