

## Chapter 16

# Army Knowledge Management

### Section I

#### Introduction

*The Army Knowledge Vision - A transformed Army, with agile capabilities and adaptive processes, powered by world class network-centric access to knowledge, systems and services, interoperable with the Joint environment.*

#### 16-1. Transformation Strategy

a. The Army is undergoing its most fundamental change in over a century while still being fully dedicated to the global war on terrorism. Army Transformation is all about transitioning from information-based to knowledge-based operations. Achieving the Army Knowledge Vision will provide the ability to achieve decision superiority and take decisive action across the spectrum - this includes both the tactical and institutional Army.

b. The Office of the Army CIO/G-6 continues to work toward the Enterprise vision of a single Army network, one Enterprise Army portal, and universal access to Army knowledge, managed by the U.S. Army Network Enterprise Technology Command (NETCOM). AKO, the Army's knowledge portal has grown to over one million soldier and civilian registered users. Through the leadership of the Army CIO Executive Board (EB), strong governance procedures for the Enterprise control of our command, control, communications, computers/information technologies (C4/IT) budget have been institutionalized, information management organizations have been realigned, and the Army Knowledge Enterprise Architecture (AKEA) has been defined.

c. Army Knowledge Management (AKM) is the comprehensive strategy to transform the Army into a network-centric, knowledge-based force. The strategy consists of a robust set of goals and objectives, which once achieved, will improve the decision dominance of our tactical commanders and our business stewards. These goals and objectives concentrate on managing the information technology (IT) infrastructure as an Enterprise in line with the Global Information Grid (GIG), with a view toward reducing the resource and equipment footprint and creating ubiquitous access through AKO as the Enterprise portal to knowledge centers, functional applications and network services. The use of best business and governance practices and the emphasis on innovative human capital strategies are key goals of AKM.

d. The AKM strategy enables transformation to the Objective Force and is based on a framework which includes: a robust infostructure, effective applied intellectual capital, and change catalysts required to enable transformation.

- Infostructure: The IT, (computers, software, architecture, security, communications, programs, and facilities) required to support the network-centric Army.
- Intellectual Capital: Individual, team, and Enterprise knowledge, systems, and services, and workforce strategies that are necessary to improve operations and decision making.
- Change Catalysts: The policies, resources, management, culture, processes, and education that are required to optimize the adaptive organization and enterprise net-centric environment.

#### 16-2. Implementation

a. The implementation of AKM means:

- (1) The infrastructure must accommodate faster processing capabilities and dissemination of requirements;
- (2) The Enterprise-wide system must be easily accessible with network-centric processes and services available through a single portal;
- (3) The information that leads to knowledge must be well organized and structured through content management;
- (4) The ability to generate knowledge requires the transfer and sharing of knowledge across the Enterprise using such techniques as collaborative processes, virtual teams, and communities of practice; and
- (5) We must recruit, train, and retain an interdisciplinary workforce (soldiers and civilians) empowered to share knowledge.

b. The implementation of AKM at the strategic, operational and tactical levels of war means designing and fielding an Enterprise-information infrastructure capable of increased data distribution and faster processing. The AKM strategy defines the AKEA framework to achieve a knowledge-based, network-centric Enterprise that uses advanced Command, Control, Communications, Computers and Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities to improve its warfighting capabilities at the tactical level. Unlike the former Army Enterprise Architecture construct, the AKEA encompasses the full spectrum of both the tactical, operational and strategic levels of war by incorporating the tactical and functional applications, computing services and communications networks into virtually one network with a single access to the Army's knowledge centers.

c. Under the HQDA Realignment in December 2001, IM across the entire Army was realigned to increase organizational effectiveness and operational performance at the Enterprise level. IM realignment objectives transformed

## How the Army Runs

the former Director of Information Systems for Command, Control, Communications and Computers (DISC4) into the Army CIO/G-6.

*d.* The Army CIO/G-6 provides Enterprise management of the AKEA through NETCOM, the Army's single authority to operate, manage, sustain, and defend the Army's infostructure at the Enterprise level. The NETCOM consists of the former U.S. Army Signal Command and other operational organizations and functions transferred from the former DISC4. The NETCOM established regional CIO offices in coordination with the Transformation Installation Management (TIM) realignment to provide management and oversight of installation operations in the TIM regions. The TIM realignment is in concert with the recent assignment of oversight of Command, Control, Communications, Computers, & Intelligence/Information Technology (C4I/IT) funding as part of AKM.

*e.* AKM gets the right information to the right person at the right time to make the right decisions. The Army's transformation is ongoing; we must continually assess our past accomplishments and move forward with urgency.

*f.* All source documents relating to the Transformation Strategy are located behind AKO at [https://www.us.army.mil/portal/portal\\_home.jhtml](https://www.us.army.mil/portal/portal_home.jhtml). Once there select the "Collaborate" tab and expand the "Army Communities" and "Army CIO/G-6" folders to locate the documents. You must first subscribe to these communities and knowledge centers prior to viewing any documents.

## Section II

### Chief Information Officer (CIO)/G-6 roles and responsibilities

#### 16-3. Clinger-Cohen Act (CCA)

*a. Law.* On 10 February 1996, the Information Technology Management Reform Act (ITMRA) became law as Division E of the National Defense Authorization Act for Fiscal Year 1996, Public Law 104-106. The law later designated as the Clinger-Cohen Act (CCA), directed that each executive agency appoint a CIO who reports directly to the head of the agency. The law required:

- Development of information resources management using a sound integrated technology architecture.
- Promotion, design, and operation of a major information resources management process, monitoring IT for the agency.
- Assessment of personnel to achieve the requirements of the information system.

*b. CCA objectives.* The CCA increased the SECARMY responsibility, authority, and accountability for the use of IT and other information resources in performing Army missions. The National Security Systems provisions of the CCA include the CIO responsibility for any telecommunications or information system operated by the U.S. Government, the function, operation or use of which involves: intelligence activities; crypto-logic activities related to national security; command and control (C2) of military forces; or, equipment that is an integral part of a weapon or weapons system. The CCA emphasized the importance of completing effective planning, analyzing processes, and, where appropriate, improving processes before applying C4I/IT solutions to known requirements. The CCA requires a process for maximizing the value, managing, and assessing the risks of IT acquisitions. The entire text of the CCA can be viewed at [http://www.itpolicy.gsa.gov/mks/regs-leg/s1124\\_en.htm](http://www.itpolicy.gsa.gov/mks/regs-leg/s1124_en.htm).

*c. Army CIO Responsibilities.* The Army CIO is the functional proponent for Command, Control, Communications, Computers and IM (C4/IM) and maintains the Enterprise policy, guidance, oversight, and resource management for all Army C4/IM efforts and also serves as the principal advisor to the SecArmy and Chief of Staff, Army (CSA) and other Army senior leaders on all matters related to managing and overseeing the Army-wide implementation of CCA mandated functions. This includes providing direction and guidance for the Transformation of the Army into a network centric, knowledge-based Enterprise and force. Focus areas within the CCA follow:

(1) *Business process analysis/improvement.*

(a) Sec. 5113(b)(2)(C): "...analyze the missions of the executive agency and based on the analysis, revise the executive agency's mission-related processes and administrative processes, as appropriate, before making significant investments in IT to be used in support of those missions..."

(b) Sec. 5125(b)(3): "Promote the effective and efficient design and operation of all major information resources management (IRM) processes..., including improvements to work processes."

(2) *Information assurance.* Sec. 5113(b)(2)(D): "...ensure that the information security policies, procedures, and practices are adequate."

(3) *Information resources management.*

(a) Sec. 5125(b)(1): "providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that IT is managed for the executive agency..."

(b) Sec. 5125(b)(3): "...promoting the effective and efficient design and operation of all major information resources management processes for the executive agency."

(4) *IT architecture.* Sec. 5125(b)(2): "developing, maintaining, and facilitating the implementation of a sound and integrated IT architecture for the executive agency."

(5) *IT acquisition oversight.* Sec. 5125(c)(2): "...monitor the performance of IT programs of the agency, evaluate the

performance of those programs on the basis of the applicable performance measurements, and advise the head of the agency regarding whether to continue, modify, or terminate a program or project;”

(6) *Capital IT investment control.* Sec. 5125(c)(2): “...monitor the performance of IT programs of the agency, evaluate the performance of those programs on the basis of the applicable performance measurements, and advise the head of the agency regarding whether to continue, modify, or terminate a program or project.”

(7) *Professional development and training.*

(a) Sec. 5125(c)(3)(A): “Assess requirements established for agency personnel regarding knowledge and skill in IRM and adequacy of such requirements for facilitating achievement of the IRM performance goals.”

(b) Sec. 5125(c)(3)(B): “Assess the extent to which the executive and management levels of the Army meet the IRM knowledge and skills requirements.”

(c) Sec. 5125(c)(3)(C): “...develop strategies and specific plans for hiring, training and professional development” in the areas of IRM and IT.

d. *G-6 Responsibilities.* The SecArmy and the CSA redesignated the ARSTAF using FM 101-5 (G-staff) terminology. The CIO is on the Secretariat staff, and is also designated the G-6 by the CSA. The G-6 serves at the staff principal for all matters concerning information and signal operations, network and communications security, force structure, equipping, and employment of signal forces.

(1) *Information and Signal Operations:*

(a) Manages and controls the use of information network capabilities and network services from the sustaining base to the forward most fighting platforms.

(b) Manages radio frequency allocations and assignments and provides spectrum management.

(c) Recommends signal support priorities for force information operations.

(d) Recommends locations for command posts within information battle space.

(e) Manages all signal support interfaces with joint and multinational forces, including host nation support interfaces.

(f) Manages the command frequencies lists.

(g) Manages communications protocols, and coordinates user interfaces of Defense Information System Networks (DISNs) and command and control systems down to battalion tactical internets.

(h) Ensures redundant signal means are available to pass time-sensitive battle command information from collectors to processors and between medical units and supporting medical laboratories.

(2) *Network and Communications Security:*

(a) Manages communications security (COMSEC) measures, including the operation of the Information System Security Office (ISSO).

(b) Establishes information systems security for all software and hardware employed by the force.

(c) Recommends C2-protect priority information requirements.

(d) Manages the Army Information Systems Security Program (ISSP).

(e) Manages Army computer network software.

(3) *Force Structure, Equipping and Employment of Signal Forces.*

(a) Manages employment of signal forces to support current/near term operations.

(b) Plans signal support structure for future systems.

#### **16-4. Army Knowledge Management (AKM)**

a. Knowledge management provides the Army with overall strategy, oversight and guidance in the area of AKM development and implementation at the Enterprise level and facilitates the transformation of the Army into a world-class, net-centric organization with access to agile and adaptive knowledge, systems and services. The CIO/G-6 manages and oversees the integration of AKM goal efforts across the Army while promulgating Enterprise solutions through managing knowledge goals, objectives, and C4/IM enabled solutions for the Army. As the functional proponent for AKO, the CIO/G-6 determines and integrates Enterprise resources, plans and policy requirements. AKM brings to the Army streamlined functional operations, the collaborative e-business model, new horizontal and virtual governance structures, evolving new technologies, and an empowered, knowledge-generating workforce. AKM goals will be achieved through active participation at every level of the Army.

b. AKM goals will be worked in parallel, not sequentially, to ensure maximum and optimal transformation.

- Goal 1: Adopt governance and cultural changes to become a knowledge-based organization.
- Goal 2: Integrate knowledge management concepts and best business practices into Army processes to improve performance.
- Goal 3: Manage the infostructure as an Enterprise to enhance capabilities and efficiencies.
- Goal 4: Institutionalize AKO as the Enterprise Portal to provide universal, secure access for the entire Army.
- Goal 5: Harness Human Capital for the Knowledge-Based Organization.

### 16–5. Army CIO Executive Board

a. The Army CIO EB was chartered in April 2001 and serves as an executive forum to advise the Army CIO on the full range of matters pertaining to IM/IT in accordance with the CCA (Public Law 104–106) and other related legislation and Federal directives. The EB is currently composed of 45 voting general officers and senior executives from the Headquarters, Department of ARSTAF agencies, MACOMs and meets on a quarterly basis. The EB also conducts its business between quarterly meetings using its private collaboration Web site located behind the AKO. The meeting minutes of the Army CIO EB are available within the AKO collaboration center at Army Communities/Army CIO/G–6/AKM/CIO Executive Board/CIO Exec BD (public)/previous meetings.

b. The purpose of the EB is to involve Army senior leadership from across functional areas in the implementation of the CCA and to identify and resolve Enterprise-level issues related to Army CIO responsibilities. In addition, the EB identifies opportunities, makes recommendations for, and sponsors cooperation in using information resources. The EB coordinates with the DOD CIO EB and the Federal CIO Council on matters of mutual interest.

c. The EB functions are identified as follows:

(1) *Management Oversight.* Advise and make recommendations to the Army CIO on overall Army IM/IT policy, processes, procedures, standards, priorities, and resources, as appropriate.

(2) *Alignment of IM/IT and Army Missions.* Ensure that IM/IT programs and systems are strategically aligned with Enterprise-wide Army missions, strategic plans, and initiatives, such as the Transformation and the QDR.

(3) *Functional System Integration.* Advise and make recommendations to the Army CIO on policies and procedures that will enhance the Army CIO's oversight and integration of IM/IT programs and systems within and across functional areas to include the horizontal integration of technology. Identify Enterprise-level CIO challenges that cross-functional boundaries and make recommendations to the CIO regarding resolution of those challenges.

(4) *Resource Allocation Process.* Recommend measures to strengthen integration of the IT capital planning and investment process with the PPBES. In addition, review IT funding and program issues and make recommendations on investment priorities and resource alignments in the context of the PPBES.

(5) *Knowledge Management.* Promote and support knowledge management concepts and initiatives throughout the Army. Identify and resolve issues relating to Enterprise knowledge management programs.

(6) *Acquisition Process.* Advise the Army CIO on program synchronization and standardization issues resulting from program and portfolio reviews. Recommend appropriate IT program and acquisition actions.

(7) *Interoperability, Information Assurance and Communications and Computing Infrastructure Reviews.* Advise and make recommendations to the Army CIO on issues of interoperability, information assurance, and communications and computing information systems infrastructures.

(8) *Human Resources Management.* Recommend and support strategies for recruiting, retaining, and training IM/IT personnel across the Army.

(9) *Architecture Management.* Assist the Army CIO in ensuring that processes are in place to enforce standardized use, management, and control of architectures.

(10) *Process Improvement and Performance Measures.* Share experiences, ideas and promising practices including work process redesign and the development of performance measures, to improve the management of information resources. Recommend and promote results-based performance measures and best practices that strengthen and optimize links between IM and Army missions, and improve Army mission performance.

(11) *Electronic Business/Electronic Commerce Operations.* Recommend measures that will promote, enhance, and safeguard the use of electronic business/electronic commerce techniques and technologies throughout the Army in such areas as smart cards and other secure electronic transactions-devices.

(12) *Other Business.* At the option of the Chair with advice of the Board, address any areas and issues not specified above.

### 16–6. C4/IT Inversement Strategy

a. The purpose of the C4/IT Investment Strategy is to make C4/IT investment recommendations that inform Army leaders and influence their POM decisions on C4/IT expenditures. The investment strategy uses a performance-based methodology and incorporates Enterprise-wide performance measures as one of its key criteria. The process also addresses capability gaps, investment risks, IT interdependencies and alignment with key Army and Joint doctrine and strategy across multiple areas of IT investment. In keeping with the legislative mandates prescribed by the CCA and Government Performance & Results Act (GPRA), the investment strategy prioritizes IT investment solutions. Investment solutions are designed to achieve the objectives of the Army and support the Army's transformation to the Objective Force. In addition, they help to ensure that the Army's portfolio of C4/IT systems is aligned with Army-wide requirements. The C4/IT Investment Strategy can be used to help determine the selection of C4/IT investments and whether to continue, modify, or terminate a C4/IT program or project.

b. The Investment Strategy helps ensure the Army's information and communications systems are strategically aligned with Enterprise-wide mission needs to achieve both dominant warfighting capabilities and world-class business process success. The strategy will identify and evaluate priorities for IT investments throughout the PPBES and acquisition processes with no dollar threshold; all C4/IT expenditures will be included in this annual MDEP or program

review process. The strategy is used throughout the calendar and budget years for planning, execution and reallocation purposes.

(1) *Portfolio Areas.* The Army Investment Strategy is composed of three portfolio areas, each with the following investment areas:

- Enterprise Enablers: Architecture, Information Assurance, and AKM.
- Communications and Infrastructure: Battlefield Communications & Network Management, Satellite Communications, and C4/IT Infrastructure.
- Functional Applications: Distance Learning/Soldier Training, Focused Logistics, Personnel Force Management Modernization & Integration, and Battle-space Awareness.

(2) *Participants.* Participants of the Investment Strategy process include multiple organizations within the Army to include the ARSTAF; MACOM/installations, Regional CIOs (RCIOs), the Army Reserve and National Guard, and NETCOM. In addition, representatives from other Federal agencies and organizations, including OSD, have participated in an observatory role.

Users of the Investment Strategy process and its strategic recommendations include but are not limited to: the Army CIO, the PEG Co-Chairs of the Installation, Equipping, Sustaining, Manning, Organizing, and Training PEGs; senior leaders of G-8, G-3, the ABO; MACOM Commanders; Combatant Commanders J-6s; Resource Review Working Group (RRWG); ACSIM; NETCOM; and the Army CIO EB.

(3) *Elements of the C4/IT Investment Strategy Process.* The C4/IT Investment Strategy process, as shown in Figure 16.1, includes multiple assessment and evaluation steps to arrive at the best-value mix of investment solutions across a broad spectrum of IT areas for the Army.

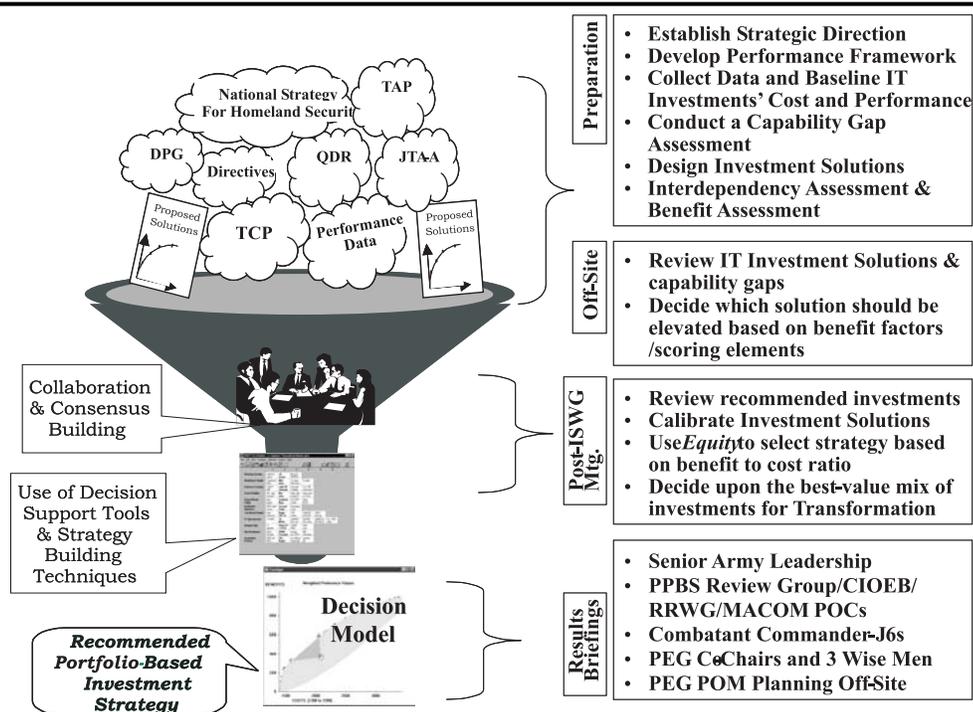


Figure 16–1. Investment Strategy Working Group Process

## How the Army Runs

c. **Performance Measurement:** This step links each investment area's mission or IT support outcomes to core competencies and resource pools, or MDEPs. Each core competency has one or more performance measures used to measure the health of the investment area. The performance measures are tracked to show progress or capability shortfalls and ultimately to help identify where investment solutions can be made to solve capability shortfalls over the POM.

- **Strategy Alignment:** An important part of the Investment Strategy includes the review of multiple strategic documents published by the Army or the JS for the warfighter, commanders, business stewards, IT PMs, and military leadership. Review of current strategy, doctrine and other guidance allows the Investment Strategy team to fully understand the goals and desires of the military leadership. The doctrine clearly states the required capability of the Armed Forces and calls out standards and specifications for IT programs.
- **Capability Assessment:** Conducting a capability assessment is necessary for aligning capability issues with strategic guidance and establishing the rationale for eventual investment solutions. The capabilities address the expected performance, or desired outcome, that current Army programs must fulfill.
- **Investment Solution Design:** Identifying capabilities and capability gaps, requirements from strategic doctrine, and performance measurement results leads to capability-based investment requirements. From the combination of this information, investment solutions are derived to support a portfolio of capabilities.
- **Risk Assessments:** The primary reason for performing a risk assessment is to provide confidence to decision-makers that the final, recommended investment strategy is rigorous and sound, founded upon a complete analytical methodology, and includes information on risks that are not consistently captured in other Army assessments.
- **Interdependency Assessment:** The purpose of this step is to identify all possible interdependencies between the proposed investment solutions of different investment areas. This will ensure that the final, recommended investment strategy makes sound, common sense.
- **Decision Support Tool:** A decision support tool helps the investment strategy working group to optimize their investment choices. The tool provides a cost-benefit analysis to determine the best value investment packages. The tool also recommends the trade-offs that can be made with each chosen set of investments.

### Section III

#### Army Enterprise Management

##### 16–7. Army Enterprise Management

The Army is an extremely large organization, spread throughout the world, accomplishing missions that span a range from warfighting, to civil affairs, to humanitarian efforts. The challenge we face to become a network-centric, knowledge based force requires that we manage the IT infostructure across this vast spectrum of activity. Our networks, systems, and information need to be enterprise based, accessible, seamless, reliable, secure, and deployable wherever we might go. Our efforts to meet this challenge required the realignment of organizations (see Figure 16–2) and the establishment of others to focus our efforts to implement transformation.

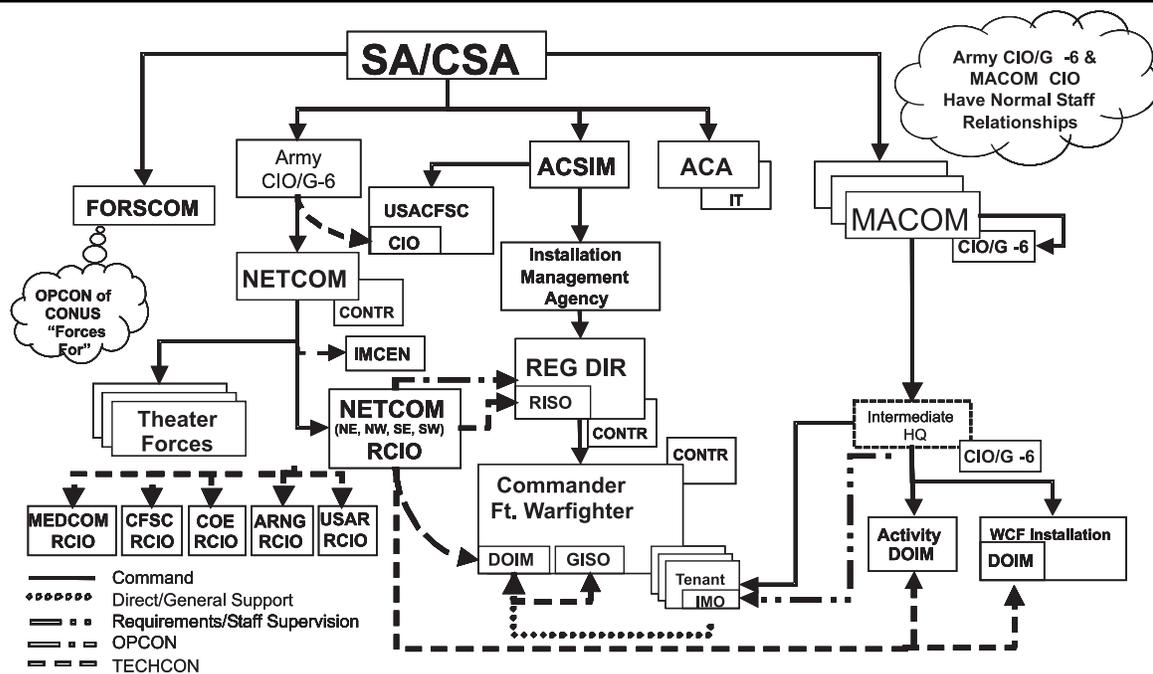


Figure 16-2. Operational relationships

a. U.S. Army Network Enterprise Technology Command (NETCOM).

(1) NETCOM serves as the single authority assigned to operate, manage, sustain, and defend the Army's Infostructure at the Enterprise level. NETCOM delivers Enterprise level C4/IT common user services and signal support warfighting forces to the Army, its ASCC Commanders, and the Combatant Commanders. NETCOM operates, sustains, and defends the Army's portion of the GIG. NETCOM is a direct reporting unit to the Army CIO.

(2) NETCOM has technical control and configuration management authority for the Army's networks and systems and functional processing centers and has operational review and coordination authority for any standard, system, architecture, design, or device that impacts the Army Enterprise Infostructure. NETCOM provides centralized management and technical control for installation Directors of Information Management. NETCOM executes these missions through an Army-wide regional/theater structure that includes Network Operations and Security Centers (NOSCs), regional directors/theater signal commanders (staff position is known as the RCIO, and centralized direction from the NETCOM Army NOSC (ANOSC).

b. *Enterprise Systems Technology Agency (ESTA)*. ESTA, an activity assigned to NETCOM, develops, implements, and enforces Enterprise Systems Management (ESM) processes and activities required to operate and manage Army infostructure at the Enterprise level. As the ESM functional proponent, ETSa develops, staffs, and manages service level agreements for the Enterprise. Additionally, ESTA is responsible for conducting the operational engineering and architectural review of the Enterprise to ensure new systems and enabling technologies or capabilities fielded within the Army infostructure comply with Enterprise-level standards, practices, and procedures.

c. *Regional Chief Information Officers (RCIO)*. In conjunction with the TIM realignment, four CONUS RCIOs are assigned to NETCOM. These CONUS regional units enforce C4/IM policies, standards, architectures, programs, plans, and budgets for all IT issues within their assigned regions. The Directors of NETCOM units are "dual hatted" as the RCIOs to their supported TIM Regional Directors. The CONUS RCIOs and locations follow:

- U.S. Army Network Enterprise Technology Command, Northeast, Fort. Monroe, VA
- U.S. Army Network Enterprise Technology Command, Southeast, Fort McPherson, GA
- U.S. Army Network Enterprise Technology Command, Northwest, Rock Island, IL
- U.S. Army Network Enterprise Technology Command, Southwest, Fort Sam Houston, TX

OCONUS, the RCIO is dual-hatted from the existing NETCOM signal commands. As the Army further implements TIM, the Reserve Components and other Army commands will move into the designated TIM regions. RCIOs for the Army Reserve, Army National Guard (ARNG), Army Medical Command (MEDCOM) and COE have been established and will remain in effect until they can be merged into the NETCOM.

## How the Army Runs

*d. Army Network Operations and Security Center (ANOSC).* The ANOSC, an activity assigned to NETCOM, manages the Army Infostructure at the Enterprise level providing decision makers a comprehensive, integrated, near real-time, situational awareness and operational reporting capability of the Army's portion of the GIG. The ANOSC serves as the single Army-level network operations (NETOPS) authority for coordinating, directing, managing, sustaining, and defending the infostructure. The ANOSC operationally integrates Systems and Telecommunication Network Management, Information Assurance (IA), and Information Dissemination Management (IDM) technologies and procedures through Technical Control (TECHCON) of Army Theater Network Operations and Security Centers (TNOSCs) in support of Army business stewards and the warfighter.

*e. Information Technology, E-Commerce, and Commercial Contracting Center (ITE-C4).* ITE-C4 is assigned to the Army Contracting Agency (ACA), a FOA under the Assistant Secretary of the Army (Acquisition, Logistics & Technology) (ASA) (ALT). ITE-C4 implements the Army's Enterprise-wide buying capability for common use IT and commercial items and provides customer support for satisfying consolidated top line IT requirements.

*f. Army Small Computer Program (ASCP).* The ASCP, an activity reporting to PEO, Enterprise Information Systems, provides a full range of IT, IT infrastructures, and information systems (hardware, software, peripherals, networking and infrastructure support services) to Army, DOD, Foreign Military, soldiers, and Federal agencies consistent with DOD and DA policy on standardization and interoperability.

### 16-8. Army Knowledge Online (AKO).

*a.* A key to Army Transformation and self-synchronizing of our operations is the Army's intranet portal named AKO. We are continuing to transition Army functional business processes behind the AKO. We have centralized our network management and continue to consolidate servers around the Army. AKO, as the Army's single point of entry, is a robust and scalable management system accessible from any Internet connection. The AKO enables people to quickly find and share information using powerful tools to access information in official Army resources, and the ability to contact other soldiers and civilians. The AKO is being used across the spectrum and provides both a NIPRNet and SIPRNet capability.

*b.* The AKO features content-management software, e-mail, instant messaging, chat rooms, knowledge centers, a people locator and white pages with more features to be added in the future. The AKO Knowledge Collaboration Center (KCC) is the Army's shared portable hard drive, which lets users store up to 50 megabytes of data online and, if they choose, share these documents securely through the portal. The KCC organizes files into knowledge centers - Army Communities and Personal and Teams. Most users can only create personal and team knowledge centers, but they can request access to Army Communities. The AKO provides mail anytime, anywhere and that gets the message to the Army community. A single AKO email address can follow the user throughout a military career and into retirement (retirees with 20 or more years of service). Registered users have a career-long email account that can be forwarded from the current location to the future location. This eliminates multiple official email addresses, as you simply change your forwarding email address at the AKO site. The AKO actually serves as an encrypted identity authentication tool that securely delivers personalized content according to the individual's rank, experience, location and duties, regardless of the domain or device the individual is using to gain entry.

*c.* The AKO provides its users a broad range of both business and tactical processes and services, including those in the personnel, logistics, acquisition and e-learning areas. The AKO accounts total well over 1.1 million with an average daily usage of well over 89 thousand hits. The "Self-Service" feature for the military currently features dental readiness, HIV/DNA status, OMPF viewing, alerts to soldiers on College Loan Repay deadlines, TDY pay status, and Promotion Boards. The "Self-Service" feature continues to be one of the fastest growing areas within the AKO.

*d.* The AKO portal is a central part of the overall strategy to transform the Army into a network-centric, knowledge-based force. It will continue to evolve and continue to improve as future capabilities become available to support of technological transformation.

### 16-9. Architecture

*a. Army Knowledge Enterprise Architecture (AKEA).* The CSA has endorsed the Army Knowledge Enterprise Architecture as the blueprint for transforming today's Army into an Objective Force (OF) that integrates Current, Stryker and Future Combat Systems (FCS) forces with Joint, Interagency and Multi-National (JIM) assets, and with the generating forces of the sustaining base including the "Institutional" Army. The AKEA is considerably more complex than the individual Army unit, installation information infostructure, and functional architectures that have been the focus of past Army architecture efforts. The intent of the AKEA is to provide the Army with clear, supportable, and integrated justifications for force development, resource allocation and procurement decisions that cross traditional boundaries.

(1) *Army Knowledge Enterprise (AKE).* Critical to Army transformation is the Army Knowledge Enterprise (AKE) - the combination of infostructure and knowledge. It provides for the integration and the interoperability of processing, storing, and transporting information over a seamless network allowing timely access to universal and secure Army knowledge across the enterprise. The AKEA is the blueprint for the AKE. The AKEA includes the Army's portion of the DOD GIG Architecture that provides the C4/IT blueprint for intra-Army, joint interoperability. The AKEA is also the Army implementation of the IT architecture required by the CCA.

(2) *Non-Information Technology Architecture*. Meanwhile, OF development will use AKEA architecture frameworks to blueprint non-IT areas - a broad range of Army enterprise functionality across DOTMLPF.

(3) *References*. The processes for developing and managing architecture are evolving rapidly. The following paragraphs provide some basic information. Additional information on AKEA can be found on AKO at <https://akea-cio.army.mil>.

*b. Architecture Views*. There are three major perspectives, or views, which logically combine to describe a single architecture. These three architecture views are the operational, systems, and technical views. Because the views provide different perspectives on the same architecture, the most useful architecture description is an integrated description—a description that consists of multiple views.

(1) *Operational View (OV)*. The OV and its associated product set, is a description of the tasks and activities, operational nodes or elements, and information exchange requirements between nodes for each software block or unit in a given architecture. It defines the type of information, the frequency and timeliness of the information exchanges, and the tasks supported by these information exchanges that are needed for warfighting, support, or combat service support functions. An OV can also be described as the total aggregation of missions, functions, tasks, information requirements and business rules.

(2) *Systems View (SV)*. An SV is a physical implementation of the OV. The SV and its products, provides graphical and textual descriptions of the C4ISR systems and interconnections used to satisfy these operational needs. The SV identifies the physical connections and locations of key nodes, circuits, and networks and is constructed per standards defined in the technical view (see below). The SV also shows how major IT systems interoperate and link to JIM IT systems. An SV may also describe the internal construction or operations of a particular system, in which case it is not an enterprise-level systems view.

(3) *Technical View (TV)*. The TV products document the minimal set of rules governing the arrangement, interaction, and interdependence of each system. The TV has been described as the “building code” upon which systems are based. It identifies services, interfaces, standards, and their relationships; and it provides the framework upon which engineering specifications are based, common building blocks are built, and product lines are developed.

*c. Roles and Responsibilities*. The following is an **abbreviated** overview of key AKEA roles and responsibilities. (see Figure 16–3) Further details including a full description of official roles and responsibilities and definitions of terms are at <https://akea-cio.army.mil>.

(1) The CIO/G–6 in coordination with the Director, OF Task Force is the Army Knowledge Enterprise Architect and provides the Army’s overarching architectural policy and guidance, including architecture standards for all AKE architectures. The CIO/G–6 Architecture Division and Army Architecture Integration Cell play central management and production roles, respectively, for development of the AKEA.

(2) The G–3 is the Army Decision Superiority Integrator with approval authority for AKEA and OVs to ensure they support Army requirements and capabilities.

(3) The G–2 is the overall integrator of Army Intelligence Transformation, which will be conducted within the context of the overall architecture development process.

(4) The G–8 will review architecture integration decisions to ensure they support future Army programming and materiel integration.

(5) TRADOC is the Army Operational Architect.

(6) The Assistant Secretary of the Army for Acquisition, Logistics, and Technology (ASA(ALT)) is the Army Systems Architect, and is supported by the PEOs and PMs who develop the systems views.

(7) The CIO/G–6 is the Army Technical Architect. The U.S. Army Communications and Electronics Command (CECOM) provides technical support to the CIO/G6 on all Joint Technical Architecture - Army (JTA–A) matters. The JTA–A is the Army implementation of the DOD JTA.

(8) Elements of HQDA (Secretariat/ARSTAF) are knowledge stakeholders for Functional Domains specifically identified in *General Order No. 3, Assignment of Functions and Responsibilities Within Headquarters, Department of the Army*, 9 July 2002 <http://www.usapa.army.mil/>.

(9) The AKEA has five infostructure components that are distinct C4/IT capabilities and related processes required to provide services across the AKE.

(a) Component: Enterprise Applications - Software applications needed to manage the Army as a knowledge-based net-centric enterprise. Lead: CECOM

(b) Component: Computing - Use of computer technology to manipulate data, information, and/or knowledge into the desired form to support decision-making and other functions such as collection, creation, and acquisition of information. Lead: ASA(ALT)

(c) Component: Communications - End-to-end movement of data, information, and/or knowledge between users and producers through other intermediate Global Information Grid entities. Lead: CECOM

(d) Information Management: - The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. Lead: CIO/G–6

(e) Network Operations - The NETOPS concept is an organizational, procedural, and technological construct for ensuring information superiority and enabling speed of command for the warfighter. Lead: NETCOM

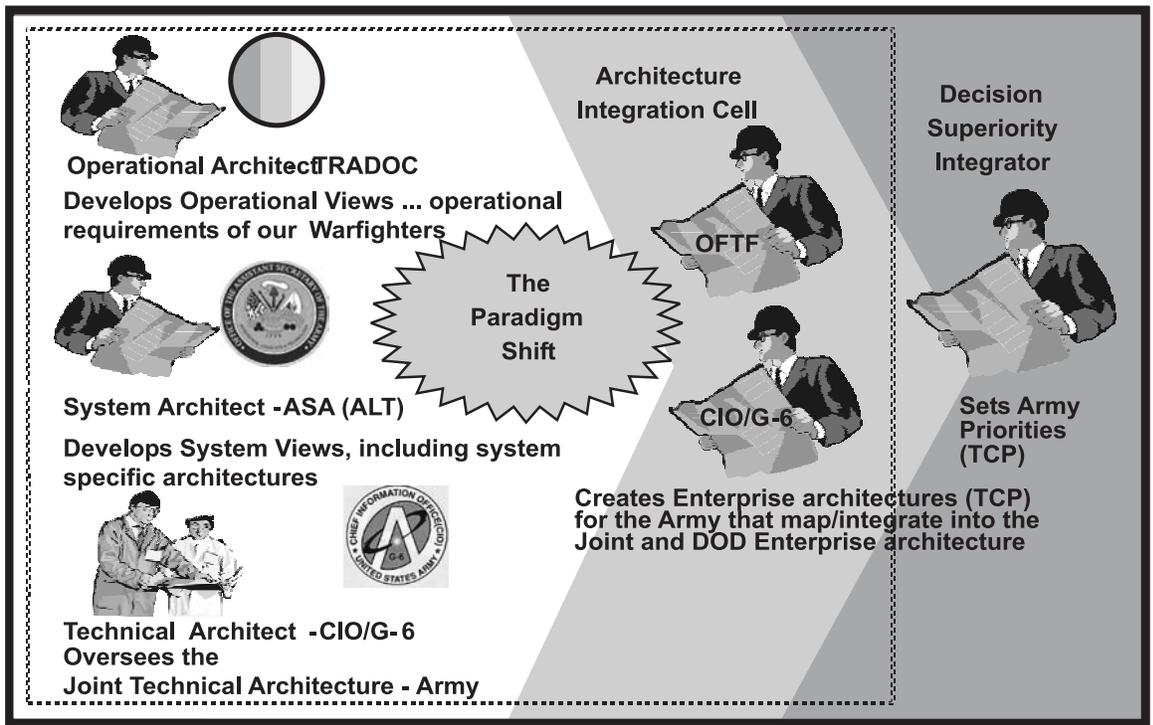


Figure 16-3. AKEA roles and responsibilities

**Section IV  
Other areas**

**16-10. The Army CIO/G-6 Organization**

The Army CIO has the principal responsibility for the Army’s IM functions pursuant to 10 USC Sec 3014(c)(1)(D), and is responsible for setting the strategic direction, determining objectives, and supervising the DA’s C4/IT functions. In this capacity the CIO provides strategic leadership, stewardship, and transformation of the Army’s C4/IT infrastructure, delivery capabilities, and assets. (see Figure 16-4)

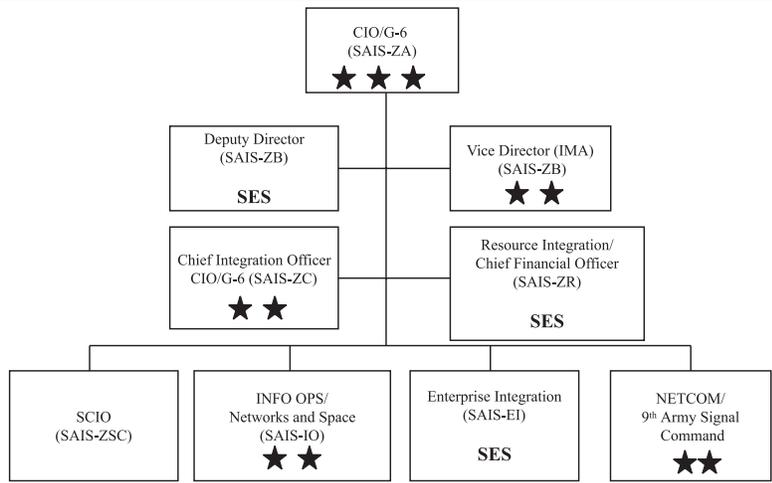


Figure 16-4. CIO/G-6 Organization

**16–11. Resource Integration (RI)**

The CIO/G–6 is responsible for oversight of all C4/IT resources and assessment, and develops and coordinates investment decisions at the Enterprise level for all C4/IT expenditures. Decision-making at the Enterprise level transforms the workforce, processes and infostructure by providing accountability, standardization and efficiencies to support AKM. Strategic resourcing decisions are made through the C4/IT Investment Strategy process in coordination with NETCOM, MACOMs, COCOMs, and ARSTAF stakeholders. MACOM investment initiatives are reviewed and evaluated by the CIO/G–6 and the ARSTAF, Resource Review Working Group, before being forwarded to the Army CIO EB for approval. All allocations of C4/IT resources undergo this review process for approval. Approved resource allocation decisions are supported in the planning, programming, budgeting and execution system (PPBES) to ensure that C4/IT resources are allocated in accordance with the priorities in the C4/IT Investment Strategy.

**16–12. Information Infostructure**

The CIO/G–6 provides functional management and oversight over the Army’s Enterprise information infostructure. These functions include developing and articulating policy, functional requirements for the Enterprise, practices, business processes, technologies, hardware, software, systems, networks, personnel, and resources that support the Army’s information infrastructure.

**16–13. C4 Systems and Networks**

The CIO/G–6 provides functional management and oversight over the Transformation of the Army’s tactical information infrastructure and strategic “reachback” enablers. In this area, the CIO/G–6 oversees, coordinates, and monitors C4/IT systems and programs throughout their life cycle; formulates acquisition policy and strategies; provides advocacy for base level systems and programs; and manages functional programs such as space and networks, C2 systems, combat service support systems, C2 Protect, and Visual Information.

**16–14. Information Assurance (IA).**

IA, a direct reporting unit of ESTA, is responsible for developing and overseeing the Army’s ISSP, which is the overarching program for securing the Army’s portion of the Defense Information Infrastructure. The Army CIO/G–6 is responsible for implementing protective measures, developing plans, policies and procedures, developing and monitoring training, and validating requirements to protect SECRET and below command, control, communications, and computer capabilities. IA develops and directs the implementation of the ISSP for product procurement, the Network Security Improvement Program (NSIP) Plan for the Army sustaining base, and the Army Protection Plan for the tactical force. Additionally, IA is responsible for developing requirements for a robust biometrics program designed to improve positive access control to facilities, workstations, systems, and networks.

**16–15. Biometrics.**

SecArmy is the Executive Agent for Biometrics Programs in DOD and is responsible for developing and implementing a biometrics Enterprise solution set that is scalable across DOD to combat identity theft, assure positive access control, and provide verification and authentication for authorized users. This program is designed to help eliminate total reliance on passwords, personal identification numbers (PINs), and tokens as a primary means of safeguarding against illegal or forced access to facilities, workstations, systems, and networks.

**16–16. Human Capital (HC)**

*a.* The CIO/G–6 supports the development of a knowledge-based workforce by leveraging intellectual assets and empowering the Army’s human resources through effective workforce planning, cutting-edge recruitment and retention initiatives, broad-based education and training, and cross-functional professional development opportunities.

*b.* A knowledge-based organization demands new organizational definitions, disciplines and structures to respond effectively to new challenges and new opportunities. Leaders must communicate their vision and expectations across the Army, and articulate clearly how we will move from our current to our “to be” state. This wholesale Transformation must embrace the principles of effective change management, and focus on building a framework for knowledge management that has a strong human capital infrastructure in which knowledge is shared across the Army enterprise.

*c.* A key to the success of a knowledge-based organization is the continuous learning and the transformation of the Army’s most valued asset - its human capital. Accordingly, education, training, mentoring, and professional development opportunities will provide soldiers and DA civilians with a global perspective, enable them to embrace and lead change, and make them adaptable to new environments and new ways of doing business. The Army should work to attract global thinkers from many disciplines, and should implement recruitment and retention strategies that include monetary incentives, workplace flexibilities, and education opportunities.

### 16–17. Policy and Governance

The CIO/G–6 manages and oversees the Army Enterprise integration of policies and functions to comply with public laws and OMB, DOD, and Army guidance and serves as the focal point for assigned AKM functions. The CIO/G–6 is also the focal point for the management and integration of Federal, DOD and Army CIO EBs. AKM Goal 1, “Adopt governance and cultural changes to become a knowledge-based organization,” is achieved through the institutionalization of policies, management structures, and leadership initiatives to support knowledge management and infostructure at the enterprise level.

### 16–18. Strategic Outreach

*a. e-GOV.* e-Government, one of five Presidents’ Management Agenda items established in 2001 ([http://www.whitehouse.gov/omb/budintegration/pma\\_index.html](http://www.whitehouse.gov/omb/budintegration/pma_index.html)), focuses on creating improved ways for the citizen to get information and services from the federal government and emphasizes the interoperability necessary to support seamless interagency operations. The e-GOV program draws on commercial e-business principles and is heavily IT-enabled ([http://www.cio.gov/best\\_practices](http://www.cio.gov/best_practices)). The E–Government Act of 2002 (P.L. 107–347) signed on 17 December 2002, created an Office of Electronic Government within the OMB (<http://cio.gov/>). The OMB e-GOV office reviews the annual OMB Form 300 reports to assess progress towards e-GOV interoperability. The Army is involved in development of several of the e-GOV initiatives, such as Disaster Assistance and Crisis Response and Recreation One Stop. The Army CIO/G–6 is the Army Point of Contact for overall e-GOV issues.

*b. Government Paperwork Elimination Act (GPEA).* Enacted in 1998, the GPEA (P.L. 105–277) (<http://www.whitehouse.gov/omb/memoranda/m00–10.html>) focuses on using IT to improve customer service and government efficiency by reducing paperwork and moving the government to a paperless environment. By 21 October 2003, Federal agencies are required to provide for, when practical, an option of electronically maintaining, submitting and disclosing information, as well as using and accepting electronic signatures. The implementation of the GPEA primarily focuses on automating forms and records and transforming the processes that support that information. Annually, the Army along with all other Federal agencies, report to the OMB on progress made in reducing paperwork in compliance with GPEA (<http://www.whitehouse.gov/omb/inforeg/infopoltech.html#gpea>). e-Army transformation incorporates GPEA into its strategy. While GPEA execution applies to all Army organizations, the CIO/G–6 is the ARSTAF proponent for coordinating GPEA compliance.

*c. e-Army transformation.* e-Business has become the hallmark of successful commercial organizations to streamline their operations and improve customer service, internal efficiencies and supplier relationships by using IT to enable their processes. The Army has adopted these commercial best practices under a strategy called e-Army, part of Goal 2 of the overarching AKM strategy. e-Army is an approach that emphasizes IT-enabled end-to-end process transformation by focusing on self-service web-based applications, the creation of Army-wide Enterprise processes and multi-functional processes, digital signature, workflow and content management to support a ‘paperless’ operating environment, and designing processes to operate in a ‘one network, one database’ construct within the Army’s Enterprise portal, AKO. e-Army focuses on improving access to the ‘business intelligence’ that exists within our systems and improves the relationships between an Army organization and its customers, its internal operations, and its information and product suppliers. Major e-Army initiatives include the implementation and integration of multiple Enterprise Resource Planning (ERP) systems, the digitization and transformation of the forms, records, and publications processes, and the deployment of automated management support tools such as the Army Workload and Performance System (AWPS). e-Army is the Army’s program to capitalize on e-business success and stimulate process transformation and is consistent with the DOD e-Business strategy and federal e-GOV guidance. The CIO/G–6 is the Army member of the DOD e-Business Board of Directors.

*d. Business Initiative Council (BIC).* The DOD BIC, established in 2001, chaired by the Under Secretary of Defense for Acquisition, Technology and Logistics with membership of the Military Department (MILDEP) Secretaries, was instituted to provide a forum to generate improved business processes applicable to the DOD Enterprise. The CIO/G–6 is the Army representative on the IT Process Functional Board (IT PFB) of the DOD BIC and coordinates staffing and execution of the IT-enabled initiatives brought to the BIC for decision/implementation. The Army BIC (ABIC), chaired by the SecArmy and run by the Army G–8, is a similar forum to generate improved business processes applicable to the Army Enterprise. The CIO/G–6 is on the Executive Steering Committee for the ABIC and chairs the IT PFB, one of six process/functional boards supporting BIC activities. The IT PFB coordinates proposals and implementation plans for IT-enabled business process change initiatives in the Army.

*e. Army Knowledge Symposium.* The CIO/G–6 sponsors an annual symposium to bring together leading practitioners of industry, government, defense and Army knowledge-based organizations to provide a development forum to stimulate The Army’s Transformation to a knowledge-based force.

### 16–19. Strategic Partnering

Strategic Partnering supports integration of AKM into the military and business functions of the Army, and advances transformation of AKO into the killer application for land-power dominance by integrating it fully into military and business operations. This effort, a form of customer relationship management, requires Strategic Partnering to determine the current needs of functionals and anticipation of their future requirements. To accomplish this, Strategic

Partnering educates functionals on the ARSTAF, and within the support and combat forces on knowledge management and what AKO can accomplish. It maps the following: mission needs and operational requirements; existing and proposed knowledge bases and expertise networks to meet those needs; and the state of webification — the prerequisite for making these knowledge assets available through AKO. Strategic Partnering implementation embeds Functional Exchange Officers (FEO) in key functional areas to work requirements and solutions from the inside out, and thereby integrates their functions into AKO, and into the “vibrant knowledge network” for the Objective, Interim and Legacy Forces.

## **Section V**

### **Objective force**

#### **16–20. Transformation changes**

The Army’s transformation changes the force from a discipline-specific, stovepiped, platform-centric organization designed for the linear fight to a network-centric, knowledge-enabled force optimized for full-spectrum operations. The Objective Force is fully integrated vertically and horizontally with joint and coalition forces, and with interagency teams. This will allow unfettered movement of large and, most importantly, relevant volumes of data, information, and knowledge between the commander’s critical decision nodes. The clear purpose of the knowledge support schema is to enable commanders to achieve dominant battlespace understanding as a precondition for rapid, decisive action.

#### **16–21. Cultral changes**

The Army’s transformation is taking us down a road of cultural changes that will revolutionize the way we acquire and employ our IT assets. These changes will forever alter how we conduct daily business and operations. To remain relevant to Army transformation and the objective force, the Army must adapt and immerse itself in this new culture as future military operations will be conducted in a fundamentally different and dynamically changing operational environment (OE). This OE is characterized by the responsiveness, agility, and full spectrum capability to dominate unstable situations. These culture changes are manifested in the Army CIO’s AKM initiative. AKM is the Army strategy to transform itself into a network-centric, knowledge-based force. This will enhance decision dominance both on the battlefield and in day-to-day operations. This requires the Army to change its cultural thinking from the “islands of automation” mentality to the enterprise management of IT resources. This means that organizational IT investments must support the Army’s enterprise-wide goals under AKM.

#### **16–22. Goal of AKM**

A goal of AKM is the establishment of both secure (AKO–S) and non-secure (AKO–N) AKO portals. The Army’s soldiers and civilians are the driving force behind the AKO vision to transform the Army into an information age, network centric organization that leverages intellectual capital to better organize, train, equip and maintain a strategic land combat force. With the help of AKM, our Army will be a full spectrum force; organized, manned, equipped, and trained to be more strategically responsive, agile, deployable, versatile, lethal, survivable, and sustainable across the entire range of military operations to swiftly and decisively defeat our adversaries.

## **Section VI**

### **Summary and references**

#### **16–23. Summary**

*a.* Army transformation is all about transitioning from information-based to knowledge-based warfare to conduct effects-based operations. Systems overmatch based on inches of homogeneous steel and platform-centricity is giving way to network-centric, knowledge-based warfare and the ability to achieve decision superiority and take decisive action across the operational spectrum. The goal of the CIO/G–6 is to provide the tools such as AKM to enable better and faster decisions than the opponent.

*b.* AKM provides for the integration and the interoperability of processing, storing, and transporting information over a seamless network, allowing access to universal and secure Army knowledge across the enterprise. In an effort to align with the AKM Strategy, current operational systems are examined relative to the results they achieve and benefits they provide to the Army’s infostructure. If they do not contribute to a world-class network-centric knowledge system, they will be eliminated or migrated to systems that do.

*c.* The CIO/G–6 is committed to meeting the challenges that transform the Army into a force that is strategically responsive and dominant at every point of the spectrum of operations. As such the CIO/G–6 is investing in today’s technology to stimulate the development of doctrine, organizational design, and leader training to improve the objective force. Doing so will extend the Army’s technological overmatch.

#### **16–24. References**

- a.* Army Regulation 25–1, *Army Information Management*, [http://www.usapa.army.mil/profiles/r25\\_1.pdf](http://www.usapa.army.mil/profiles/r25_1.pdf).
- b.* Army Regulation 70–1, *Army Acquisition Policy*.

## How the Army Runs

- c. Army Regulation 71–9, *Materiel Requirements*.
- d. Army Regulation 380–19, *Information Systems Security*.
- e. General Order 3, *Assignment of Functions and Responsibilities Within the Headquarters, Department of the Army*, <http://www.army.mil/usapa/epubs/pdf/go0203.pdf>
- f. General Order 5, *Establishment of the U.S. Army Network Enterprise Technology CMD/9<sup>th</sup> Army Signal CMD; Transfer and Redesignation of the HQ and HQ Company, 9<sup>th</sup> Army Signal CMD; Discontinuance of the Communications Electronics Services Office and the Information Management Support Agency*, <http://www.army.mil/usapa/epubs/pdf/go0205.pdf>
- g. White Paper, *The Objective Force in 2015* (Final Draft), 8 December 2002.
- h. HQDA Information Management Execution Plan, Phase I, 1 July 2002.
- i. Army Knowledge Management Guidance Memorandum Number 1, 8 August 2001.
- j. Army Knowledge Management Guidance Memorandum Number 2, 19 June 2002.
- k. CSA Transformation Review, 2 January 2003.