

CHAPTER 16

ARMY INFORMATION MANAGEMENT

Our vast, unapplied deposits of corporate knowledge and information have little power when they're tucked away in reports, file drawers, and databases. Organizations today do not lack information. They lack the tools to get the right information to the right people at the right time.

Information Ecology: Mastering the Information and Knowledge Environment, Thomas H. Davenport and Laurence Prusak, Oxford University Press, 1997

SECTION I INTRODUCTION

16-1. General background

a. Financial. According to Thomas H. Davenport, noted knowledge expert and consultant, in the United States more than fifty percent of all capital spending goes to information technology (IT). Over the past decade, IT spending in the U.S. alone, has been estimated to be over three trillion dollars.

b. Importance. IT is now considered a strategic resource and its management has been elevated to the top reporting level in most organizations. The National Defense University, located at Fort McNair, Washington, D.C. has added an Information Resources Management College to support the Department of Defense and other Federal agencies.

c. Enabler. IT supports and increases value to strategic planning, organization core competencies, and is a critical enabler in organizational transformations. IT is a powerful technology that is changing how things are done in the world and how we will work in the future. Time and distance are no longer considered to be barriers or constraints to organizations, which must now consider themselves global participants.

d. Information Age transformation. The Industrial Age is transforming into the Information Age. IT is accelerating this change by replacing the paradigm of wealth and powered based on physical things to one based on knowledge and information. New metrics for controlling and measuring organization effectiveness are required and are beginning to emerge. Organizations that are transforming themselves are taking new names such as, knowledge-based, learning, or sense and respond.

16-2. The Army in the Information Age

The Army's vision for information technology is to support and enable the United States Army as the preeminent land power in the world. The command, control, communications, computers and intelligence/information technology (C4I/IT) investment strategy stems from this vision as it embodies the basic tenets of *Joint Vision 2020* and *The Army Vision*. The vision serves as a vector for the Army's C4I/IT investment strategy for the future. Information dominance is the key to successful operations on the 21st Century battlefield. Information dominance is the

organizing principal for *Joint Vision 2020* and *The Army Vision*, with IT as the critical enabler to achieve the Army's Transformation Strategy.

16-3. Army Transformation Strategy

C4/IT programs are key to the core of the *Army Vision* and the Army Transformation Strategy. The *Army Vision* and Transformation Strategy stress the importance of IT for both achieving a decisive edge in operational warfighting capabilities, as well as the means to support those capabilities through the concomitant business economies and efficiencies that these technologies provide. The Army's Transformation Campaign Plan strongly relies upon the integrated command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) capabilities for joint situational awareness and the global velocity and agility of the projected force required by 21st century warfighting doctrine. Power projection and reach-back connectivity for split-base operations and support requires a secure, robust information infrastructure. This infrastructure is the central platform for the strategic communications also required by ready and rapidly deployable active Army forces in accordance with the operational concepts of *The Army Vision* and *Joint Vision 2020*.

SECTION II

CHIEF INFORMATION OFFICER (CIO)

16-4. CIO authority

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)*, directs that each executive agency appoint a chief information officer (CIO) who reports directly to the head of the agency. The Secretary of the Army designated the Director of Information Systems for Command, Control, Communications, and Computers (DISC4) and the Vice DISC4 as the CIO and Deputy CIO respectively.

b. Clinger-Cohen Act (CCA) objectives. The CCA increased the Secretary of the Army's responsibility, authority, and accountability for the use of IT and other information resources in performing Army missions. The National Security Systems provisions of the Act 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; cryptologic activities related to national security; command and control of military forces; or, equipment that is an integral part of a weapon or weapons system. The Act emphasizes 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.

c. CCA on the World Wide Web. The entire text of the CCA can be viewed at http://www.itpolicy.gsa.gov/mks/regs-leg/s1124_en.htm.

16-5. CIO responsibilities and duties contained in the CCA

The Army CIO's responsibilities and duties are taken from the CCA and presented below (section references are to the Act):

a. Responsibilities.

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

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

b. Duties.

(1) *IT acquisition oversight*. Sec. 5125(c)(2): "...monitor the performance of information technology 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;"

(2) *Business process analysis/improvement*. 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 information technology to be used in support of those missions..."

(3) *Capital IT investment control*. Sec. 5125(c)(2): "...monitor the performance of information technology 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."

(4) *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.

SECTION III ARMY ENTERPRISE

16-6. Definition

The Army Enterprise (AE) is defined as the entire Army—major commands, headquarters, agencies, installations, and Army forces—and the activities that those organizations perform, including relationships with external organizations and activities, that is the Army and government and on-government organizations and activities. The AE represents the Army as a corporate entity and prescribes a new way of accomplishing the Army’s missions by taking full advantage of IT, using innovative business practices, and synchronizing Army IT resource management activities toward common goals.

16-7. Army Enterprise Strategy (AES)

a. Definition. The AES is the single, unified vision for the Army command, control, communications, computers, and intelligence (C4I) community and is presented in the Army Enterprise Vision document.

b. AES goals. The AES focuses on the information needs of the Army. It emphasizes a seamless information environment to support the Army warfighter into the 21st Century. This strategy supports the objectives of *Joint Vision 2020* and *The Army Vision*. It defines what the Army must do to “win the battlefield information war,” including the Horizontal Technology Integration (HTI) initiative and the digitization of the Army in support of the Army transformation Campaign.

c. AES scope. The scope of the AES is to encompass all embedded and stand alone C4I systems for sustaining base (Power Projection Platforms), Theater/Tactical, and Strategic environments. The AES provides a holistic view of the information systems and interconnections required to enable a Force Projection Army to attain the *Joint Vision 2020* Information Dominance objective. AES also addresses the requirement to organize, train, and equip the force and to operate and sustain the force as a component of any Joint and Combined force from home base to the foxhole.

16-8. Components of the AES

The Army Enterprise Strategy consists of two documents, the AES Vision and the Enterprise Implementation Plan (EIP).

a. The AES Vision. The AES Vision describes the principles necessary to ensure warfighter information technology superiority over any opponent. These principles are—

- Focus on the warfighter.
- Ensure joint interoperability.
- Capitalize on space-based assets.
- Digitize the battlefield.
- Modernize power projections platforms.
- Optimize the information technology environment.
- Implement multilevel security.
- Acquire integrated systems using commercial technology.
- Focus on information security.
- Exploit modeling and simulation.

b. Enterprise Implementation Plan (EIP). The EIP shapes the Army's C4I/IT Investment Strategy as described by the Army Enterprise (C4I/IT) Architecture. The Enterprise General Officer Steering Committee (EGOSC) monitors the development of this architecture using a common set of evaluation criteria to analyze, assess, and prioritize future information system capabilities, which the warfighter needs.

16-9. Major participants in the process

The Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA(ALT)), the Assistant Secretary of the Army, Financial Management and Comptroller (ASA(FM&C)), the DISC4, the Deputy Chief of Staff for Operations and Plans (DCSOPS), and the Deputy Chief of Staff for Intelligence (DCSINT) co-sponsor the Enterprise Strategy. Training and Doctrine Command (TRADOC) is also a major player, as are other functional proponents.

SECTION IV CIO INVESTMENT STRATEGY

16-10. General background

The investment strategy provides a focused approach and enables the Army to evolve into a network-centric force in 2010 and finally into the knowledge-centric force of 2025 through the Army Transformation Strategy. This evolution will provide soldiers with the ability to capitalize on knowledge obtained from unlimited access to a global, seamless, secure enterprise network to achieve information dominance. Central to these concepts is the creation of a global secure network. This network will allow soldiers to access the knowledge capital offered by the network, thus enabling the realization of a knowledge-centric force.

16-11. Army CIO strategy and implementation

Executive Order (EO) 13011 mandates that Federal executive agencies promote the effective design and operation of all major IRM processes with oversight by a CIO. CIO management focuses on those policies, processes, and organizational responsibilities necessary to accomplish the mission-defined primary in governing legislation and other guidance. Such responsibilities include strategic planning, business process analysis and improvement, assessment of proposed systems, resource management (to include investment strategy), performance measurements, IT acquisition, and training.

a. Participants. HQDA, MACOMs, installations, and other Army activities are required to participate in executing the IRM management process and assisting the CIO.

b. The Army Plan. The Army C4I/IT Investment Strategy conveys the CIO's investment framework and is based upon the Army's strategic plan, that is, The Army Plan (TAP). TAP provides a focused and consistent azimuth for the development of the Army's Program Objective Memorandum (POM) to meet the strategic planning objectives of the Army Transformation Strategy. TAP also provides the strategic framework for sound C4I/IT programming decisions by providing the Army strategic direction, required operational capabilities, and the programmatic guidance, which ultimately produces the Army's investment program and budget.

c. Processes. TAP mission areas are supported by operational tasks, capabilities, and performance standards linked to six program evaluation groups (PEG). The PEGs represent funding for the six Title X functional areas, resource goals, objectives, and tasks. This linkage ensures that the CIO's C4I/IT investment strategy supports the Army's core competency and core warfighting and business processes required for the Army Transformation Campaign. The

CIO's investment strategy focuses on investment capability areas critical to attaining information dominance. Focusing on capabilities rather than individual systems or programs is the key underpinning of the C4I/IT investment strategy. Capabilities needed to accomplish the Army's mission are highlighted and aligned with C4I/IT investments required to achieve the Army's transformation objectives. The C4I/IT capabilities that Army warfighters and decision-makers depend upon must be interoperable and effective to ensure information dominance across the operational continuum. Basing the C4I/IT investment strategy on required mission capabilities strengthens the linkage between programs and successful mission performance outcomes.

d. Value. The CIO investment strategy framework adds value to Army C4I/IT investments in two respects:

(1) Planners and programmers work collaboratively to determine optimal, affordable C4I/IT investments that will deliver a capabilities-based return on investment in support of the A TAP.

(2) The investment strategy is based upon a crosscutting analysis of the value that C4I/IT investments can leverage - or balance - across the mission areas of TAP.

e. Continuous transformation. The CIO investment strategy continues to undergo process improvement through subsequent iterations and the involvement of C4I/IT stakeholders. This strategy helps ensure that 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.

SECTION V ARCHITECTURE

16-12. Army Enterprise Architecture (AEA)

The Army Enterprise Architecture fulfills the CCA requirement to develop enterprise-wide IT architecture. The AEA is an Army-wide IT architecture that describes the relationships among key Army institutional processes and IT to ensure the alignment of information systems acquisition and related processes with validated warfighting operational and support requirements. It also ensures adequate Army, joint, and combined interoperability; redundancy and security of information systems; and the application and maintenance of a set of standards by which the Army evaluates and acquires new systems. (The DISC 4 Architecture Directorate Home Page is at <http://arch-odisc4.army.mil>.)

16-13. Tool and products

a. Tool. The AEA is both a tool and a set of products. The AEA is a tool to describe the Army's IT requirements and capabilities. As a tool the AEA directs the development, management, and use of architecture and supporting architecture products through such means as the AEA Guidance Document (AEAGD). In addition, the AEA includes a recapitulation of applicable architecture policy and a set of architecture development and management tools.

b. Products. As a set of products, the AEA is the validated description of the Army's IT requirements, existing capabilities, projected needs, and prescribed IT standards based on a consistent methodology.

c. Evolution. It is important to note that the AEA is not an entity unto itself. It derives from the AES and the Army EIP, which were agreed to at the highest levels in the Army in 1993 and 1994. These efforts gained additional impetus from *Joint Vision 2020* and *The Army Vision* and

from the CCA of 1996. The AEA continues to evolve in concert with The Army Plan and Army Strategic Planning Guidance.

16-14. Army Operational Architecture (AOA)

The AOA is the operational elements, assigned tasks, and information flows required to accomplish or support a warfighter function. It defines the type of information, the frequency and timeliness of the information exchange, and the tasks supported by these information exchanges. An operational architecture can also be described as the total aggregation of missions, functions, tasks, information requirements, and business rules. TRADOC, as the Army's Operational Architect, develops and maintains the AOA. The AOA products are reviewed and integrated into the Joint Operational Architecture. DCSOPS, as the DA staff proponent for the AOA, will be supported by the Army CIO throughout the AOA process.

16-15. Army Systems Architecture (ASA)

The ASA is a high-level systems architecture that describes the IT systems that support the principal activities of the Army. The ASA identifies the physical connections and locations of key nodes, circuits, and networks. It is constructed to satisfy AOA requirements per standards defined in the Army Technical Architecture (ATA). The ASA shows how the Army's major IT systems inter-operate and link to joint IT systems. The ASA may also describe the internal construction or operations of particular systems in the ASA. A systems architecture is a physical implementation of the operational architecture, the layout and relationship of systems and communications. The Army CIO develops and maintains the ASA.

16-16. Joint Technical Architecture—Army

a. What it is. The JTA-A is minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements of a system that ensures that a compliant system satisfies a specific set of requirements. It identifies services, interfaces, standards, and their relationships. It provides the framework, thus guiding the implementation of systems, upon which engineering specifications are based, common building blocks are built, and product lines are developed. These technical rules, or the building code, are based on Operational Architecture requirements and will constrain Systems Architecture development. A technical architecture has been described as the "building codes" upon which systems are based.

b. Responsibility. The CIO maintains the JTA-A. The JTA-A serves as the Army's implementation of the DOD Joint Technical Architecture (JTA).

SECTION VI PROCESS ANALYSIS AND REVISION

16-17. Responsibilities

a. CCA. The CIO is the functional proponent for business process reengineering/improvement with a C4I/IT impact. The CCA mandates that the CIO will be responsible for "promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency." It also directs that the head of the executive agency 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 information technology. Also see AR 25-1, *Army Information Management*.

b. CIO. The CIO proponent will ensure that a process is analyzed and revised, as appropriate, before making significant C4I/IT investments in support of those processes. Additionally, process analysis and appropriate revision will be accomplished as mission needs change and periodically for mission and performance effectiveness.

c. Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4). The ODISC4 provides a value added to HQDA functional proponents, MACOM commanders, and others by means of a clearinghouse on the CIO Website of the DISC4 homepage at www.army.mil/disc4.htm.

16-18. Documentation

a. Process analysis documentation. Process analysis for warfighter and warfighter-related processes will be documented in the mission needs statement (MNS) and operational requirements document (ORD) using the doctrine, training, leader development, organizational design, material, and soldiers (DTLOMS) requirements methodology in AR 71-9, *Material Requirements* and TRADOC Pamphlet 71-9. Process analysis and revision will be accomplished before submitting a MNS or ORD.

b. Army Process Improvement Database System. Process analyses, improvements, and reengineering of mission-related and administrative work processes are documented in the Army Process Improvement Database System at <https://armypi.us.army.mil/armypi>. Army organizations, through a designated point of contact who is authorized to input to the database, provide information and data on improvement initiatives for the database. Army organizations can search the database for similar processes to eliminate redundancy of process analyses.

SECTION VII PERFORMANCE MEASUREMENT

16-19. Objectives

Measuring IT performance assesses IT effectiveness and efficiency on an organization's missions, goals, and quantitative objectives. The impact is measured using quantifiable, outcome-based criteria that are compared against an established baseline.

16-20. Measurement types

IT performance measurements consist of the following:

a. Effectiveness. Measures of effectiveness demonstrating that an organization is executing its mission. These focus on outcomes, for example, achievement of missions and goals, quality of work, and/or customer satisfaction.

b. Efficiency. Measures of efficiency demonstrate that an organization is executing its mission optimally. These include outputs, e.g., quantity of work and timeliness of delivery.

c. Performance. Performance measures are developed for each IT investment which supports organizational missions before execution or fielding of that investment. The performance measures:

(1) Gauge the value-added contribution of the IT investment to missions, goals, and objectives;

(2) Include only the critical few measures that provide a clear basis for assessing accomplishment, aiding decision-making, and assigning accountability at each management level.

d. Cost-benefit analysis. A cost-benefit analysis must be applied against any proposed performance measurement system. If the cost of collecting and analyzing the required data exceeds benefit to the organization, a measure will not be used unless directed by higher authority. Performance measures in support of warfighting materiel requirements with a C4I/IT impact will be included in the appropriate requirement document per AR 71-9, *Material Requirements*.

SECTION VIII

CHIEF INFORMATION OFFICER (CIO) ACTIVITIES

16-21. Digitization of the battlefield

a. Background. The Army of the next century will be required to operate across a broad operational spectrum including space, cyberspace, and ever-larger segments of the electromagnetic spectrum. On the other hand, the information age and the absence of a peer competitor provide the United States the opportunity to pursue transformation to achieve radically new and more effective capabilities. Thus, we must transform to maintain overmatch over potential enemies and threats, operate in new environments, and capitalize upon opportunities to achieve unprecedented leaps in capabilities.

b. Digitization. Digitization is the means by which we will achieve information dominance to enable mental agility, and is the number one modernization priority for the near- and mid-term. Digitization involves the use of modern communications capabilities and computers to enable commanders, planners, and executors to rapidly acquire, share, and use information. The digitization effort includes the fielding of the Army Battle Command System (ABCS), the central framework for networking the battlespace, to execute operations faster and more decisively than the enemy. The cornerstone of this effort is the equipping of the first digitized division (FDD) by 2000 and the first digitized corps (FDC) by 2004.

16-22. Digitizing the sustaining base

The primary initiative for digitizing the Army installation is the Installation Information Infrastructure Modernization Program (I3MP). I3MP modernizes the digital infrastructure of Army installations to enable us to import best commercial practices and labor saving technology. This is a “key enabler” for implementing the Revolution in Military Logistics, Business Process Reengineering, and supporting the Defense Reform Initiatives. This infrastructure is also critical to supporting deployed warfighters with reach back capabilities. I3MP has four components: (1) Outside Cable Rehabilitation which replaces totally inadequate copper wiring with a high capacity fiber backbone, (2) Common User Installation Transport Network (CUITN) provides servers and cables to connect the backbone to buildings and distribution nodes for high-speed data transfer on installations, (3) the Defense Information System Network (DISN) Router Program that provides gateways to the DISN (off-post connections) and network management capabilities, and (4) the MACOM Telephone Modernization Program that provides modern digital telephone switches and linkages to Army users.

16-23. Information assurance

The Information Assurance Directorate is responsible for developing and overseeing the Army's Information Systems Security Program (ISSP), which is the overarching program for securing

the Army's portion of the Defense Information Infrastructure. The DISC4, as the Army's Chief Information Officer, 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. The Information Assurance Directorate 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, the Directorate is responsible for developing a robust biometrics program designed to help eliminate passwords as the primary means of safeguarding against illegal or forced access to workstations, systems, and networks.

16-24. Army acquisition and CIO assessment

a. Need requirement. The process for acquiring systems or capabilities begins when an organization's C4I/IT needs are established (per AR 71-9, Material Requirements) through the appropriate requirement document.

b. Acquisition. Acquisition involves the description of requirements to satisfy the needs, how business process analysis was accomplished, outcome and output-oriented performance measurements, 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 the needs by contract.

c. CIO responsibilities.

(1) The Army CIO ensures that IT systems are acquired and information resources are managed within an integrated acquisition strategy and framework. The Army CIO provides oversight for C4I/IT systems during the acquisition approval process (AR 25-1, *Army Information Management* and AR 70-1, *Army Acquisition Policy*).

(2) Per the CCA, the Army CIO recommends to the Secretary of the Army whether to continue, modify or terminate Army programs with a C4I/IT impact. CIO assessments are conducted at the appropriate acquisition milestone.

d. Army responsibility. To successfully implement the CCA, the Army must embrace new ways of doing business and ensure that IT investments provide measurable improvements in mission performance.

16-25. Electronic commerce (EC)

a. Army need. The quick and seamless transfer of knowledge is key to the Army achieving its vision of the future. The *Army Vision* focuses on six aspects of achieving full spectrum dominance: project the force, protect the force, shape the battlespace, decisive operations, sustain the force, and gain information dominance. This last aspect is by no means the least; it is fundamental to the success of each of the preceding aspects. To gain information dominance, the Army must have a strategy that addresses the effective and efficient management and use of EC technologies.

b. EC origins. Electronic business/electronic commerce (EB/EC) continues to emerge as one of the dominant concepts in commercial IT. A number of trends have contributed to this development, including the need to cut costs and realize savings through process improvements, paperwork reduction, and reengineering. In 1997, Congress defined electronic commerce (EC) as "electronic techniques for accomplishing business transactions, including electronic mail or messaging, World Wide Web (WWW) technology, electronic bulletin boards, purchase cards,

electronic funds transfers, and electronic data interchange.” Since that time, the more descriptive term electronic business/electronic commerce has been adopted throughout the Government and the private sector.

c. Army implementation. For the Army, an integral part of implementing EB/EC is the application of business process improvement/reengineering to streamline and remove non-value added functions from Army business processes prior to the incorporation of technologies facilitating the electronic exchange of business information. Examples of technologies that are frequently employed as EB/EC enablers include bar coding, workflow management systems, public key infrastructure, smart cards, and web based applications. The Army policy is that its activities will use EB/EC technologies to the maximum extent practicable to promote the goal of a paper-free (or near paper-free) business environment within the Army.

d. Army planning and implementation. The Army has developed, formally coordinated, and published three key EB/EC documents that lay the foundation for Army-wide adoption of EB/EC techniques. These documents are the Army Electronic Commerce Strategic Plan (March 1998), HQDA Letter 25-99-1, U.S. Army Electronic Commerce Policy(15 October 99), and the U.S. Army Electronic Business/Electronic Commerce Implementation Plan (Oct 99). All three of these documents affirm the value of a process-based view of EB/EC and emphasize the need to streamline business processes and leverage EB/EC technologies to support the information needs of the warfighter and other stakeholders. Collectively, these three documents provide the policy framework, strategic roadmap, and implementation details to achieve an Army-wide integrated electronic business environment targeting all functional areas (logistics, transportation, procurement, etc.) with special emphasis on cross-functional integration. These key Army EB/EC documents may be viewed at <http://www.armyec.com/core.html>.

e. Enabling technology programs. Two key enabling technology programs, Smart Cards and Public Key Infrastructure (PKI), are managed under the EB/EC umbrella. These technologies are EB/EC enablers mandated for Department-wide implementation. Beginning in Fiscal Year 2001 and through 2002, the Army will issue Smart Cards to 1.4 million Active Army, Selected Reserve, National Guard, civilian, and eligible contractor personnel. The Smart Card will be used as a common access card (CAC) for personnel identification, building access, and network access via PKI certificates. Once implemented, the Smart Card/CAC has the potential to facilitate EB/EC and provide portable electronic capabilities to multiple business processes across the Army. The Army CIO released interim CAC and PKI Policy messages in December 2000. These documents establish the policy and roles and responsibilities in the Army for CAC and PKI implementation. Key Army Smart Card, CAC, and PKI documents may be viewed at: <http://www.armyec.com>.

f. Results. Through the cost-effective application of EB/EC, the Army will be able to achieve improved business processes, respond to changing environments, and effect timely, accurate, and secure information sharing. Moreover, by capitalizing on streamlined and technically innovative business practices, Army EB/EC unites all functional areas into a cohesive electronic business network. Further information on EB/EC—both within the Army and more broadly—can be found at the Army’s EB/EC website located at <http://www.armyec.com>.

SECTION IX SPACE AND NETWORKS

16-26. Contracting for telecommunications services

Telecommunications support provides inter- and intra-communications between various information systems. To foster improved telecommunications economy and discipline, Army personnel should be familiar with contracting telecommunications services through the U. S. Army Signal Command Networks, Engineering, and Telecommunications Activity (USANETA), Army Network and Systems Operation Center (ANSOC), and U.S. Army Communication and Electronics Command's (CECOM) Systems Management Center (SMC).

16-27. Roles of USANETA, ANSOC, and CECOM

USANETA at Fort Huachuca provides deployable contingency information systems engineering and implementation support to warfighting commanders-in-chief; serves as the Army's centralized office for long-haul telecommunications (Defense Information Systems Network, Federal Technology Service 2001, etc.) and provides support for short-haul telecommunications. The ANSOC consists of dedicated teams providing system, network, database management, and information assurance (security) support to U.S. Army customers. CECOM's Systems Management Center acquires and fields telecommunications systems, equipment, and services for Army and DOD customers.

16-28. The Global Command and Control System-Army (GCCS-A)

a. GCCS-A provides for the apportionment, mobilization, allocation, deployment, and sustainment of Army forces to the combatant commands during a war, crisis situations, stability and support. The GCCS-A is also the Army's link into the Joint GCCS – the DOD's GCCS-A supports the Army's functional "mission needs" defined for the Joint GCCS and the Army Horizontal Integration of the Battlefield MNS. GCCS-A provides a modernized and integrated C4I system supporting the monitoring, planning, and execution of the full range of Joint, Combined and Army operations.

b. Serving as the bridge between the tactical components of Army Battle Command System (ABCS) and the Joint GCCS, GCCS-A provides additional Army specific strategic and component command level functionality that leverages existing ABCS and GCCS capabilities. GCCS-A provides Army command and control (C2) at the strategic and operational/theater level of command. As part of the ABCS, GCCS-A incorporates the necessary interoperability, integration, and common requirements of the ABCS Capstone Requirements Document (CRD). GCCS-A is an operational C2 system that supports the force projection strategy by providing a suite of applications, mission critical information, and automated decision support tools to Army commanders, operators and planners, operations, or peacetime.

SECTION X C4/IT INFRASTRUCTURE

16-29. Synchronization tool

The Installation Information Infrastructure Architecture (I3A) is a synchronization tool encompassing major Army automation and communications programs, thus supporting the sustaining base of the JTA-A. It is used for designing target system architectures and cost models for Army installations worldwide.

a. Compliance. Army organizations must comply with I3A guidelines for modernizing IT infrastructures from the installation gateway to the end user boundary.

b. Components. I3A includes all components of the office installation communications capabilities. It addresses the details of the common user facilities providing the transport capability for voice, data and imagery and the appropriate information assurance thereof. The I3A also addresses the components that are required to provide connectivity from the installation long-haul point of presence to the end user device, supporting the warfighter.

16-30. CIO responsibilities.

The CIO is the Army's functional proponent for modernization of the installation C4/IT infrastructure. Using the I3A, the CIO determines the infrastructure requirements. C4/IT Infrastructure modernization is the main initiative to digitize installations and provide connectivity within the installations and to other CONUS support activities as well as the deployed combat forces. The C4/IT Infrastructure consists of all the elements of the communications capability required to transmit voice, data and images within the installation and provide the connection to government and commercial long haul networks. C4/IT infrastructure represents the installation-level distribution portion of the Warfighter Information Network (WIN). Modernization of the C4/IT Infrastructure provides the necessary installation infrastructure to enable process improvement and mission economies which will implement efforts such as paperless contracting, digital publication distribution, internet commerce, public key initiatives, the redesigned travel system, and velocity logistics management initiatives.

SECTION XI RESERVES

16-31. General background

According to the CCA, Executive Branch offices below the agency level may be delegated the authority for a CIO at the discretion of the agency head. This authority was extended to the U.S. Army Reserve by the Secretary of the Army. In September 1997, the Chief, Army Reserve (CAR) established a program to stand up the Army Reserve CIO. The following year, the first Army Reserve CIO was appointed. While the first and second Army Reserve CIOs were military people, the current CIO is a civilian. The long-term nature of the organizational development task and the need for continuity led to the decision ultimately to staff the Army Reserve CIO position with a Senior Executive Service (SES) level civilian.

16-32. Reserve overview

a. CIO goals. The immediate goals of the CIO were to unify and improve the provision of IT services across the U.S. Army Reserve while building the capabilities necessary to perform the IT investment management processes envisioned in CCA. To meet these goals, organizational capabilities are required in the areas of services planning and management, IT investment management, architecture planning, data management, personnel management, financial management, and information assurance. Initial CIO organizational capabilities existed in the area of services management, implementation planning, financial management, and system and technical architecture planning.

b. Organizational changes. Information assurance expertise was transferred into the CIO from the U.S. Army Reserve Command (USARC) Deputy Chief of Staff for Intelligence (DCSIntel), along with the network security mission formerly provided by the DCSIntel. From

the beginning, the Army Reserve CIO has been engaged in developing the additional capabilities.

c. Other CIO responsibilities. The Army Reserve CIO retains responsibilities that are not related to CCA. The CIO subsumed the positions and responsibilities of the Director of Information Management, Office of the Chief, Army Reserve (OCAR); the Deputy Chief of Staff for Information Management (DCSIM), USARC; and elements of Personnel Systems Information Operations (PSIO), Army Reserve Personnel Command (AR-PERSCOM). As a result, the Army Reserve CIO functions as a Director of Information Management (DOIM) for those three major headquarters and as the program manager for automation, telecommunications, postal services, printing, and publications Army Reserve wide. As the result of recent directives, the CIO also has program management responsibility for all cross-functional application systems. The principle application that is of concern at this time is the Regional Level Application Software (RLAS), an application suite of personnel, finance, and training functions provided to Army Reserve units and their command and control up-trace.

d. Accomplishments. As a part of the organizational development effort, the CIO has begun the annual development and revision of the Army Reserve CIO Strategic Plan. The Strategic Plan covers both on-going CIO activities and development of the specific CCA related capabilities that the organization requires. The Army Reserve CIO Strategic Plan serves these purposes:

(1) Integrate the principles and processes of strategic planning for information management into the CIO organization.

(2) Help communicate to Army Reserve CIO customers where the CIO program is today and where it needs to be in the future.

(3) Begin to satisfy IT management strategic planning requirements established by the CCA.

(4) Set the stage for further CIO and Army Reserve level IT strategic and operational planning cycles under the direction of the CAR and other Army Reserve senior leaders.

(a) The Plan sets forth the following Army Reserve CIO mission and vision:

1 Army Reserve CIO Mission – Provide centralized direction and accountability for information technology and information resource management to enhance Army Reserve users' ability to achieve recruiting, retention, readiness, resourcing, and relevance goals and objectives.

2 Army Reserve CIO Vision – Users working in a seamless, integrated, compatible, secure, robust, and cost-efficient Army Reserve information technology enterprise environment. An environment capable of providing effective mission support and ease of use at all levels.

(b) The Plan sets forth seven top-level CIO goals supported by 37 transition objectives. The goals are these—

1 Establish a SES-level Army Reserve CIO reporting to the CAR/CG USARC.

2 Provide unified information systems support to the Army Reserve.

3 Establish Army Reserve and command-level IT/C4 investment management capabilities.

4 Establish a data management capability in the CIO organization.

- 5** Establish an IT/C4 career development program.
- 6** Improve information systems service levels and performance.
- 7** Create an environment in which information security requirements are fully understood and risks are mitigated in the most cost-effective manner.

e. Metrics. From these goals and associated transition objectives, the CIO has fashioned specific transition programs with performance metrics suitable for rigorous results management. This work includes the construction of a balanced scorecard.

SECTION XII

ARMY MISSION AND TRANSFORMATION CAMPAIGN PRIORITIES

16-33. General background

IT has been identified as a critical enabler for the Army to achieve its Transformation Campaign objectives in a timely and cost effective manner. The Army is looking to IT to speed its transformation from a platform-centric organization to a knowledge-centric organization where the right information is given to the right individual at the right time.

16-34. CIO priorities

The Army CIO has identified the following priorities that support the Army's mission and Transformation Strategy:

a. Digitizing the battlefield.

(1) Definition. Digitization is the collective name for Army programs that provide warfighters a horizontally and vertically integrated digital information capability to support warfighting systems and to assure command and control decision cycle superiority. A unique management structure is used to oversee, coordinate, and direct the integration of digitization activities. The Deputy Chief of Staff for Programs (DCSPRO) provides guidance across the Army on matters related to digitization.

(2) Benefits. Digitization improves effectiveness by enabling near real-time situational awareness, making it possible for soldiers to know their location, the enemy's location, and the location of other friendly forces. Inter-netted computers, linked to sensors and satellite-based navigation systems by robust communications networks, are the essential components of this capability. The Army is fielding a suite of command and control systems, selectively procuring weapons systems designed for the digitized battlefield, and integrating required digital components on fielded systems to tap the potential of digitization.

b. Knowledge management.

(1) Vision and mission. The Army's Knowledge Management (KM) vision is to transform the Army institutional elements and operating forces into an information-age, networked organization that leverages its intellectual capital to better organize, equip, and maintain the world's premier land combat force. Our mission is to institutionalize knowledge management into Army culture and processes to achieve a sustaining momentum that will carry it forward through the Army beyond 2025. We will accomplish this through changes in organizational structure, facilities, people, processes, and technology.

(2) Army Knowledge Online. The Army Knowledge Online (AKO) is the Army's focal point for knowledge management. Essentially, AKO is digitizing the institutional Army just as the Army Transformation Campaign is digitizing the tactical Army. AKO users are projected to

reach over one million by 2005. Ultimately the intent is to have all uniformed, civilian, reserve, and (possible) retired Army personnel as AKO users, with each group and sub-group of users having access to content based on their specific information requirements and access permissions.

(3) *Other projects.* Two on-going KM projects that hold a great deal of promise to support force management and knowledge sharing efforts are the Army Flow Model and the HQDA Data Sharing initiative. The Army flow model integrates functional systems across the personnel, logistics, and operational communities to support production of the Total Army Equipment Distribution Plan (TAEDP), the digitized force conversion studies, the Army National Guard Redesign, and Total Army Analysis . The HQDA Data Sharing Initiative allows for a single data collection effort, allows staff analysts to view one authoritative, and single repository for Army systems meta-data; essentially a data mart for specific analytical requirements allowing expanded cross-functional analysis from a single source, leveraging the best commercial practices to support our warfighters.

c. Information assurance.

(1) *Objectives.* The Army Information System Security Program (AISSP) supports two major Army force protection initiatives, which are information assurance and computer network defense (CND) with the goals to secure the Army portion of the Defense Information Infrastructure (DII) and to provide secure information and information based system protection to the force. Securing the DII is accomplished by investments that develop, procure, and sustain Information System Security hardware, software, techniques, procedures, and technologies needed to ensure sustainment of information and communications across the full spectrum of military operations. Information Assurance is not simply an “add-on” to existing IT, but is an integral part of IT development and investment from the identification and validation of a material solution to counter a threat or exploit technology.

(2) *Training programs.* The AISSP also provides for System Administrator/Network Administrator training to assess and counter computer hacker attacks and provides training for Information Systems Security Managers/Officers to assist them in understanding their ISSP responsibilities, as well as providing education and awareness for their leadership and Army commanders.

(3) *Response.* The AISSP program includes defense of major Army Automated Systems both at the perimeter and in-depth, to protect them from disruption caused by attacks originating at multiple entry points. Operational support for Army Information Assurance is enhanced by the Army Computer Emergency Team (ACERT), at Fort Belvoir, VA; and its regional computer emergency response teams (RCERT) in Hawaii, Fort Huachuca, AZ, and 5th Signal Command in Europe. The mission to provide information and information systems protection to the force consists of ensuring that vulnerabilities to Information Warfare Operations are mitigated and computer network attacks within all phases of military operations in all environments are quickly detected and are protected to the greatest extent possible. The AISSP supports detecting system intrusions, alteration, and provides capability to react to information warfare attacks in a measured and coordinated manner. Another RCERT is being developed in Korea. Sustainment of the Army’s initial network security improvements for the out years and continuation of information assurance modernization are key to realization of a truly protected force.

d. Army Enterprise Architecture. Successful warfighting in the 21st Century depends upon warfighters making rapid and correct decisions using accurate and timely information. The availability of such information depends upon information systems that are robust and fully

interoperable within Army units and within the joint environment. Using DOD methodology embodied in the C4ISR Framework Document, and under the mandate of the *Clinger-Cohen Act of 1996*, the Army Enterprise Architecture (AEA) is a cohesive approach to tying the design and fielding of such systems to warfighter requirements. It is now the basis for the Army CIO's (theODISC4) C4I/IT Investment Strategy that encourages synergies between functional areas. Thus, funding the AEA is necessary to attain the goals of *Joint Vision 2020* and the CSA's goal of a digitized division by the year 2000, a digitized corps by 2004. Current AEA efforts include the development of the First Digitized Division architecture and the Installation Information Infrastructure (I3A).

SECTION XIII

SUMMARY AND REFERENCES

16-35. Summary

The Army is in the process of transforming itself into a 21st Century fighting force that employs state-of-the-art IT technology to dominate the information battle space at all times. IT is the critical enabler the Army is employing to achieve its Transformation Campaign Plan goals.

16-36. References

- a. Army Regulation 25-1, *Army Information Management*.
- b. Army Regulation 70-1, *Army Acquisition Policy*.
- c. Army Regulation 71-9, *Materiel Requirements*.
- d. Army Regulation 380-19, *Information Systems Security*.
- e. DA Information Technology Exhibit, *FY 2001 Budget Estimate*, February 2000.