USAR Regulation 25-3

Information Management

Army Reserve Command, Control, Communications, Computers, and Information Technology (C4/IT) Investment Management

Department of the Army
Office of the Chief, Army Reserve
Washington, DC 20310-2400
1 December 2004

SUMMARY OF CHANGE

USAR Reg 25-3
Army Reserve Command, Control, Communications, Computers, and Information Technology (C4/IT) Investment Management

This regulation—

- Prescribes policies and responsibilities and provides guidance on the management of the Army Reserve portfolio of Command, Control, Communications, Computers, and Information Technology (C4/IT) investments.

- Prescribes USAR Form 125-R (Army Reserve Certificate to Operate), USAR Form 133-R (Army Reserve C4/IT Acquisition Request), and USAR Form 139-R (Army Reserve C4/IT Investment Assessment Score Sheet).

Department of the Army
Office of the Chief, Army Reserve
Washington, DC 20310-2400
1 December 2004

Information Management

Army Reserve Command, Control, Communications, Computers and Information Technology (C4/IT) Investment Management

For the Chief, Army Reserve:

JAMES A. KELLEY
Brigadier General, U.S. Army
Chief of Staff

OFFICIAL:

ARTHUR R. TAYLOR
Director
Enterprise Services Activity

History. This is the initial publication of USAR Regulation 25–3.

Summary. This regulation contains guidance on the management of the Army Reserve portfolio of command, control, communications, computers, and information technology (C4/IT) investments.

Applicability. This regulation applies to the Army Reserve, which, for purposes of this regulation, is comprised of the Office of the Chief, Army Reserve (OCAR); the U.S. Army Reserve Command (USARC); and any other activity requesting Army Reserve funding for information technology investments. In accordance with AR 25-1, this regulation applies to all information technology investments, whether for base operations or mission requirements.

Proponent and exception authority. The proponent of this regulation is the Director, Enterprise Services Activity (ESA). The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The proponent may delegate this approval authority, in writing, to an individual under their supervision within the proponent agency in the grade of colonel or the civilian equivalent.

Army management control process. This regulation is subject to the requirements of AR 11-2, Management Control. It contains management control provisions and checklists for conducting management control evaluations of critical management controls associated with C4/IT investment management within the Army Reserve. Checklist questions are provided in appendix B, and additional checklist information is available from AR 25-1, appendix B, paragraph B-4.

Supplementation. Supplementation of this regulation is prohibited without prior approval from the Chief, Army Reserve, ATTN: AFRC-ES, 1401 Deshler Street SW, Fort McPherson, GA 30330-2000.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Chief, Army Reserve, ATTN: AFRC-ES, 1401 Deshler Street SW, Fort McPherson, GA 30330-2000.

Distribution. This publication is available in electronic media on the USARC Intranet web site at https://usarcintra and on the Army Reserve Component portion of the Army Knowledge Online (AKO) web site. It is intended for command level B. Local reproduction is authorized.

Contents (Listed by paragraph number)

Chapter 1
Introduction
Purpose • 1-1
References • 1-2
Explanation of abbreviations and terms • 1-3
Recordkeeping requirements • 1-4
C4/IT investment management in the Army Reserve • 1-5

Chapter 2
Responsibilities
Army Reserve senior leadership • 2-1
Director, Enterprise Services Activity (ESA) • 2-2
Army Reserve functional proponents (principal staff) • 2-3
USARC major subordinate commands • 2-4

Army Reserve automated information system (AIS) developers • 2-5
Army Reserve financial officers • 2-6
Contract Administration Support Office (CASO) • 2-7

Chapter 3
C4/IT Investment Management Procedures
General • 3-1
C4/IT investment planning • 3-2
C4/IT investment programming • 3-3
C4/IT investment project initiation • 3-4
C4/IT investment acquisition • 3-5
C4/IT investment fielding and operation • 3-6
C4/IT investment project evaluation and disposal • 3-7

Chapter 4
Enterprise Architecture Management
Overview • 4-1
Operational architecture management • 4-2
Systems architecture management • 4-3
Technical architecture management • 4-4
Data administration • 4-5

Chapter 5
Army Reserve Automated Information System (AIS) Management
General • 5-1
Target application architecture • 5-2
AIS development • 5-3

Chapter 6
Certificate to Operate
Backgkround • 6-1
Applicability • 6-2
Documentation • 6-3
Testing • 6-4
Processing • 6-5
Documentation • 5-3

Appendixes
A. References
B. Critical Management Controls for Information Management in the Army Reserve
C. Investment Management Process Flow
D. C4/IT Investment Decision Package Outline
E. Architecture Impact Assessment Outline
F. Instructions for Required Forms
G. Requirements Statements and Audit Identification Numbers

Figure List

Figure 1-1: Sample global DOD architecture
Figure C-1: C4/IT investment planning
Figure C-2: C4/IT investment programming
Figure C-3: C4/IT project initiation and authorization (1)
Figure C-4: C4/IT initiation and authorization (2)
Figure C-5: C4/IT project acquisition
Figure C-6: C4/IT fielding and operation
Figure C-7: C4/IT investment evaluation and disposal
Figure D-1: Sample format for C4/IT investment decision package outline
Figure E-1: Format for Architecture Impact Assessment Outline

Glossary

Chapter 1
Introduction

1-1. Purpose
This regulation establishes the policies and assigns responsibilities for the management of the Army Reserve portfolio of investments supporting command, control, communications, computers, and information technology (C4/IT). It implements the provisions of Public Law 104-106, Clinger-Cohen Act of 1996 (formerly Division E, Information Technology Management Reform Act, Defense Authorization Act of 1996), AR 25–1, and other related Department of Defense (DOD) and Department of the Army directives. It addresses the management of information as a mission-critical Army Reserve resource, the technology that supports information requirements, and the resources supporting C4/IT.

1-2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Recordkeeping requirements
This regulation requires the creation of records to document and support the business processes of the Army Reserve. Records created under the purview of this regulation, regardless of content or format, will be kept in accordance with the retention schedules found in AR 25-400-2, Army Records Information Management System (ARIMS).

1-5. C4/IT investment management in the Army Reserve
a. The Army Reserve, like the Army as a whole, is increasingly reliant on automation for mission effectiveness and operational efficiency. As a result, any action that affects C4/IT has an amplified impact on the whole organization. The C4/IT investments must be evaluated, selected, and controlled to achieve the best organizational outcomes possible using limited resources. Ineffectively managed investment decisions of the past resulted in corrective legislation. The Government Performance and Results Act of 1993 requires linking investments directly to targeted organizational outcomes. The Clinger-Cohen Act of 1996 mandates that Executive Agencies implement rigorous C4/IT investment management practices that rationalize the ranking and prioritization of C4/IT projects based on benefits, cost, and risk. Supported by Office of Management and Budget (OMB) policies and AR 25–1, the Act directs the Army Reserve to implement C4/IT strategic planning, investment management, and architecture modeling processes.

b. Another major factor influencing the management of C4/IT within the Army and the Army Reserve is the Army Transformation. As a part of the Army Staff Redesign and Army Knowledge Management initiatives, C4/IT support is being consolidated across the Army. All network and telecommunication services eventually will transition to the Network Enterprise Technology Command (NETCOM) under the Army CIO/G-6. At the same time, base operations C4/IT support for the Active Component is being transitioned to the Installation Management Activity. In the Army Reserve, Information Management Officers are established to provide base operations C4/IT support. Other aspects of the Army Knowledge Management and Army Knowledge On-line initiatives are driving the centralization of common service provisioning, C4/IT investment management processes, and architecture impact assessments.

c. Effective management of Army Reserve C4/IT investments has impact far beyond Army Reserve boundaries. DOD is formulating new joint war-fighting doctrine that relies heavily on the enabling capabilities of advanced information technologies. This new doctrine is called net-centric operations and warfare (NCOW) and is based on the concept of the Global Information Grid (GIG), the totality of all Department of Defense networks, computers, applications, and data and the people that use them. While the Army remains the primary proponent of land warfare doctrine within the DOD, specific Army initiatives, such as Digitization of the Army and the Future Force, must be realized within the context of this new DOD vision for joint, inter-agency, and multinational (JIM) operations. The Army Knowledge Management (AKM) initiative broadly embeds the net-centric vision into our concept of daily operations through pervasive application of knowledge management principles.

d. Becoming a knowledge-based, network-centric force in all aspects of warfare, support, and business will be a key enabler of enhanced mission performance. The Army must align the information infrastructure (“infostructure”) to the new doctrine. A key element of Army efforts to align the infostructure is AKM Goal 4: Scale AKO to become the Army portal. Associated guidance requires all applications to be “webified” and linked to AKO for single sign-on. Translating all applications to this specific architecture is the first step in achieving the DOD GIG Enterprise Services Architecture (see fig 1-1).

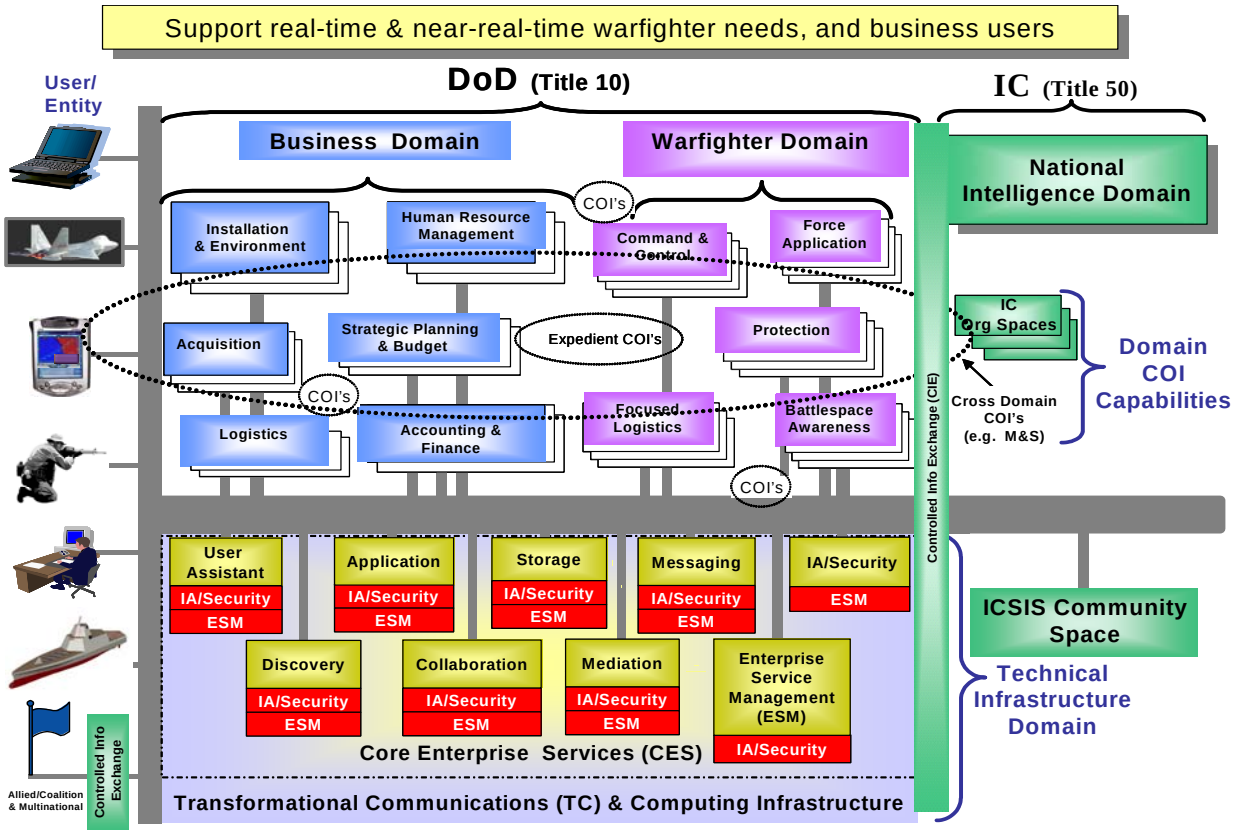

Figure 1-1. DOD GIG Enterprise Services Architecture

e. In the target architecture, all applications will be programmed as services that will be available on the network to users with Web browsers and to other applications. The network itself will host certain services called GIG Enterprise Services (GIG-ES or GES) that will be shared by all applications and users. DOD plans to implement nine of these services. All other services will be built by joint communities-of-interest to support their business and command decision-making processes. The network itself will be multifaceted to bridge the different locales from which users will access the network. These include battlefields, theater support areas, home bases of operations, training venues, business venues, soldiers' homes, and other locations.

f. The Army implementation of the GIG architecture is called the GIG-Army architecture. This architecture enables critical tenets of the Future Force, such as integration of information flows from "foxhole to factory." The Army Reserve, as a key provider of reach-back support to the combat team, will transition our applications and networks into the GIG-Army architecture to realize this vision. Beyond that, day-to-day Army Reserve operations must be streamlined and managed more effectively within a constrained resource environment. To maximize return on investment, Army Reserve training, sustainment, and business operations must be redesigned around an infostructure that provides access to decision information anywhere at anytime.

g. The Army Reserve is realigning organizationally to facilitate these transitions both now and into the future. Just as importantly, Army Reserve management of C4/IT investments must be aligned with this guidance to achieve the goals envisioned by DOD and Army leadership.

Chapter 2
Responsibilities

2-1. Army Reserve senior leadership

a. Army Reserve Investment Review Council (IRC). The Army Reserve IRC is the authorizing body for the Army Reserve regarding C4/IT investments. The Army Reserve IRC will operate within the context of Clinger-Cohen requirements and the integrated Planning, Programming, Budgeting, and Execution (PPBE) process.

(1) The Army Reserve IRC will—

(a) Review and approve the Army Reserve C4/IT Strategic Plan and other Army Reserve C4/IT plans.

(b) Review and approve Army Reserve C4/IT investment strategies and set priorities for C4/IT programs and resources.

(c) Ensure Army Reserve C4/IT resources are efficiently applied to meet the missions, goals, and objectives of the Army Reserve.

(d) Review and authorize all Army Reserve C4/IT projects, including Command level projects elevated to the Army Reserve level (see paragraph 3–2b(3)).

(e) Prioritize Army Reserve C4/IT projects for PPBE purposes.

(2) Membership. The Army Reserve IRC has the following membership:

(a) Army Reserve Chief of Staff (Chair).

(b) Director, ESA (Secretary of the IRC). In this role, the Director, ESA will—

- Plan for and provide appropriate automation support for IRC processes, including collaboration sites, e-mail, and other electronic means of conducting IRC business.
- Establish processes for and supervise the flow of actions between functional proponents and the IRC.
- Schedule IRC meetings, if required (most IRC work should be accomplished through normal staffing channels), and provide logistical support.
- Assemble agenda materials for IRC meetings and finalize agendas with the IRC chair.
- Document IRC proceedings, decisions, and directives. (Records associated with Army Reserve IRC proceedings, decisions, and directives will be filed under ARIMS Record Number 25-1a2.)
- Route investment proposals requiring further authorization to and from the Army CIO Executive Council.

(c) Deputy Chief, Army Reserve (DCAR).

(d) Chief Financial Management Officer (CFMO).

(e) Principal Staff Directors.

(f) Inspector General (IG).

(g) Director, Internal Review (IR).

(h) Director, Installation Management Agency–Army Reserve (IMA-AR).

b. Operating Agency (OA) 23/24 IRC. The OA 23/24 IRC has responsibilities similar to the Army Reserve IRC for those C4/IT investments within their purview as defined in paragraph 3-3c. Records associated with OA 23/24 IRC proceedings, decisions, and directives will be filed under ARIMS Record Number 25-1a3. The membership of the OA 23/24 IRC is as follows:

(1) Army Reserve Chief of Staff (Chair).

(2) Director, ESA (Secretary).

(3) Principle Staff Directors.

(4) Inspector General (IG).

(5) Director, Internal Review (IR).

c. Other commands executing Army Reserve resources. Other commands executing Army Reserve resources should institute C4/IT investment bodies similar to the OA 23/24 IRC, consistent with AR 25-1 and this guidance, to control those C4/IT investments within their purview as defined in paragraph 3-3c.

2-2. Director, Enterprise Services Activity (ESA)

a. The Director, ESA serves in Army Reserve enterprise roles as well as in USARC-specific roles. At the enterprise level, the Director, ESA acts as an agent of the CIO/G-6 of the Army to manage Army Reserve C4/IT investment management processes and serves as the Director of ESA, the Army Reserve Chief Technology Officer, and the Army Reserve Regional CIO (RCIO). Throughout this document, all of these roles are referred to as the Director, ESA.

b. The Director, ESA will—

(1) Serve as the Chief Information Officer (CIO) of the USARC. (Many of the duties and responsibilities of a chief information officer are specified in the Clinger-Cohen Act of 1996 and within AR 25-1 for the Army.)

(2) Formulate policy and manage C4/IT for the Army Reserve.

(3) Plan, organize, and execute Clinger-Cohen compliant Army Reserve C4/IT investment management processes and serve as the Secretary of the Army Reserve and OA 23/24 IRCs.

(4) Evaluate all non-tactical Army Reserve C4/IT resource requirements submitted in the Planning, Programming, Budgeting, and Execution (PPBE) process.

(5) Maintain a comprehensive portfolio of approved and proposed Army Reserve C4/IT investments ranked by benefits, costs, and risks.

(6) Represent the Army Reserve in CIO decision forums at the Department of the Army and the Department of Defense. Pass actions between the Army Reserve and the Army CIO Executive Council.

(7) Act as the designated approving authority (DAA) for the Army Reserve Network (ARNet).

(8) Develop requirements and direct and manage the information management activities of sustaining base information systems.

(9) Centralize and consolidate, wherever practical, C4/IT services to the Army Reserve in support of the Army CIO/G-6 transformation goals.

(10) Plan and execute transition of the Army Reserve Network into the “One Army” network at the appropriate time.

(11) Execute and enforce NETCOM and Army information management policies, standards, and architectures. Maintain the Army Reserve portion of the Army Information Technology Repository (AITR).

(12) Execute technical control over all Information Management Officers at OCAR, USARC Headquarters, and major subordinate commands.

(13) Act as the Army Reserve Enterprise Architect. Facilitate and coordinate development of operational architectures and functional plans for data and application portfolios. Maintain an Army Reserve C4/IT Strategic Plan including "as is" and "to be" views and integrated transition plans.

(14) Act as the Army Reserve Systems Architect. Define and document the architecture of the Army Reserve portfolios of data and applications and the supporting technological infrastructure. Implement the GIG-Army architecture within Army Reserve systems and networks.

(15) Act as the Army Reserve Technical Architect. Define the technical standards needed by the Army Reserve beyond the Joint Technical Architecture–Army (JTA–Army).

(16) Act as the Army Reserve Component Data Administrator (CDAd).

(17) Act as Army Reserve C4/IT Acquisition Executive. Review and approve all acquisition plans, contracts, and tasks for the acquisition of C4/IT equipment, software, and related services within the Army Reserve.

(18) Review new technologies and advise Army Reserve leadership on the readiness of those technologies for use within the Army Reserve.

(19) Coordinate development and monitor execution of organizational strategic and annual performance plans.

(20) Develop courses of action (COAs) and perform impact analysis on technology-related decision situations for Army Reserve leadership.

(21) Represent the Army Reserve in all Army RCIO venues, ensuring that Army Reserve requirements are included in all Army initiatives to move toward the "One Army" network.

2-3. Army Reserve functional proponents (principal staff)

All Army Reserve functional proponents will—

a. Develop functional C4/IT plans in support of the programming and budgeting cycles and coordinate their plans through the Director, ESA. The Director, ESA will assist the functional proponents in this process.

b. Establish C4/IT investment Integrated Product Teams (IPTs) as required in paragraph 3–2c. The IPTs or other proponent representatives will prepare decision packages, including architecture impact analyses, for all proposed C4/IT investments and will provide investment measurement data to the Director, ESA for investment evaluation. The Director, ESA will assist in these processes.

c. Submit all acquisition plans, contracts, and tasks for the acquisition of non-tactical C4/IT equipment, software, and related services to the Director, ESA for approval prior to executing any such contract or task.

d. Assume the role of Functional Data Administrator (FDAd) for their respective function within the Army Reserve. They will participate in the communities of interest (COIs) to which they have been assigned for implementation of the Army Network-Centric Data Strategy.

2-4. USARC major subordinate commands

All USARC major subordinate commands (MSC) will—

a. Perform C4/IT planning, programming, investment management, and acquisition responsibilities at their respective command levels similar to those outlined for functional proponents in paragraphs 2–5a through 2–5c. MSC plans and operations will support the Army Reserve C4/IT Strategic Plan and other guidance.

b. Coordinate their mission-related C4/IT plans, requirements, and acquisitions through the USARC functional proponents appropriate to the mission areas affected.

c. In preparation for the eventual transfer of base operations support to the Installation Management Activity (IMA), report all base operations C4/IT requirements and execution according to the Army Reserve Region(s) to which each investment pertains. (For example, a Division Training Support may have copier requirements for facilities in multiple Regions. The copier requirements and execution will be identified with the Regions within which the respective facilities reside.)

d. Ensure that no Army Reserve resources are expended on C4/IT goods or services that have not been authorized in accordance with this guidance.

e. Document C4/IT expenditures for their organizations and associate all C4/IT expenditures with authorized requirements. On at least an annual basis, provide these data to the Director, ESA for inclusion in the C4/IT investment evaluation process (RCS: CSIM49, Part 2).

2-5. Army Reserve automated information system (AIS) developers

Army Reserve AIS developers will—

a. Adhere to the Army Reserve application architecture in all AIS designs and implementations. AIS developers will document AIS utilization of business data objects and maintain program data objects in a central repository to be provided by ESA.

b. Utilize the Center of Excellence provided by the Director, ESA (described in chap 5) to ensure the controlled transition of the Army Reserve to the GIG-Army architecture.

2-6. Army Reserve financial officers

Army Reserve financial officers (Chief Financial Management Officers (CFMOs); Deputy Chiefs of Staff, G-8; comptrollers) will—

a. Ensure that all Army Reserve requirements submitted in the PPBE process that have a C4/IT component have been validated by the Director, ESA.

b. Provide advice and assistance as requested to enable the Director, ESA to ensure that no Army Reserve resources are expended on C4/IT goods or services that have not been authorized in accordance with this guidance.

c. Provide advice and assistance as requested to enable ESA to document C4/IT expenditures and to associate all C4/IT expenditures with authorized requirements. Provide advice and assistance as requested in ESA's performance of the C4/IT investment evaluation process.

2-7. Contract Administration Support Office (CASO)

The CASO will ensure that all acquisition plans submitted that have a non-tactical C4/IT component have been approved by the Director, ESA.

Chapter 3
C4/IT Investment Management Procedures

3-1. General

The Army Reserve C4/IT investment management process is defined below and shall comprise those steps depicted graphically at appendix C. All Army Reserve C4/IT investments, including both capital investments and expenses as defined in DFAS-IN Manual 37-100-XX (current edition), for both base operations support and mission requirements, will be managed by a proponent within the respective command. The respective CIO, G-6, Information Management Officer (IMO), or Director of Information Management (DOIM) will be the proponent for investments principally concerned with C4/IT infrastructure and services for base operations support. Functional investment projects will be managed, in terms of requirements and resources, by the respective functional proponents with architecture and technology support from ESA. All processes depicted here will be managed to be responsive within the decision horizon for both normal and contingency operations as appropriate.

3-2. C4/IT investment planning

Refer to figure C-1. Additional details regarding C4/IT investment planning are in chapter 4.

a. On at least a biannual basis, functional proponents and MSCs will construct or update functional C4/IT plans (see paras 2–3 and 2–4). The MSCs will submit their mission-related plans through the respective USARC functional proponents appropriate to the mission areas affected. Based on required mission capabilities and business processes, proponents will determine the portfolios of C4/IT capabilities (equipment, communications, applications, and data) that will most effectively support their areas of responsibility. Proponents will compare their idealized portfolios with existing C4/IT capabilities and perform a gap analysis, which will result in prioritized lists of transitional projects to fill critical gaps. The target functional portfolio together with the list of transitional projects constitutes a functional C4/IT plan. Functional C4/IT plans will be provided to ESA, ATTN: Chief, Enterprise Plans Office, during the first quarter of the respective fiscal year (RCS: RCIM-080). Functional and MSC C4/IT plans and related documents will be filed under ARIMS Record Number 25-1c2.

b. Using a similar process, the Director, ESA will plan C4/IT projects to upgrade and maintain the enterprise infrastructure to meet current and projected requirements. In coordination with functional proponents, the Director, ESA will integrate functional C4/IT projects with ESA projects to produce a time-phased Army Reserve C4/IT Strategic Plan. In this process, C4/IT projects may be combined, eliminated, or reconfigured to produce the set of C4/IT investments most beneficial to the Army Reserve. The Director, ESA will staff the resulting proposed plan to all functional proponents and MSCs.

c. The Director, ESA will present the proposed C4/IT Strategic Plan and a proposed set of C4/IT investment selection criteria to the Army Reserve IRC for approval. The IRC will review, adjust, and approve the Strategic Plan and investment selection criteria. Based on IRC decisions, all proponents will revise their own C4/IT plans. The approved Army Reserve C4/IT Strategic Plan and related documents will be filed under ARIMS Record Number 25-1c2.

3-3. C4/IT investment programming

Refer to figure C-2.

a. Based on the approved C4/IT Strategic Plan, functional proponents and MSCs will submit their proposed investments as requirements to the PPBE process. MSCs will submit their mission-related requirements through the USARC functional proponents appropriate to the mission areas affected. Proponents will document each proposed investment with a Requirement Statement (RS) and assign each a unique Requirement Statement Audit Identification Number (RSAIN) as outlined in appendix H (RCS: CSIM-49, Part 1). Financial managers will screen submissions for requirements that contain proposed expenditures for C4/IT and route those to the Director, ESA for analysis. The RSs will be filed under ARIMS Record Number 25-1e1 if validated or 25-1e2 if not validated.

b. The Director, ESA will compare the proposed investments represented in the RSs to the approved Army Reserve C4/IT Strategic Plan, previous C4/IT investment performance, and other existing or planned C4/IT capabilities. To avoid making C4/IT investments for business functions that are not inherently governmental, the Director, ESA will analyze each proposal for possible outsourcing of the associated business function in accordance with AR 25–1, paragraphs 3-3b, 3-3d, and 3-5. The Director, ESA will assure that mission-related requirements have been validated by the USARC functional proponents appropriate to the mission areas affected. Based on these analyses, the Director, ESA will make the following recommendations for each proposed non-tactical C4/IT investment to the respective IRC:

(1) Whether or not to authorize the investment.
(2) To study the business function for possible outsourcing if appropriate.
(3) The relative priority of the investment within the portfolio of Army Reserve C4/IT investments.
(4) To consolidate multiple existing or proposed C4/IT investments that duplicate C4/IT capabilities.
(5) To manage the investment as a "major C4/IT investment project" as defined in paragraph 3-4.
(6) To elevate mission critical OA-level investment projects to the Army Reserve level (see para 3-3c below).

c. The Director, ESA will collate all C4/IT proposed investments into a consolidated portfolio of all existing and proposed Army Reserve C4/IT investments ranked by benefits, costs, and risks. The consolidated portfolio will be presented to the respective IRC for validation and prioritization at their respective level. All C4/IT investment proposals will be considered at the operating agency (OA) level unless any one or more of the following apply, in which case the investment must be authorized at the Army Reserve level. Investments must be elevated to the Army Reserve level that—

(1) have a scope of requirements that spans more than one operating agency within the Army Reserve;
(2) require funding beyond operating agency obligation authority;
(3) are estimated to cost more than $200,000 per year or more than $5 million in life cycle costs; or
(4) are deemed by the Chief, Army Reserve (CAR) to be critical to the mission success of the Army Reserve.

d. For purposes of coordination with the CIO/G-6 of the Army, the CIO will enter information for selected C4/IT investments validated at the IRC level into the Army Information Technology Repository (AITR) database as appropriate. (The AITR serves as the Army repository of all C4/IT investments that are subject to AKM Goal 1, AKM Goal 4, and Certificate of Networthiness and Certificate to Operate processes.)

e. All C4/IT investments greater than the level determined by the Army CIO/G-6 must be authorized by the Army CIO Executive Council. The Executive Council will use PPBE requirements justifications plus any information in the AITR database to evaluate C4/IT investment proposals. The Program Evaluation Groups (PEGs) use CIO Executive Council recommendations in making final requirements validation and resource allocation decisions.

f. IRC and higher validation and prioritization decisions will be returned to the respective financial officers for further PPBE processing. Functional proponents will revise their C4/IT plans based on final validation, prioritization, and resource allocation decisions.

3-4. C4/IT investment project initiation

Refer to figures C-3 and C-4. During requirements validation, all Army Reserve C4/IT investment projects that significantly expand existing capabilities or that acquire new capabilities may be identified as "major C4/IT investment projects" by the respective IRC. All major C4/IT investment projects will be subject to the following management and authorization process. All documents relating to the management of an Army Reserve major C4/IT investment project throughout its life cycle will be filed under ARIMS Record Number 25-1ppp3.

a. All Army Reserve major C4/IT investment projects will be conducted under the oversight of an integrated product team (IPT) in accordance with AR 70–1, paragraph 1-4a. The primary functions of an IPT are to establish the business case for the investment, to define the scope of the investment and the associated requirements, to manage the execution of resources for the investment, and to measure and take appropriate actions regarding investment performance. The investment proponent will appoint the IPT chair. IPTs will include representatives of their respective CIO, G-6, IMO, or DOIM to assist with all technical aspects of their investment projects. IPTs will also include representatives of other directorates and commands directly affected by their investment projects.

b. AR 25–1, paragraph 3-4, mandates levels of C4/IT investment above which business process analysis and revision must be completed before the investment can be authorized. Only those C4/IT investments listed in AR 25-1, paragraph 3-4i, may be authorized without formal analysis or revision. All business process analysis and revision will be completed before C4/IT needs and requirements are specified. Process identification, documentation, and improvement will be consistent with AR 5-1, strategic management and performance measurement plans, and Federal Information Processing Standards (FIPS). In this process, business functions that are clearly not inherently governmental will be analyzed for possible outsourcing.

c. The proponent will document the business requirements and the associated automation requirements in accordance with AR 71-9, which may be adapted for the needs of the Army Reserve. The proponent will develop a concept of implementation with prospective timelines and costs, identifying major implementation activities and the business processes they will affect.

d. The proponent will prepare an architectural impact assessment for the proposed C4/IT investment outlining impacts on the Army Reserve architecture (business processes, applications, data, devices, networks, models and simulations, and standards in accordance with the DOD Architecture Framework (DODAF), information assurance, and other proposed or on-going C4/IT investment projects. The respective CIO, G-6, IMO, or DOIM will assist in this analysis. The Architecture

Impact Assessment Outline is located at appendix E. Proponents should use the Army CIO/G-6 Certificate of Networthiness Self Assessment checklists to ensure completeness of documentation.

e. The proponent will coordinate financial estimates of annual, program, and life cycle costs with the respective resource management office (but funding sources need not yet be identified). Impacts will also be coordinated with the owners of affected business processes, data, and other investments. The investment proponent will review the proposal against the C4/IT management policies at AR 25–1, chapter 6.

f. The investment proponent will document the estimated benefits, costs, and risks associated with the proposed investment. Specific investment selection criteria specified by the Army CIO/G-6 must be addressed. Federal Acquisition Regulations (FAR) Part 39.102 provides additional specific guidance on risk categories that should be considered in the analysis. The proponent will propose the risk and return criteria and the performance measurement strategy to be used to evaluate the investment. AR 25–1, paragraph 3-6 outlines this process. The Army Reserve C4/IT Investment Assessment Score Sheet (USAR Form 139-R) will be used to assist in this analysis.

g. The investment proponent will submit a C4/IT investment decision package to ESA, ATTN: Chief, Enterprise Plans Office. The decision package will include, as appropriate to the proposed investment, requirements document(s) and business justification, a summary of business process analysis and revision, the architecture impact assessment, the implementation (milestone) concept, financial estimates, risk analysis, and the proposed investment performance measurement plan. A sample format of a C4/IT investment decision package outline is at figure D-1.

h. The Director, ESA will review the decision package for completeness and for adherence to the C4/IT Strategic Plan, validated requirements, investment selection criteria, and architecture standards. Based on the analysis, the Director, ESA will make a recommendation to the respective IRC as to whether and how the investment should proceed. If the IRC chooses to authorize the investment, they will finalize the risk and return criteria and approve the performance measurement strategy for the investment. The IRC also may choose to establish decision milestones at which the proponent must return to the IRC for continued authorization.

i. Upon authorization, the investment proponent will perform a funding analysis and develop a funding plan for the investment. Defense Finance and Accounting Service – Indianapolis Center (DFAS-IN) Manual 37-100-XX, (latest edition), appendix X1, provides specific guidance on the considerations for capital investments. The funding plan will cover the entire life cycle cost of the investment. C4/IT investments will be screened for "consulting services" per AR 5-14 and Defense FAR Supplement (DFARS), Part 237.201 when the investment is supported by contract.

j. The respective Command may choose to fund all, part, or none of any validated investment in any fiscal year. Resources may be applied to C4/IT investments across multiple fiscal years provided the investment continues to be authorized in accordance with this guidance.

3-5. C4/IT investment acquisition

Refer to figure C-5.

a. When appropriate to the scope of a C4/IT investment project, the investment proponent should name a project manager (PM) to lead the investment acquisition. The PM should be appropriately trained in acquisition and project management disciplines and may act as the contracting officer's representative (COR) as appropriate. (If the PM is to act as a COR, then he or she should be appointed as an alternate COR for the contract.) The Director, ESA will provide PM support services through the Center of Excellence as described in paragraph 5-3a. Proponents are strongly encouraged to use these services when available.

b. The PM will conduct acquisition planning to ensure that full and open competition is obtained to the greatest extent feasible and that commercial items are procured to the maximum extent practicable. See FAR, Part 7 and DFARS, Part 207; see also FAR 39.103 and 39.107. An acquisition plan is required for all USARC procurements exceeding $25,000. The PM will write performance work statements and product descriptions, produce other documentation as required by acquisition regulations, and participate in vendor selection activities as appropriate. All acquisition plans will address the Government's rights in accordance with DFARS Part 227. All projects exceeding 60 days duration will include a program management plan, a project plan, a risk management plan, and a quality control and testing plan scaled appropriately to the specific project. The PM must ensure that the project satisfies all C4/IT management policies in AR 25–1, chapter 6.

c. Proponents will document all acquisition plans and procurement requests involving purchase of non-tactical C4/IT hardware, software, or related services on USAR Form 133-R and forward it to ESA, ATTN: Chief, Enterprise Plans Office. Instructions for completing the form are in paragraph F-2. The Director, ESA will forward all approved plans and requests to the CASO as required by acquisition policies.

d. Army Reserve C4/IT investment projects will be divided into no less than six phases: a business analysis and requirements phase, a design phase, a construction/testing phase, a fielding phase, an operations and maintenance (O&M) phase, and a disposal phase. As noted above, the respective command may choose to authorize the investment by phases with milestone reviews required to obtain continued authorization. Additionally, the Director, ESA will impose a design review at the end of the design phase to ensure that the solution design adheres to Army and Army Reserve architecture guidance and plans, and is supportable on the Army Reserve network.

e. Army Reserve-sponsored development of applications will be performed in conjunction with the capabilities provided by the Director, ESA in the Center of Excellence as described in paragraph 5-3a.

3-6. C4/IT investment fielding and operation

Refer to figure C-6.

a. All investment proponents will follow the guidelines of the Army CIO/G-6 and NETCOM to obtain a Certificate of Networthiness and a Certificate to Operate, including providing ESA with all data required to maintain the AITR. All documentation required by the Army Reserve C4/IT investment management process is designed to feed these Army level processes directly to minimize additional effort for the proponent. Until the NETCOM Certificate to Operate (CTO) process is fully operational, proponents will not field solutions until they have been granted an Army Reserve Certificate to Operate as described in chapter 6.

b. No automated systems that contain or process sensitive but unclassified (SBU) or classified data may be fielded or operated without being certified and accredited in accordance with DODI 5200.40 and AR 25-2. The PM must ensure that appropriate activities are included in all statements of work to provide the required information assurance capabilities. Simulations and models must be managed in accordance with AR 5-11.

c. All C4/IT investment proponents must gather the investment performance measurements mandated for their investments and provide the measurements to the Director, ESA. Performance measurement data, analysis, and results set out in performance measurement plans will be provided to the Director, ESA no less than 30 days before IRC validation of further authorization is due (RCS: RCIM-081).

3-7. C4/IT investment project evaluation and disposal

Refer to figures C-6 and C-7.

a. No less than annually, the Director, ESA will review all Army Reserve C4/IT investments and assess them for continued validity in accordance with AR 25–1, paragraphs 3-3b and 3-3d. Director, ESA assessments will be given to the respective IRC for decisions on continued authorization and funding.

b. The respective IRC will review all fielded systems (including systems already initiated or fielded at the effective date of this policy) for potential disposal or termination at the end of their original estimated useful life, at a minimum.

c. When investments reach end of life, proponents will assist the Director, ESA in the shut down and transition of operations, close-out of all open contracts and tasks, and redistribution of serviceable equipment and unexpired maintenance agreements and software licenses.

Chapter 4
Enterprise Architecture Management

4-1. Overview

a. Purpose. The purpose of enterprise architecture management is to document the Army Reserve C4/IT Strategic Plan and to instill the disciplines necessary to make controlled changes to our architecture. The goal is to maximize the effectiveness of the organization through appropriate application of technology while minimizing loss of performance because of disruptions associated with architecture changes. The Army Reserve C4/IT Strategic Plan is a key component of the C4/IT investment decision process as required by the Clinger-Cohen Act. All Army Reserve architecture management will be performed in the context of overarching architecture decisions promulgated by higher command authority and will not duplicate architecture management activities performed at higher levels.

b. Architecture framework. The Army Reserve adheres to the DOD Architecture Framework (DODAF), which defines three levels of architecture. The operational architecture defines how an organization goes about its business, whether that is going to war or performing training or administrative functions. The operational architecture consists of the organization's structure, processes, and information requirements. The system architecture depicts the portfolio of data and AIS that support the execution of the operational architecture, including how the individual parts of the portfolio interact with one another, how they are built, and where and how they provide their services to the user. The technical architecture defines the standards by which C4/IT capabilities are designed and built. A full C4/IT Strategic Plan consists of a current situation picture ("as is" view), a target picture ("to be" view), and transition plans to move from the "as is" to the "to be" architecture. The Army Reserve will use the DODAF framework to manage Army Reserve unique C4/IT implementations, including our implementation and use of systems and data mandated by higher levels of authority.

c. Data architecture. A common thread in both the operational and systems architectures is the data used by the organization. Data are the medium by which information is conveyed from its source to its users. The information content of data depends on two aspects. First, there must be semantic agreement between the creator of the data and the users of that data; that is, there must be agreement on what the data purports to represent and how it will be represented. Second, there must be confidence in the reliability of the actual data to convey its intended meaning; that is, there must be the ability to judge if the data were collected and processed in a way that is consistent with how it is intended to be used. Data architecture management (also called data administration) consists of managing the definition, collection, processing, storage, and dissemination of data as an enterprise asset to maximize the effectiveness of the organization. The Army Reserve will perform data administration for Army Reserve unique data and for Army Reserve use of data defined at higher levels of authority.

4-2. Operational architecture management

a. Operational architecture documentation. Functional proponents will maintain their portions of the Army Reserve operational architecture. The Director, ESA will coordinate documentation of the Army Reserve operational architecture in a centralized Army Reserve architecture repository. The Director, ESA will leverage existing Army and DOD architecture repositories to prevent duplication. The Repository will include electronic documents where possible, as well as hardcopy. The Director, ESA will provide ready access to the information contents of the Repository to all stakeholders.

b. C4/IT strategic planning. As described in paragraph 3-2a, functional proponents will plan the business processes and the supporting C4/IT capabilities required to achieve the missions assigned to the Army Reserve. Functional proponents will also plan the integration of systems and data mandated by higher levels of authority. The Director, ESA will assist the functional proponents with planning C4/IT transition projects to implement their desired target portfolios. The Director, ESA will integrate functional projects with ESA-generated projects for infrastructure and services to produce a time-phased architecture transition plan as described in paragraph 3-2b. The Director, ESA will combine documentation on "as is" and "to be" operational, system, and technical architectures with the architecture transition plan to produce an Army Reserve C4/IT Strategic Plan. The Director, ESA will present the C4/IT Strategic Plan for senior leader approval (see para 3-2c). This Plan will be brought into compliance with the GIG-Army architecture and the Army Network-Centric Data Strategy through time.

c. Functional C4/IT planning. Leveraging C4/IT strategic planning, all Army Reserve functional proponents and MSCs will submit functional C4/IT plans in support of the PPBE as described in paragraph 3-2. Functional C4/IT plans will include "as is" and "to be" views of their portfolios of data, applications, and other automation requirements. The plans will include the projects and associated resources required within the Program Objective Memorandum (POM) period to maintain desired capabilities and to achieve the "to be" state. Functional C4/IT plans will be coordinated through the Director, ESA for command approval. Approved plans will be incorporated into the Army Reserve C4/IT Strategic Plan. The ESA will assist the functional proponents in this process.

d. C4/IT investment management. The Director, ESA will use the Army Reserve C4/IT Strategic Plan and functional C4/IT plans in the C4/IT investment management process described in chapter 3, as required by the Clinger-Cohen Act and AR 25-1.

4-3. Systems architecture management

a. Systems architecture documentation. The Director, ESA will coordinate with all Army Reserve functional proponents, AIS developers, and infostructure managers to document the "as is" Army Reserve systems architecture in the Army Reserve Architecture Repository. The Director, ESA will leverage existing Army and DOD architecture repositories to prevent duplication and to detect variances in systems architecture between the Army Reserve and the Army or DOD. Where possible, the Director, ESA will provide tools that allow functional proponents and AIS developers to maintain their portions of the Repository.

b. Systems architecture planning. The goal of the Army Reserve is to bring systems architecture into conformance with DOD and Army architecture. The Director, ESA will determine the physical distribution of data and applications throughout the Army Reserve network that best supports Army Reserve mission requirements subject to resource constraints. The Director, ESA will design the networks necessary to transport data from where they are stored to where they will be processed.

c. Configuration management. The Director, ESA will direct the configuration of all equipment and software necessary to implement the Army Reserve systems and technical architectures. The Director, ESA will schedule, track, and control all changes to the Army Reserve systems configuration to mitigate risk to Army Reserve missions. The Director, ESA will publish standard workplace provisioning hardware and software configurations (desktop computers, office automation software, laptops, personal digital assistants (PDAs), etc.) that are compatible with the Army Reserve network and applications. IMOs, DOIMs, and users may attach like components conforming to Army Reserve standard configurations to the Army Reserve network upon coordination with the Director, ESA. Otherwise, no hardware or software components will be attached to the Army Reserve network until the proposed components have been granted a Certificate to Operate as described in chapter 6.

4-4. Technical architecture management

a. Technical profiles. The Director, ESA will maintain the Army Reserve Technical Reference Model (TRM), which will document the technical standards governing the allowable configurations of C4/IT assets within the Army Reserve. The Army Reserve TRM will be compliant with the Joint Technical Architecture-Army (JTA-Army). Where alternatives are allowed within the overarching guidance, the Director, ESA may choose more restrictive standards for the Army Reserve in the interests of effectiveness, costs, and supportability.

b. Security profiles. The Director, ESA will maintain information assurance standards covering such measures as public key infrastructure (PKI), encryption, electronic signature, biometric authentication, intrusion detection, firewalls, access lists, ports, protocols, virus protection, and similar issues.

c. Technology research and development. The Director, ESA will investigate new or emerging technologies, standards, and products for suitability for use within the Army Reserve. Investigation may include testing, prototyping, architecture impact analysis, and economic analysis. The Director, ESA will track industry trends and recommend changes to the Army Reserve system and technical architectures when benefits, costs, and risks justify such changes.

4-5. Data administration

a. Data stewardship. Functional proponents will assume the role of Functional Data Administrator (FDAd), as defined in DODD 8320.1, within their functional areas. They will participate in data-oriented communities of interest (COI) as designated by the Army CIO/G-6. Army Reserve data stewards will coordinate metadata definitions and data quality, access, and security requirements across all users of the data objects within their COI for the Army Reserve.

b. Data quality. Army Reserve data stewards are responsible for the quality of their data and will work with other functional proponents to maintain enterprise business processes to achieve required levels of data quality. Functional proponents will execute their portions of enterprise business processes to preserve or enhance the quality of the data objects they create or use in accordance with the rules determined by the respective data stewards. Functional proponents that have business process design responsibility will fully consider the data quality requirements of all data users in the design and improvement of the respective business processes.

c. Data analysis. As required for C4/IT planning and acquisition purposes, functional proponents will identify the data requirements of the Army Reserve. Functional proponents will assist in defining any or all of the following for inclusion in the Army Reserve Metadata Repository:

(1) The business processes in which they participate, both operations and decision support, and the information requirements of those processes.

(2) The AIS from which they obtain or into which they enter data to support their processes.

(3) Within these processes and AIS, the business data objects they create or use.

(4) The metadata associated with each business data object and business process. (Metadata includes such elements as data element name, size, type, allowable values, aggregations, transaction rules, business process rules, quality requirements, sources, uses, security constraints, longevity, and so forth.)

(5) Business requirements for data quality, including data content, accuracy, currency, and availability.

d. Metadata repository. The Director, ESA will implement an Army Reserve Metadata Repository capable of supporting data stewards in establishing standards and implementing procedures for ensuring sufficient data quality for Army Reserve mission requirements. The Repository will track the metadata for significant data objects and business processes within the Army Reserve and track their use in the AIS that support those processes. In addition, the Repository will capture metadata necessary to implement the requirements of the Army Network-Centric Data Strategy including eXtensible Markup Language (XML) tagging, authoritative data sources, enterprise identifiers, and information exchange standards. The Repository will also incorporate NCOW standard metadata (including taxonomies and ontologies) to facilitate information dissemination management (IDM). The Director, ESA will operate and maintain the Repository. Data stewards and AIS developers will maintain the content of the Metadata Repository.

e. Data architecture. The Director, ESA will document an "as is" data architecture depicting where and how data are stored; where they are used or processed; how they are moved; where duplicates are stored and how duplicates are maintained in synchronization with originals; and how data are protected from compromise, corruption, and loss. In conjunction with AIS and network design processes, the Director, ESA will coordinate a "to be" data architecture for the Army Reserve depicting the target state of Army Reserve data assets required to meet Army Reserve requirements. The Director, ESA will coordinate a transition plan for transforming Army Reserve data assets from the "as is" to the "to be" state. The Director, ESA will incorporate the data architecture and transition plan into the Army Reserve C4/IT Strategic Plan for approval by Army Reserve senior leadership. The "to be" data architecture will be brought into compliance with the GIG-Army architecture and the Army Network-Centric Data Strategy.

f. Data warehouses and data marts. The Director, ESA will coordinate a framework for the design and implementation of data warehouse structures to provide a single logical source of all Army Reserve decision support data. The architecture of the data warehouse will allow for multiple user views of the data to be tailored to individual functional specifications (data marts) without duplication of data extraction, transformation, and load (ETL) from the operational data sources. Subject to C4/IT investment approval, the Director, ESA will build, operate, and maintain the data warehouse.

g. Information assurance. The Director, ESA will define and implement such standards, procedures, training, and other measures as may be required to provide appropriate safeguards for Army Reserve data and associated infrastructure in accordance with DODI 5200.40 and AR 25-2.

h. Knowledge management. The Director, ESA will design and implement standards, policies, procedures, training, databases, collaboration tools, and like measures to support Army Knowledge Management (AKM). The Director, ESA will not duplicate but will supplement the capabilities provided by Army Knowledge On-line (AKO) and GIG Enterprise Services (GES).

i. Coordination with higher echelons. The Director, ESA will coordinate with the Army Data Management Group to ensure that the Army Reserve data administration program complies with all mandated requirements (such as the Army Network-Centric Data Strategy), to exchange metadata with higher-level repositories, and to minimize duplication of metadata and data administration efforts across the Army and DOD.

Chapter 5
Army Reserve AIS Management

5-1. General

After the acquisition and sustainment of the C4/IT infrastructure, desktop appliances, and office software, the next largest use of resources within the Army Reserve for C4/IT investments is in the realm of Army Reserve-specific application software. The cost-effectiveness of AIS investments in the Army Reserve depends heavily on avoiding duplication of functionality or data available through centrally developed solutions (either Army or DOD systems); avoiding duplication between Army Reserve solutions; and adherence to DOD, Army, and Army Reserve application and technical architectures. Duplication will be detected and resolved in the investment screening process. Application and technical architectures will be controlled through the Certificate of Networthiness and Certificate to Operate processes. Proper selection of architectures will promote cost-effectiveness by eliminating the need for duplication by enabling re-use of existing C4/IT capabilities.

5-2. Target application architecture

Adherence to the application architectures defined by the Director, ESA and compliance with the AIS development guidelines set forth below are key decision criteria in the Army Reserve C4/IT investment management process. The Army Reserve will implement an application architecture in line with DOD and Army target architectures, and all Army Reserve applications will eventually transition to this architecture.

a. The Director, ESA will specify the Army Reserve implementation of the GIG-Army architecture through the enterprise architecture process defined in chapter 4. All new and revitalized Army Reserve AIS will adhere to the specified architecture as determined in the Certificate of Networthiness and Certificate to Operate processes.

b. Webification. AKO mandates a "webified" architecture using industry standard Web browsers for user presentation. To qualify as "webified," the user must not need any software other than a browser to link to the application for the first time.

c. Integration with Army Knowledge Online (AKO). AKO will be scaled as the Army's enterprise portal. Unless exempted, all Army Reserve applications will be linked through the AKO portal and will incorporate the interfaces specified by AKO to enable a single enterprise sign-on via the portal.

d. Public key infrastructure (PKI). All Army Reserve AIS will be PKI enabled in accordance with applicable guidance.

e. AIS design. The Director, ESA will review all new AIS designs for adherence to the approved Army Reserve C4/IT Strategic Plan and enterprise architecture.

5-3. AIS development

As the Army implements the Defense Integrated Military Human Resource System (DIMHRS), SAP, and other overarching automation projects, the Army Reserve must synchronize our existing portfolio of applications with the migration of data and functions into the Army and DOD systems and out of Army Reserve systems. As a part of this effort, and in support of AKM Goal 3, the Army Reserve will make a concerted effort to consolidate and eliminate as many Army Reserve unique applications as possible. In order to manage our AIS transition effectively, the Director, ESA will establish a Center of Excellence to provide a robust application development environment and associated management processes to assist all Army Reserve AIS developers.

a. The Director, ESA will provide the following services to the Army Reserve in support of the entire application software life cycle:

(1) Build and maintain an enterprise architecture repository capable of providing effective decision support to Army Reserve leadership regarding alignment of organization structure, processes, and automation with mission performance.

(2) Build and maintain an application architecture that provides effective decision support regarding current and future states of Army Reserve applications. Guide and assist planners, designers, and implementers in determining dependencies and impacts of potential changes to the application portfolio.

(3) Build and maintain an enterprise Metadata Repository to capture the business rules and data model associated with Army Reserve business objects and processes to support use of the repository to control the specification, generation, deployment, and maintenance of application and database objects that embody Army Reserve business objects and rules.

(4) Provide a highly efficient and effective services-oriented development architecture (SODA) environment based on a model driven architecture (MDA) framework and that integrates repository, modeling, design, code generation, and deployment tools supporting a services-oriented architecture (SOA) run-time environment.

(5) Provide tools and processes capable of specifying, creating, testing, deploying, and maintaining application objects that adhere to DOD and Army specified application architecture patterns.

(6) Provide the expertise required to assist planners, business and requirements analysts, software and database designers, and implementers to achieve maximum leverage from the tools provided. Maximize the re-use of analysis, design, and implementation results from previous projects.

(7) Provide qualified individuals to serve as project managers to operate the Center of Excellence and AIS development and maintenance projects at high levels of process maturity, such as the Software Engineering Institute (SEI) Capabilities Maturity Model (CMM) at level 3 or above.

b. Both Director, ESA and functional developers will use these capabilities. In so doing, all Army Reserve AIS developers will adhere to the following guidelines:

(1) All Army Reserve AIS that are not explicitly exempted will be developed within or translated to the Army Reserve target application architecture utilizing the resources and capabilities described above.

(2) Business and requirements analysts will enter data attributes and business rules regarding Army Reserve business objects and processes into the Metadata Repository. Application and database designers will record their design decisions in the Repository. As applications are developed or modernized, their associated metadata will be captured in the Repository. Automated tools will be used to extract metadata from existing applications.

(3) As Enterprise Resource Planning (ERP) implementations and AKM consolidations are executed, multiple locally developed applications will be wholly or partially subsumed. Duplicate functionality and data will be removed from converted applications. Capabilities that can be provided by GIG Enterprise Services will use those services as they become available. Other shared processing logic and data access will be converted to Community of Interest network services in accordance with the GIG-Army architecture.

Chapter 6
Certificate to Operate

6-1. Background

Attaching unauthorized devices to Army Reserve networks or loading unauthorized software onto Army Reserve computers can compromise information security, impact network availability, and undermine other C4/IT services, degrading mission performance. Also, the addition of large numbers of previously approved devices and software without proper planning and control can overload network bandwidth and support resources. For C4/IT investment projects, obtaining an Army Reserve Certificate to Operate (CTO) is the last hurdle prior to implementation of the acquired solution. The Army Reserve CTO process supports eventual implementation of the NETCOM CTO process.

6-2. Applicability

The procedures described in this guidance are applicable to all actions by Army Reserve proponents that would—

a. Field new or revitalized DOD, Standard Army Management Information Systems (STAMIS), commercial-off-the-shelf (COTS), Government-off-the-shelf (GOTS), or locally developed devices or software to Army Reserve networks. This includes new applications that will run across Army Reserve networks, and new versions of existing devices or software that differ in architecture or network configuration from previous versions.

b. Field approved devices or software to additional sites or numbers of users beyond those specified in previously approved implementation plans.

6-3. Documentation

No unauthorized devices or software will be used on Army Reserve networks until granted an Army Reserve Certificate to Operate. Proponents requesting to add devices or software to Army Reserve networks will apply for the CTO by submitting a package including USAR Form 125-R and required attachments to their respective command Information Management Officer (IMO). Instructions for completing the form are located in paragraph F-1. Additional CTO documentation requirements include the following as applicable to the intended deployment:

a. Architecture Impact Assessment Outline as shown in appendix E.

b. Supporting documents such as the relevant System Security Authorization Agreement (SSAA), Authority to Operate (ATO), C4I Support Plan (C4ISP), acquisition artifacts, product documentation, configuration workbooks, fielding plans, and support agreements.

6-4. Testing

Devices and software will be tested to ensure compliance with Army Reserve architectures and information assurance standards. The Director, ESA will provide a testing facility equipped to emulate the standard Army Reserve operating environment. Proponents requesting CTOs will coordinate with the Enterprise Plans Office (EPO) to establish a testing plan. Proponents will provide all materials necessary to establish an appropriate test environment, either within the ESA-provided test facility or in another environment approved by ESA.

6-5. Processing

The IMOs will evaluate all requests and forward them with their comments to ESA, ATTN: Chief, Enterprise Plans Office. After analysis and testing, the Director, ESA will grant or deny each request for Certificate to Operate. Adverse actions may be appealed through command channels. The Director, ESA will publish approved and disapproved Certificates to Operate and lists of approved devices and software on the USARC Intranet Web site (https://usarcintra/cioweb/CTO.htm).

Appendix A
References

Army Regulations and DA Forms are available online from the Army Publishing Directorate (APD) web site (http://www.apd.army.mil). Department of Defense Instructions (DODIs) are available at the following web site: http://www.dtic.mil/whs/directives.

Section I
Required Publications

AR 5-1
Total Army Quality Management (Cited in paras 3-4b and 4-2d.)

AR 5-11
Management of Army Models and Simulations (Cited in para 3-6b.)

AR 5-14
Management of Contracted Advisory and Assistance Services (Cited in para 3-4i.)

AR 25–1
Army Information Management (Cited in paras 2-1c, 2-2a, 3-4b, 3-4e, and 4-2d.)
AR 25-2
Information Systems Security (Cited in paras 3-6b, 4-5g, and B-9.)

AR 25-400-2
Army Records Information Management System (ARIMS) (Cited in paras 1-4 and B-11.)

AR 70-1
Army Acquisition Policy (Cited in para 3-4a.)

AR 71-9
Materiel Requirements (Cited in para 3-4c.)

DODI 5200.40
DOD Information Technology Security Certification and Accreditation Process (DITSCAP) (Cited in paras 3-6b, 4-5g, B-9, F-1b(7)(e).)

DOD Architecture Framework (DODAF) [formerly named and shown on document as "Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework"]
(Cited in paras 3-4d, 4-1b, E-1d, and fig 3-1.)
(Available at http://www.defenselink.mil/nii/org/cio/i3/AWG_Digital_Library/pdfdocs/fw.pdf.)

Government Performance and Results Act of 1993 (Cited in para 1-5a.)
(Available at http://www.whitehouse.gov/omb/mgmt-gpra/text/gplaw2m.html.)

Information Technology Management Reform Act of 1996
P.L. 104-106, Div. E (later renamed the Clinger-Cohen Act, codified at 40 U.S. Code Chapter 25) (Cited in paras 1-1, 1-5a, and 2-2a.)
(Available at http://wwwoirm.nih.gov/itmra/itmra96.html.)

Federal Acquisition Regulation (FAR) (Cited in paras 3-4f and 3-5b.)
(Available at http://www.arnet.gov/far/loadmainre.html.)

Defense Federal Acquisition Regulations Supplement (DFARS) (Cited in paras 3-4i and 3-5b.)
(Available at http://farsite.hill.af.mil/archive/DFars/DCN19990201/Dfar1TOC.htm.)

DFAS-IN Manual 37-100-XX
Financial Management: The Army Management Structure, Fiscal Year XX (current edition) (Cited in para 3-4i.)
(Available at http://www.asafm.army.mil/secretariat/document/dfas37-100/dfas37-100.asp.)

Joint Technical Architecture-Army (JTA-Army) (Cited in paras 2-20 and 4-4a.)

Section II
Related Publications

AR 1-1
Planning, Programming, Budgeting, and Execution System

AR 5-9
Area Support Responsibilities

AR 11-2
Management Control

DOD 7000.14-R
Department of Defense Financial Management Regulations (FMRs)
Volume 2A, Chapter 3, and Volume 2B, Chapters 4 and 18

DODI 5000.2
Operation of the Defense Acquisition System

DODI 7045.7
Implementation of the Planning, Programming, and Budgeting System (PPBS)

DOD 8910.1-M
DOD Procedures for Management of Information Requirements

DODD 8320.1
DOD Data Administration

U.S. Army Forces Command (FORSCOM) Regulation 715-3 (CI)
Acquisition Instruction for the FORSCOM Central Contracting Office

Assistant Secretary of the Army (Financial Management and Comptroller) Policy
Subject: US Army Base Support Reimbursement Policy
(Available at http://www.asafm.army.mil/budget/di/dbof/dbof-pol.asp.)

DOD Net-Centric Data Strategy
(Available at http://www.afei.org/pdf/ncow/DoD_data_strategy.pdf.)

Section III
Prescribed Forms

The following forms are available on the USARC Intranet web site (https://usarcintra) and on the Army Reserve Component portion of the Army Knowledge Online (AKO) web site.
*[**Note:** PDF versions are also included at the end of this publication.]*

USARC Form 125-R
Army Reserve Certificate to Operate (Prescribed in paras 6-3 and F-1.)

USARC Form 133-R
Army Reserve C4/IT Acquisition Request (Prescribed in para F-2.)

USARC Form 139-R
Army Reserve C4/IT Investment Assessment Score Sheet (Prescribed in para 3-4f and para F-3.)

Section IV
Referenced Forms

DA Form 2028
Recommended Changes to Publications and Blank Forms

Appendix B
Critical Management Controls for Information Management in the Army Reserve

B-1. Have all C4/IT requirements been validated prior to commitment of funds?

B-2. Have all expenditures for C4/IT been collected by investment project and reported to the Director, ESA at least on an annual basis?

B-3. Does the Director, ESA maintain a comprehensive portfolio of Army Reserve C4/IT investments ranked by benefits, costs, and risks?

B-4. Is a C4/IT investment decision package on file with the Director, ESA for all active and proposed major investments?

B-5. Has the Director, ESA evaluated all active investments on at least an annual basis and made recommendations to continue, modify, or terminate each investment?

B-6. Have all C4/IT acquisitions been approved by the Director, ESA?

B-7. Are all Army Reserve C4/IT capital acquisition projects exceeding 60 days in duration documented with a program management plan, a project plan, a risk management plan, and a quality control and testing plan and are C4/IT projects being actively managed against these plans as evidenced by appropriate work papers or records?

B-8. Does the Director, ESA maintain an Army Reserve C4/IT Strategic Plan and staff it at least once every 2 years?

B-9. Have all fielded or operated automated systems that contain or process sensitive but unclassified (SBU) or classified data been certified and accredited in accordance with DODI 5200.40 and AR 25-2?

B-10. Is any unauthorized equipment or software being operated on Army Reserve networks?

B-11. Are C4/IT investment management records maintained in accordance with AR 25-400-2 regulation and USAR Regulation 25-3?

B-12. Are known C4/IT investment management issues and material weaknesses addressed in the command Annual Statement of Assurance?

Appendix C
Investment Management Process Flow

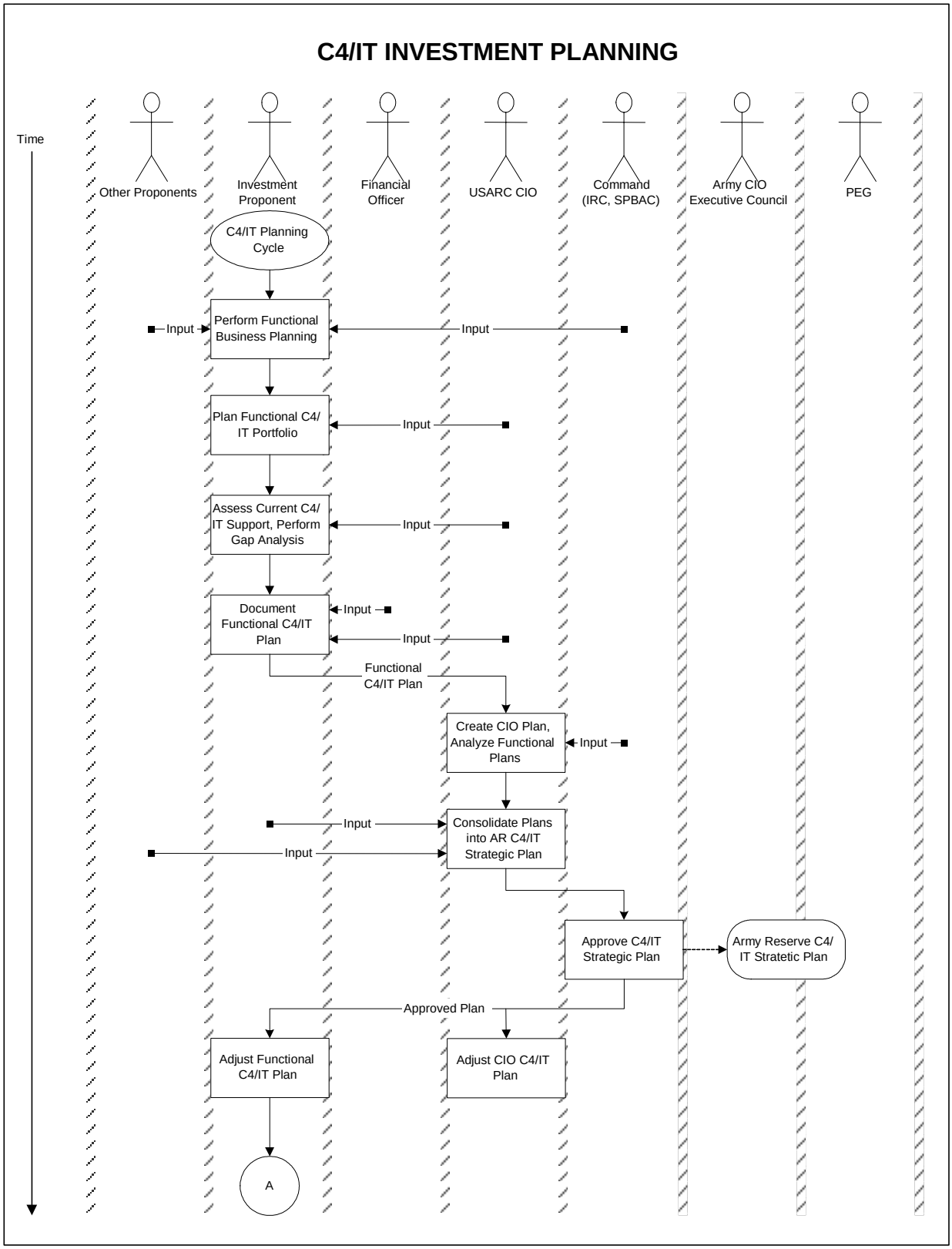

Figure C-1: C4/IT investment planning

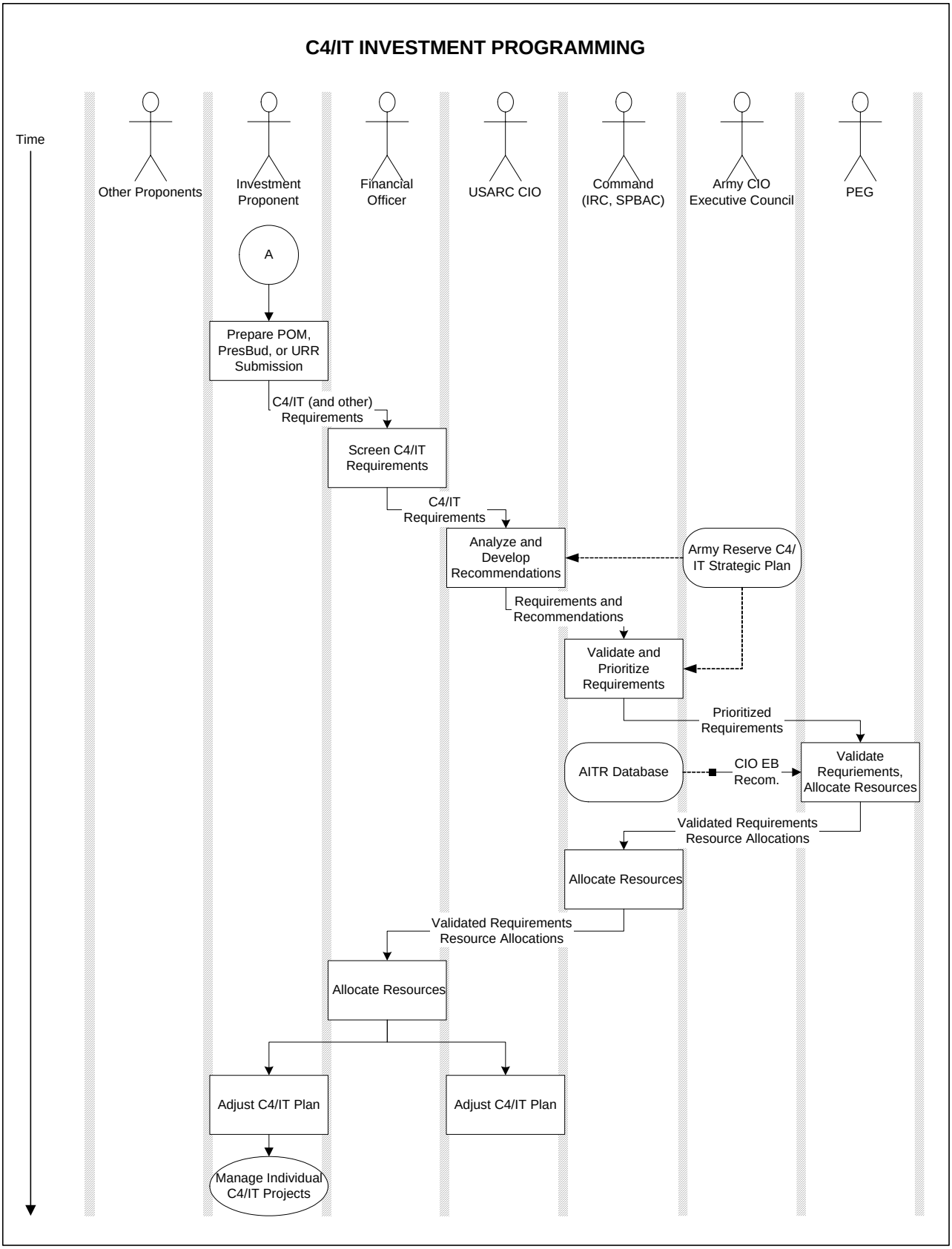

Figure C-2: C4/IT investment programming

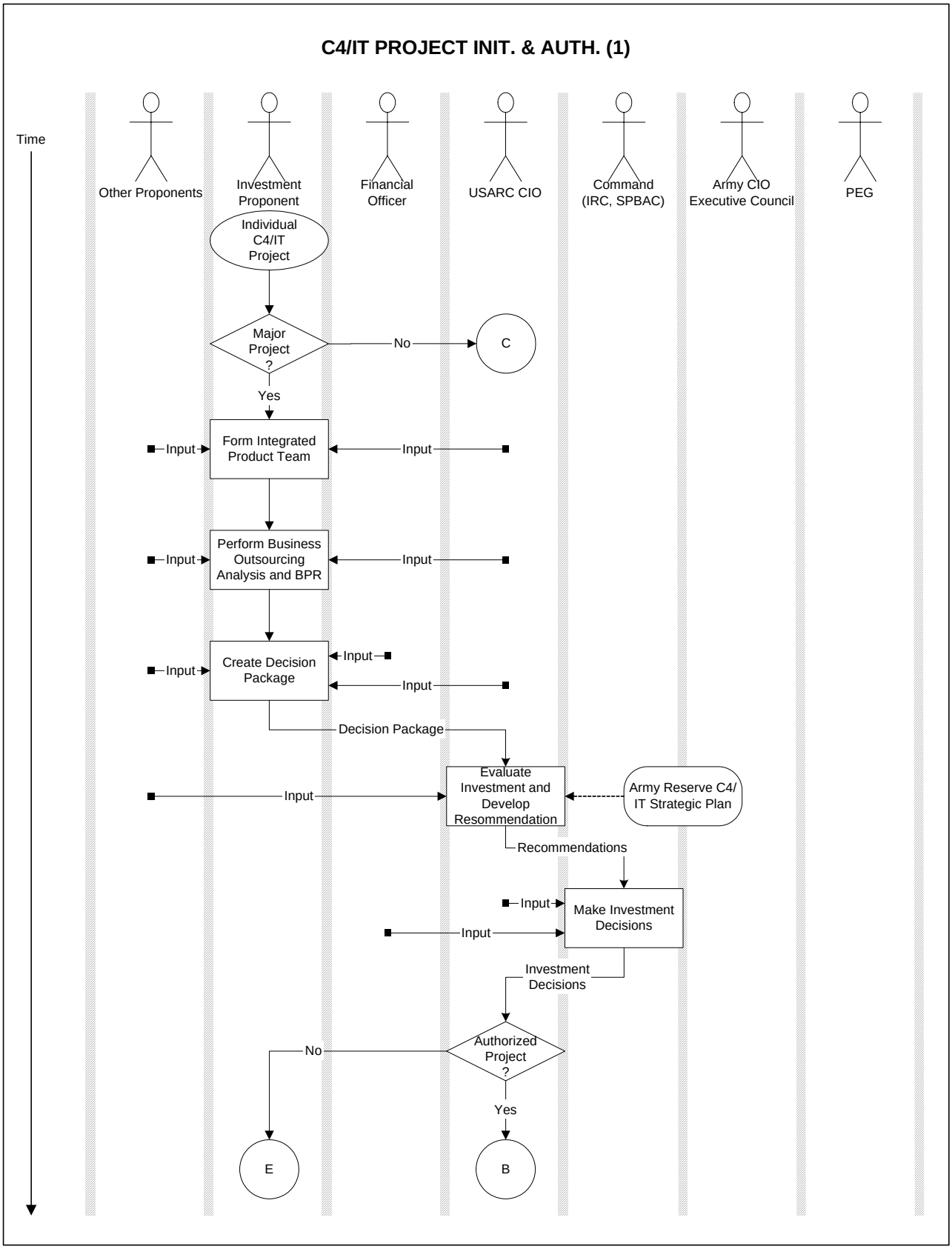

Figure C-3: C4/IT project initiation and authorization (1)

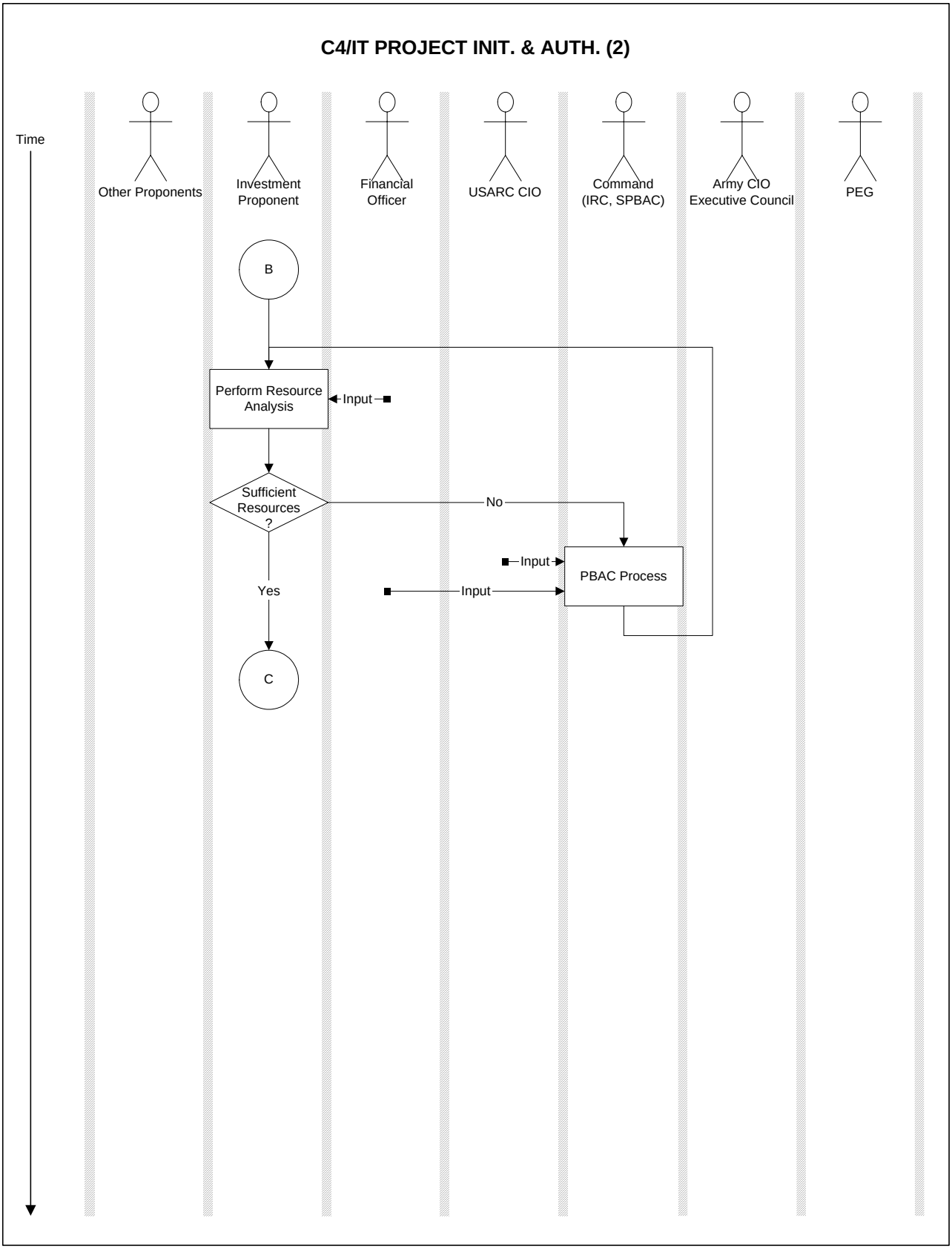

Figure C-4: C4/IT initiation and authorization (2)

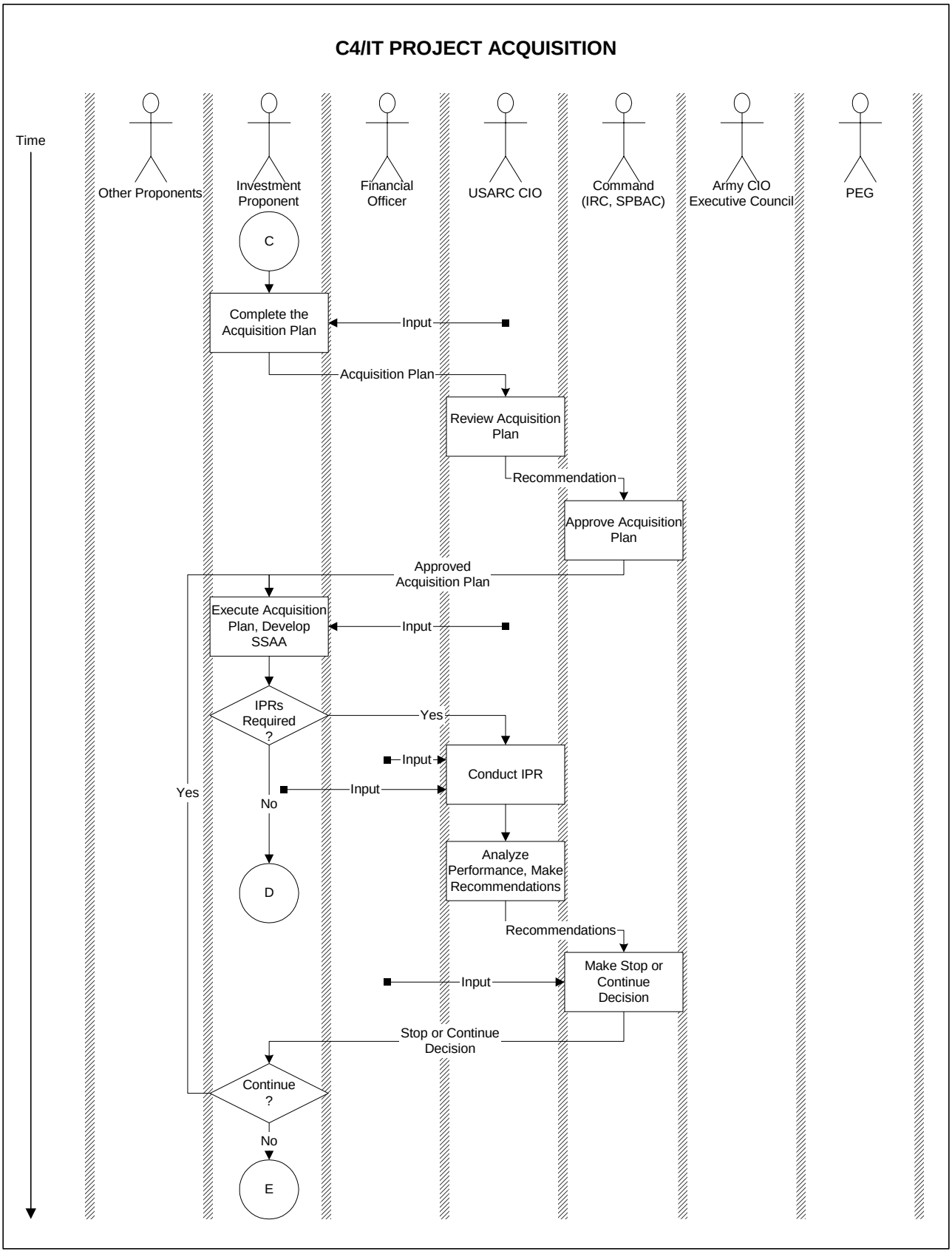

Figure C-5: C4/IT project acquisition

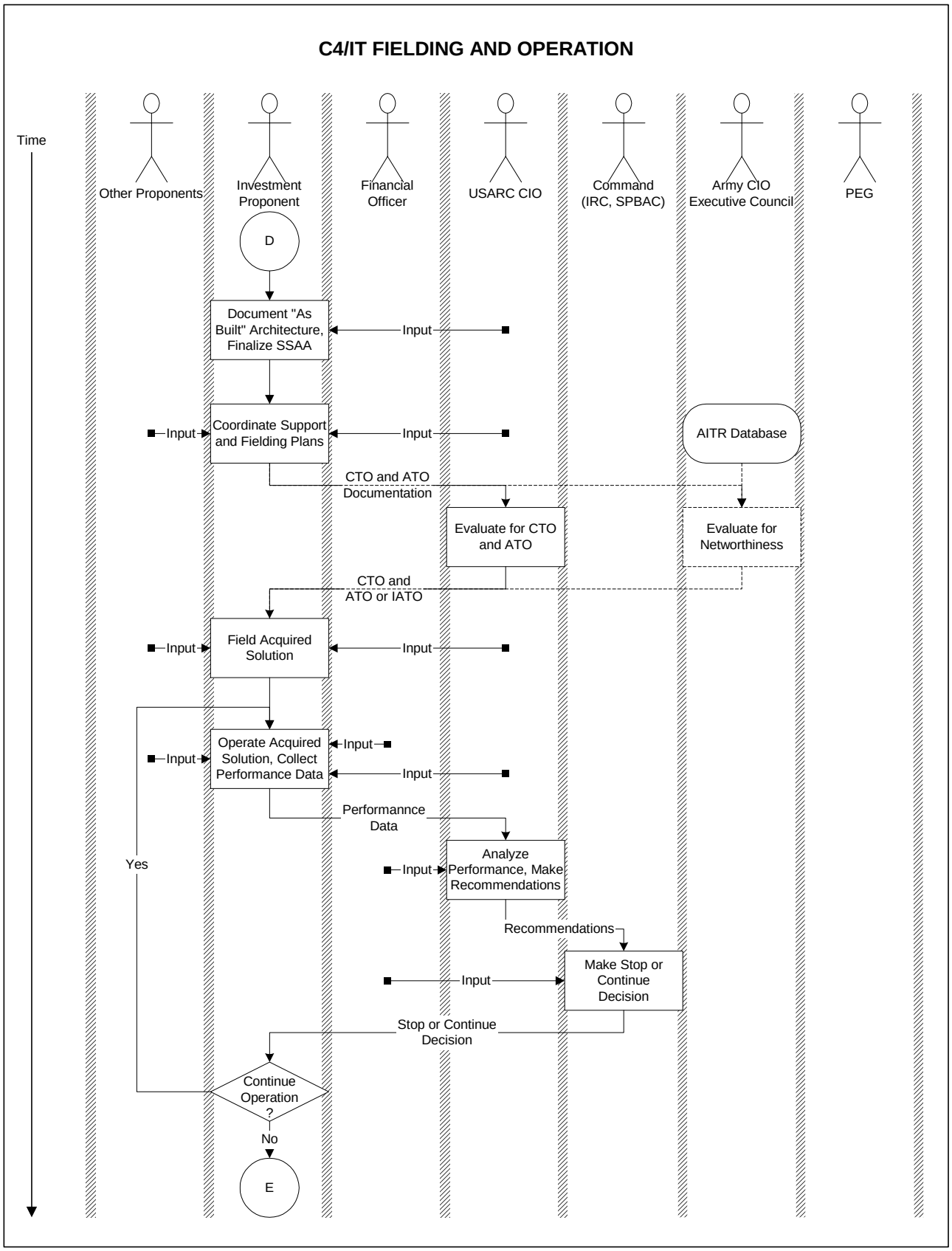

Figure C-6: C4/IT fielding and operation

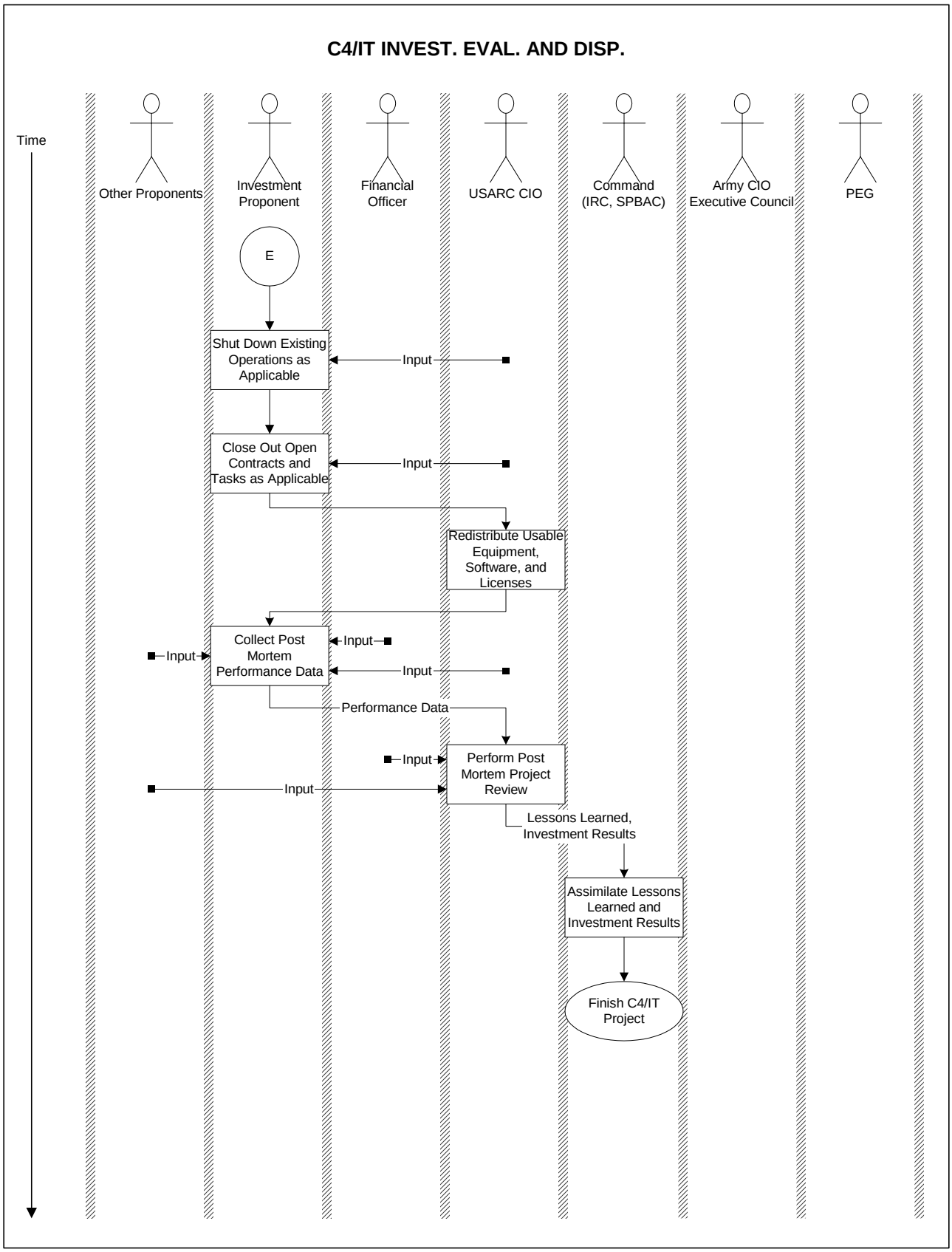

Figure C-7: C4/IT investment evaluation and disposal

Appendix D
C4/IT Investment Decision Package Outline

1.0 Purpose. State the purpose of the investment. Identify the investment and the functional proponent.

2.0 Background. Provide information that describes the present situation and/or present architecture.

3.0 Mission Needs Statement Summary.

3.1 Business Problem Assessment. Provide clear statement of the business problem to be solved in functional business terms. Identify the business process(es) that will be improved by the C4/IT investment. Tie the business process improvements to improvements in mission performance, both measurable and non-measurable.

3.2 Mandates and Drivers. List legislative, regulatory, or other mandates that will be satisfied by this investment. Define the Critical Time Drivers—activities that must be finished or opportunities that will be lost by a certain date; and the Critical Event Drivers—important events that cannot proceed until some action has taken place.

4.0 Acquisition Strategy. Describe the solution alternatives considered (nonmaterial, material) and the selected solution strategy. Identify the acquisition phases requested (business process reengineering/business process redesign (BPR), requirements definition, design, construction, implementation and turnover, or sustainment). Indicate how the required functionality will be acquired.

5.0 Architecture Impact Analysis. Use the outline and configuration spreadsheet documented in appendix E.

6.0 Financial Plan. Set out the resource plan for the investment, listing by fiscal year the capital requirements separate from the operations and maintenance requirements. Begin with the current year of execution and go out to the expected useful life of the investment.

7.0 Selection Criteria.

7.1 Standardized Return on Investment (ROI) Criteria. Propose how the ROI should be measured once the investment is implemented. Provide estimates of benefits and costs through time and calculate an estimated ROI.

7.2 Alignment with Army Knowledge Management (AKM). Indicate how the investment supports the AKM Goals.

7.3 Assessment Score Sheet. Complete and attach the C4/IT Investment Assessment Score Sheet, USAR Form 139-R.

Figure D-1. Sample format for C4/IT investment decision package outline

Appendix E
Architecture Impact Assessment Outline

E-1. The format for the Architecture Impact Assessment Outline is at figure E-1. Proponents should submit all materials in one package, preferably electronically. Brevity and economy of effort should be stressed, subject to the information requirements of the Director, ESA to make an informed decision regarding the architectural and organizational impacts of each project. This outline overlaps considerably with other documentation that may be developed during the course of a C4/IT project. When existing documents address the required information, proponents should simply provide a copy of the external documents and insert appropriate references into this outline; for instance, "See SSAA for ARNet, Section 3.0." Typical sources of data for this outline include the following:

a. The DITSCAP System Security Authorization Agreement (SSAA). The SSAA includes a great deal of the information required for the impact assessment. If an SSAA exists for the system of which this project will become a part, then that SSAA should be updated to reflect the impact of this project. The updated SSAA then can be used as an effective source of data for this outline.

b. Acquisition-related documentation. During the course of development, the program manager (PM) for a project may have produced a mission needs statement (MNS); a requirements document (operational requirements document (ORD), initial capabilities document (ICD), or Capstone requirements document (CRD)); system designs; fielding plans; or other artifacts that address one of more areas of concern here.

c. C4/IT investment management documentation. An investment management decision package may include acquisition documentation, business case analysis, financial justifications, operational concepts, architecture concepts, business process analysis, or other useful information. If this outline is a part of a C4/IT decision package, you need not duplicate other decision package information in the architecture impact assessment.

d. DOD Architecture Framework (DODAF) documentation. Major projects at the Army or DOD level are documented according to a defined set of artifacts, or in the Core Architecture Data Model (CADM) database format. This information may be available from the PM. Refer to the following web site for additional information on the DODAF (C4ISR Architecture Framework): http://www.defenselink.mil/c3i/org/cio/i3/AWG_Digital_Library/

e. COTS product literature and specification sheets. Typically, COTS end-user devices and software come with user manuals, marketing literature, specification sheets, and other items that help identify the technical details associated with the products.

E-2. Not all of the sections in figure E-1 will be applicable to all projects, and for a given project, some sections will require more detail that others. Proponents should coordinate closely with the Director, ESA to determine the specific requirements for their projects.

E-3. The Architecture Impact Assessment Outline and the Configuration Workbook (fig E-1, item 4.0) are available on the ESA CTO Intranet web page at https://usarcintra/cioweb/CTO.htm.

1.0 Background

This section should name the project and identify the project proponent. In this section, proponents will identify the systems, hardware, software, and capabilities that will be implemented and the intended users and mission purpose of the project. Information may include system criticality and classification of data processed or stored, and the operational environment of the system.

Sources of data for this section include SSAA Sections 1 and 2, acquisitions documents, investment management documents, and DODAF document AV-1.

2.0 Operational Concept

Proponents will describe the life cycle operation of the capabilities to be put in place by their projects. Proponents should use graphics and narrative to outline normal operations including location of work, major manual and automated processes, and information flows. Information may include organizations, missions, geographical configurations, and communication paths.

Sources of data for this section include the SSAA section 1.4 and Appendix D, acquisitions documents, investment management documents, and DODAF documents OV-1, OV-2, OV-3, and OV-5.

3.0 System Layout

Proponents will describe the placement of processing nodes, data stores, communications links, and paths of system interfaces. Appropriate graphics should be included to convey logical and physical layouts necessary to identify additional network or facility capabilities or capacities. For instance, improvements to a local area network (LAN) might be identified schematically through overlays on a building line diagram. Maps may be useful for wide area network documentation. Information may include information exchange, logical and physical data models, system interfaces, and logical and physical communication configurations (such as LANs, WANs, physical nodes, and their layouts).

Sources of data for this section include the SSAA section 3 and DODAF documents OV-2, OV-3, OV-7, SV-1, SV-2, SV-3, and SV-11.

4.0 Configuration Workbook

Proponents will document the numbers, locations, and configurations of all equipment, software, and data stores to be put in place by their projects. In addition, proponents will document estimates of network message loads between major sources and destinations of data within the updated system. The ESA has developed a sample workbook that proponents may use to document this information. The workbook contains separate worksheets for the hardware and software configurations, data stores, operating locations, and network message loads.

Sources of data for this section include the SSAA Section 2, detailed system design documents from the PM, COTS product documentation, and DODAF documents SV-1, SV-2, and SV-11.

5.0 Configuration Control Policies

Proponents will document the policies that will govern the management of changes to hardware, software, and network configurations associated with their projects. At a minimum, proponents will identify all critical configuration components and indicate who has the authority to grant requests to modify each configuration, and who will be responsible for implementing approved requests. These policies will be fully coordinated with all affected parties.

Configuration control policies may refer to external agreements such as service level agreements (SLAs) or Memorandums of Agreement (MOAs).

Figure E-1. Format for Architecture Impact Assessment Outline

6.0 Support Plan

Proponents will fully coordinate a full life cycle support plan for the C4/IT capabilities that their projects will put in place. At a minimum, support plans will address the service levels, manpower requirements, locations, and responsible offices for each of the following services:

Operations (server operations, system administration, database backup/restore, database administration, network operations, network administration)
Helpdesk (telephone support, desk-side assistance)
Helpdesk escalation procedures
Hardware maintenance and support
System software maintenance and support
Application maintenance and support

The support plan may refer to a service level agreement (SLA) or memorandum of agreement (MOA) signed by all of the affected parties. Maximum leverage should be made of existing SLAs and MOAs. External assistance plans, such as vendor maintenance and support plans, should be summarized briefly.

7.0 Fielding Plan

Proponents will fully coordinate their fielding plans through the Director, ESA, the USARC IMO, and all affected field IMOs. The USARC IMO will assist in coordinating plans with the field IMOs. Proponents will complete staffing with sufficient lead-time to secure the implementation resources that are required from the field and to allow controlled changes to data center and wide area network configurations. Proponents may render fielding plans in word processing, spreadsheet, or project management tools. At a minimum, fielding plans will identify tasks, manpower requirements, locations, timeframes, and responsible offices for all major activities and critical events. Areas of concern include field-testing, pilot implementations, training, and other work interruptions for end-users.

Fielding plans may refer to external agreements such as SLAs or MOAs.

8.0 Technical Reference Model

Proponents will coordinate their architectural designs with the Director, ESA to determine what changes or exceptions are required to Army Reserve C4/IT standards. Proponents will justify all changes and exceptions with technical, financial, and mission impacts. Proponents will identify future technology trends and emerging standards against which their project will track through its life cycle.

Sources of data for this section include investment management documents, system design documents, and the DODAF documents TV-1 and TV-2.

Figure E-1. Format for Architecture Impact Assessment Outline—Continued

Appendix F
Prescribed Forms and Instructions

F-1. USAR Form 125-R (Army Reserve Certificate to Operate)

a. USAR Form 125-R is a multipurpose form. As an origination document, proponents will complete this form to request a Certificate to Operate for a designated system, devices, or software. The form also serves as a cover sheet for any attachments that are submitted with it and for comments from various reviewers of the request that may accumulate during processing. During processing, the form acts as a routing sheet and a record of recommendations from various sections that must review the request. Finally, the form serves as a permanent record of the action taken by the Director, ESA on the request.

b. Instructions.

(1) **System Name.** Provide a unique descriptive identifier for the system or other items you wish to add to Army Reserve networks. Typically, DOD or STAMI systems have already been named and have an approved acronym. The acronym is sufficient if it uniquely identifies the system. Otherwise, please qualify the name in some way. If the request is for COTS or locally developed software, provide a similar identifier. Alternatively, proponents may wish to provide a project name in this field.

(2) **Date Submitted.** FormFlow will automatically provide the current date in this field when filling the form electronically. If you require, you may enter a different date. When filling in a printed form, simply provide the appropriate date.

(3) **Army Reserve Proponent.** Indicate the agency or official within the Army Reserve that will direct the use of the items under request. For instance, a system distributed by the Army to support Staff Judge Advocate personnel would fall under the USARC Staff Judge Advocate. Similarly, a logistics system would fall under the USARC DCS, G-4. Unless the Army Reserve Proponent makes prior arrangements with the Director, ESA, the Army Reserve Proponent is responsible for providing all support to Army Reserve users of the system.

(4) **System Owner.** Enter the proponent agency for the system that is responsible for system development and sustainment. For COTS products, this is the vendor. For DOD and STAMI systems, this is usually a DOD or Army staff agency, respectively. For instance, the system owner for RIDES-E is the Surgeon General of the Army. For systems developed locally, this is normally the respective functional staff agency at the command that developed the system. For example, the system owner for ARSAMS is the USARC DCS, G-4. Unless the Army Reserve Proponent makes prior arrangements with the Director, ESA, the System Owner is the Army Reserve Proponent's sole source of system development and sustainment services.

(5) **POC.** Provide the name of the individual who will answer questions from ESA regarding the request.

(6) **System includes.** Check all of the boxes that apply to the system for which you are submitting this request.

(a) ***Hardware.*** Check this box when any physical devices will be provided as part of the solution.

(b) ***System software.*** This item pertains to operating systems, utilities, compilers, device drivers, and other software that supports the application environment but does not provide business functionality.

(c) ***Application.*** If the solution includes a separate program or module that provides business functionality, check this box.

(d) ***Office automation scripts.*** Some "applications" are really just document templates with embedded macros and such. Check this box as appropriate.

(e) ***Other.*** List any items not adequately described by the other boxes.

(7) **Attachments.** Indicate the documentation you are submitting that describes the system and how it will be fielded and supported. The following items should be provided as applicable:

(a) ***C4/IT investment decision package.*** When a significant Army Reserve investment in C4/IT is anticipated, the Army Reserve proponent must submit a justification package to the Army Reserve Investment Review Council. (See sample format at fig D-1.)

(b) ***Architecture impact assessment.*** This document describes the architecture of any C4/IT project and estimates the impact on operational, system, and technical architecture, and on other C4/IT projects. The assessment also indicates system support strategies and information assurance plans.

(c) ***Implementation plan or operations order.*** All significant implementation efforts should have a fully coordinated implementation plan before application is made for a Certificate to Operate. Unless prior arrangements have been made with the Director, ESA, system implementation is the responsibility of the proponent.

(d) ***Operations support plan or C4ISP.*** Responsibility for all helpdesk, database management, and other operational services required to use a system should be fully coordinated and documented before application is made for a Certificate to Operate. Unless prior arrangements have been made with the Director, ESA, all operational support requirements are the responsibility of the proponent.

(e) ***DITSCAP SSAA.*** All systems and networks must be certified in accordance with DODI 5200.40. This certification should be accomplished during acquisition. For systems subject to DODI 5200.40, or parts of such systems, attach a copy of the System Security Authorization Agreement (SSAA).

(f) ***Other.*** Indicate nature of other attachments.

(8) **Hardware, software, data, and documentation provided to ESA for examination**. Under most circumstances, ESA will need a sample or copy of all items that are part of the request. The items will be "fielded" in a test lab to determine compatibility and network impacts. List the items submitted for testing or examination.

(9) **Reviewed by Command IMO.** This field is to be filled in by the proponent's respective IMO to indicate that the IMO has reviewed the proposal and has had opportunity to provide comments. Proponents should leave this field blank and allow the IMO to provide a POC. All POCs who review the request will be allowed to attach their recommendations and other comments as it goes through the staffing process. The IMO will check the "Comments attached" box to indicate that a comment sheet has been attached.

(10) **Reviews completed by ESA.** This section will be filled out by the sections within ESA that evaluate the request. In accordance with standard staffing practice, if any reviewer has issues with the request, every reasonable attempt will be made to resolve the issues with the proponent before final decision. The reviewer will check the "Comments attached" box if a comment sheet is attached.

(11) **Certificate to operate within Army Reserve networks is – *(Granted…Denied)***. An official within the ESA will grant or deny the Certificate to Operate for a period of time indicated. Any restrictions imposed on the use of an item will be noted. If the decision is made to deny the request after attempts at resolution, the reasons for denial will be given.

(12) **Signature block.** The official making final determination on the request will fill in this section.

(13) **Date of issue.** If the request for Certificate to Operate is granted, this date will govern the maximum time span over which the system may be operated before the certificate must be revalidated. Otherwise, this field simply indicates the date upon which the request was closed.

F-2. USAR Form 133-R (Army Reserve C4/IT Acquisition Request)

a. The purpose of this form is to provide a standard, easily understood vehicle for Army Reserve proponents to submit requests for C4/IT acquisitions.

b. Instructions.

(1) **Date Requested.** Self-explanatory.

(2) **Date Received.** For ESA use only.

(3) **Tracking Number.** For ESA use only.

(4) **Originator:** Indicate the person in the staff element requesting the procurement or the designated staff automation point of contact.

(5) **Org/Directorate.** Indicate the command and staff element making the request.

(6) **Estimated total acquisition value.** Estimate the total life cycle cost of the acquisition. If this is part of a larger project, the financial plan for the entire project should be reflected in the C4/IT investment decision package (see item 16 below).

(7) **ESA acquisition.** Check this box if the acquisition is to be funded by centrally managed C4/IT funds.

(8) **Local acquisition.** Check this box if the acquisition is to be funded by distributed C4/IT funds or with mission funds.

(9) **MDEP.** For locally funded acquisitions, enter the Management Decision Package (MDEP) from which resources will be used.

(10) **APE.** For locally funded acquisitions, enter the Army Program Element (APE) that will be used.

(11) **AKM waiver attached.** If the acquisition will be funded by a MDEP or APE that is not recognized by the Army CIO/G-6 for C4/IT spending, an AKM waiver is required, in which case, check this box. If a waiver has previously been submitted, attach the response. Otherwise, attach the waiver request. Note: Processing the acquisition requests will be delayed until the waiver is approved.

(12) **Description of items or services to be acquired.** Indicate the items that are being requested. The ESA will determine products and detailed configurations to be acquired unless project requirements dictate otherwise. Product selections and configurations provided by proponents are subject to revision by ESA for completeness, workability, network supportability, information assurance, and architecture compatibility subject to project requirements.

(13) **Product specifications attached.** Check this box if there are attached requirements statements or other product information that will assist ESA in selecting products meeting your requirements.

(14) **Statement of work attached.** Check this box and attach the statement of work if this acquisition requires the acquisition of services.

(15) **Business justification.** If this acquisition is not part of a "major C4/IT investment project," then provide the business justification in the space provided. If the space provided is insufficient, make an entry in the "Other attachments – Other" block (see para F-2b(18)(b), below) and attach additional information.

(16) **C4/IT investment decision package attached.** If this acquisition pertains to a "major C4/IT investment project," unless previously provided to the Director, ESA, check this box and provide a C4/IT investment decision package in accordance with chapter 3, figure D-1, and appendix E.

(17) **RSAIN.** All requirements should have an assigned Requirement Statement Audit Identification Number (RSAIN), see appendix G. If this acquisition pertains to a previously validated requirement, provide the RSAIN under which it was previously submitted. Otherwise, assign a new, unique RSAIN.

(18) Other attachments.

(a) ***Acquisition strategy and plan.*** Unless previously provided, check this box and attach the acquisition strategy memorandum and any acquisition planning information required by the contracting officer.

(b) ***Other.*** Check this box and list any additional attachments to the request if applicable.

(19) **Signature of requesting authority.** The proponent staff director, chief of staff, or commander must sign the request.

(20) Reviews and Approval/Disapproval. For ESA use only.

F-3. USAR Form 139-R (Army Reserve C4/IT Investment Assessment Score Sheet)

Proponents will complete the C4/IT Investment Assessment Score Sheet to provide a means of ranking investments against each other. The Score Sheet also serves as a planning checklist, suggesting to proponents the types of actions they should take to maximize the value and minimize the risk of any C4/IT investment. Individual items on the Score Sheet are scored on their own criteria and multiplied by a weighting factor to arrive at an adjusted score for that item. The total score is the sum of the adjusted item scores. The Score Sheet produces a total adjusted score of between 0 and 100 points, with 100 being the best score possible. Bear in mind that a "perfect" score does not guarantee a successful investment, but it does indicate that everything has been done to improve the chances.

a. The Score Sheet is divided into three basic sections.

(1) The first section deals with preparation for automation and project planning. All of these factors are under the investment proponent's control and the proponent should use this section to drive preparation and planning actions that maximize this score.

(2) The second section deals with various types of risks that can affect a C4/IT investment. In this section, a *low* score equates to a *high probability* of an adverse event occurring and a *high negative impact* if such an event occurs. While the proponent may not be able to control all external factors that could impact the investment, the proponent can use this section of the Score Sheet to determine critical risk areas to which risk mitigation strategies should be applied. The risk scores should be reassessed after applying the mitigation strategies to achieve the best score given the risks involved. The risk factors listed will be sufficient for most Army Reserve C4/IT projects. If the investment is subject to additional risk factors based on the DOD Risk Management Framework, or any other relevant risk criteria, attach a separate sheet (or an electronic spreadsheet) listing the additional risk factors to be included, and score them according to the rating scheme found here. This additional information will be made available to the investment authorizing body to aid in ranking this investment.

(3) The third section evaluates the strength of the overall business case for the investment. Generally speaking, a low score in this section indicates an investment that, while it may have a good chance of success, will not produce much in the way of tangible mission results.

b. Instructions.

(1) **Investment Name.** Self-explanatory.

(2) **Assessment Date.** Self-explanatory.

(3) **Section I – Preparation for Automation and Project Planning.** Rate each item in this section according to the rating scheme provided and place the rating in the Project Scoring column. The form will compute the Adjusted Score.

(4) **Section II – Risk Assessment.** Rate each item in this section from 0 (high probability and high impact) to 4 (low probability and little or no impact) by adding together a score of 0-2 for risk (probability) and a score of 0-2 for impact. Place the rating in the Risk Score column. The form will compute the Adjusted Score.

(5) **Section III – Overall Business Case.** Score each item according to the rating scheme provided and place the score in the Project Scoring column. The form will compute the Adjusted Score.

Appendix G
Requirements Statements and Audit Identification Numbers

G-1. Requirements

A requirement is an unmet need or capability that affects an organization's ability to accomplish its mission. Each requirement is expressed in functional terms. Generic hardware, software, and training descriptions are used to estimate quantity requirements and life cycle costs. The method of meeting the requirement should comply with the guidance, standards, goals, objectives and strategies of the Army and the Army Reserve. The requirement must not be fragmented to circumvent expense/investment criteria or to change the type of funding.

G-2. Requirement Statements

a. A Requirement Statement (RS) is a synopsis of the business requirement with supporting mission impact and financial documentation. The format of an RS is provided by the Chief Financial Management Officer (CFMO) in support of the PPBE process into which it is submitted. Accordingly, each RS will be resourced within a single Management Decision Package (MDEP) and Army Program Element (APE) code. Within the MDEP/APE, requirements that are not related to a specific major C4/IT investment project (see para 3-4) but address a generic C4/IT capability (such as copier provisioning and life cycle replacement) should be grouped together into a single RS, except as when divided by Army Reserve Region (see para 2–4c) or mission category (below).

b. Requirements are evaluated in part on mission category criteria. Only one mission category will appear on an RS. The categories are:

(1) ***Mission Critical*** -- Requirements that are absolutely fundamental to mission performance. Include in this category those requirements that are mandated by higher authority; e.g., requirements that directly support a program directed by the Executive Office, Congress, OMB, OSD, HQDA, Army Reserve, or USARC.

(2) ***Mission Essential*** -- Requirements that are necessary for optimum mission performance; e.g., life cycle replacement.

(3) ***Mission Desirable*** -- Requirements that measurably enhance mission performance.

G-3. Requirement Statement Audit Identification Numbers

Use the Requirement Statement Audit ID Number (RSAIN) to track Requirement Statements, out-of-cycle requests, and other documentation pertaining to the planning, approval, and procurement of C4/IT assets. The RSAIN consists of the following:

a. The designation "ARC" (Accounting Requirements Code);
b. The current two-digit budget year;
c. The RSAIN category (as indicated below);
d. The unit identification (ID); and
e. A sequence/control number assigned by the Command or directorate.

[For example, to identify a requirement for a facsimile machine during budget year 2004, select the RSAIN ARC04014, followed by the unit ID and a sequence number. Facsimile equipment is in RSAIN Category 014.]

G-4. RSAIN Categories

a. ***RSAIN 001 – Office Automation (OA).*** Use this RSAIN to address requirements for and track automated data processing equipment (ADPE) that supports desktop technology, multifunction workstations, and associated peripherals which enable an individual to perform independent, stand-alone processing of such functions as office data processing, graphics, PC video/facsimile, word-processing, database management, spreadsheets and electronic mail.

b. ***RSAIN 002 – Office Local Area Network (OLAN).*** An office LAN operates solely within a building or isolated complex of buildings to interconnect the occupants of that building or complex. This RSAIN also provides for the interface for connecting functional OLANs to an installation or functional backbone LAN.

c. ***RSAIN 003 - Non-Tactical Trunked Radio and Base Support Radio (NTTR&BSR).*** Use this RSAIN to address requirements for base support radio equipment, including cellular phones, fixed base or mobile radio systems (including those unique to intelligence activities), repeaters, multiplexers, antennas, pagers and associated plant and distribution systems in support of administrative networks. Also use this RSAIN to upgrade or replace multiple netted systems with Non-Tactical Trunked Radio systems or equivalent technology. These systems are used by utilities, transportation, emergency services, security/guard forces, medical services and range control.

d. ***RSAIN 004 - Telecommunications Life Cycle Management (TELCOMLCM).*** Use this RSAIN to upgrade switch software, perform minor equipment upgrades, and add lines and trunks to an existing plant. Use this RSAIN to upgrade/replace cable that cannot wait for construction programs/projects.

e. ***RSAIN 005 - Installation Local Area Network (ILAN).*** An installation LAN operates between facilities, complexes, and organizations that are physically separated (not in the same building or local complex). Use this RSAIN to create, expand, or upgrade an installation or power projection platform LAN. Also use this RSAIN to connect OLANs to backbone ILANs and to create a delta between OLANs and PPC4I programs.

f. ***RSAIN 006 - Integrated Services Digital Network (ISDN).*** Use this RSAIN to replace or upgrade telephone switches to ISDN or latest technology, to provide expanded capability in voice, data, and video information exchange.

g. ***RSAIN 007 - Defense Message System Lifecycle Management (DMS).*** The centrally managed DMS program identified a limited distribution with the balance of the program designated as the end-user responsibility. Use this RSAIN for user supplemental support of the program and to make office automation systems compliant with the DMS.

h. ***RSAIN 008 - Standard Systems Lifecycle Management (SSLM).*** Use this RSAIN to address initial procurement and life cycle maintenance of equipment and software required to operate Standard Army Management Information Systems (STAMIS) and DOD systems. Document each STAMIS and DOD system on a separate RS.

i. ***RSAIN 009 - Information Systems Security (ISS).*** Use this RSAIN to address requirements for the procurement or LCM of equipment or software that manages or creates a secure environment for interactive (voice, data, facsimile, video) information processing. This RSAIN includes Secure Telephone Units III (STU-III), secure facsimiles, multilevel security devices, ANDVTs/MINITERS, and INFOSEC devices (cipher locks, shredders, etc.).

j. ***RSAIN 010 - DPI Centric OSE (OSE).*** Use this RSAIN to address requirements for new technology and servers to modernize Installation Centric minicomputers and Command Data Base servers through LCM.

k. ***RSAIN 011 - Mission Support Information Technology (MSIT).*** Use this RSAIN to address requirements for IMA equipment and software to support mission requirements, including training, mobilization and non-STAMIS programs directed by USARC or higher authority (e.g., Crisis Action Teams, Counter-Drug Operations, Center Level Applications System (CLAS), etc.). This equipment must appear on a TOE, TDA, or supplement to a TDA. Use this RSAIN in a separate RS to address requirements to provide critical information services to Emergency Operations Centers (EOC), mobilization

planners, and other staffs directly involved in crisis management. In addition to computers and software, these services include providing connectivity to gateways to other DOD/government networks (e.g., FEMA).

l. ***RSAIN 012 - Office Copiers (OC).*** Use this RSAIN to address requirements for office copiers and printing and duplicating equipment.

m. ***RSAIN 013 - Records Management (RM).*** Use this RSAIN to address requirements for RM equipment and software, including filing equipment and microfiche.

n. ***RSAIN 0014 - Facsimile Equipment (FAX).*** Use this RSAIN to address requirements for unsecured, stand-alone facsimile equipment.

o. ***RSAIN 015 - Visual Information (VI).*** All VI requirements are included in this RSAIN.

p. ***RSAIN 016- Postage Metering System (PMS).*** All postal equipment or postal-related equipment is included in this RSAIN.

Glossary

Section I
Abbreviations

ADPE
automated data processing equipment

CAR
Chief, Army Reserve

COR
contracting officer's representative

DCS
Deputy Chief of Staff

DOD
Department of Defense

DFARS
Defense Federal Acquisition Regulations Supplement

FAR
Federal Acquisition Regulation

LCM
life cycle management

MOA
Memorandum of Agreement

MSC
major subordinate command

O&M
operations and maintenance

OCAR
Office of the Chief, Army Reserve

OMB
Office of Management and Budget

PM
program (or project) manager

POM
program objective memorandum

RCS
requirement control symbol

Section II
Terms

Chief, Army Reserve (CAR)
The individual charged under Title 10 of the U.S. Code with executing all funds appropriated for the Army Reserve. The CAR serves as an advisor to the Army Chief of Staff regarding Reserve matters. The CAR also serves as the Commanding General of the U.S. Army Reserve Command and as the Deputy Commander of Forces Command (FORSCOM) for Reserve Affairs.

Contracting officer's representative (COR)
An individual warranted to represent the contracting officer in dealings with vendors to perform limited functions, such as monitoring the performance of contractors and quality of deliverables. (The COR is not authorized to commit, indebt, or otherwise obligate the Government. This authority resides with the contracting officer.)

Deputy Chief of Staff (DCS)
A military staff officer overseeing a functional directorate reporting to the Chief of Staff of a command.

Defense Federal Acquisition Regulations Supplement (DFARS)
Supplemental regulations for the acquisition process promulgated by the Department of Defense (s*ee* FAR).

Federal Acquisition Regulation (FAR)
The Federal Acquisition Regulations System is established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies. The Federal Acquisition Regulations System consists of the Federal Acquisition Regulation (FAR), which is the primary document, and agency acquisition regulations that implement or supplement the FAR (*see DFARS*).

Life cycle management (**LCM)**
The management of an asset (such as a computer) throughout its useful life, including analysis of the cost/benefits of continuing to use the asset and replacing or retiring the asset when most economically beneficial.

Major subordinate command (MSC)
A Regional Readiness Command or Direct Reporting Command of the USARC.

Office of the Chief, Army Reserve (OCAR)
An Army staff agency supporting the Chief, Army Reserve (*see* CAR).

Program (or project) manager (**PM**)
An acquisition officer that has responsibility for meeting cost, performance, and schedule goals for one or a related set of acquisition projects.

Program objective memorandum (POM)
The 2 to 7 year out financial plan of the Army aligned with the requirements of the Army missions as defined in the Total Army Plan (*see* PPBE *in sec III, below*).

Portfolio
A collection of investments (actual or potential) that is managed as a whole for maximum advantage to the organization by balancing benefits, costs, and risks, particularly C4/IT-related investments.

Requirement control symbol (RCS)
A symbol assigned to a management information requirement in accordance with AR 335-15.

Repository
A facility for the collection, organization, and dissemination of information, particularly a set of electronic capabilities to capture architectural artifacts and metadata descriptions.

Title 10
The Title of the United States Code that authorizes the organization and funding of the Department of Defense and the military service departments.

Section III
Special Abbreviations and Terms

This publication uses the following abbreviations, brevity codes, or acronyms not contained in AR 310-50.

AIS
automated information system

AITR
Army Information Technology Repository

AKM
Army Knowledge Management

AKO
Army Knowledge Online

APE
army program element

ARNet
Army Reserve Network

ATO
Authority to Operate

BPR
business process reengineering; business process redesign

C4/IT
command, control, communications, computers, and information technology

CADM
Core Architecture Data Model

CDAd
Component Data Administrator

CFMO
Chief Financial Management Officer

CIO
Chief Information Officer

CMM
Capabilities Maturity Model

COA
course of action

COI
community of interest

CON
Certificate of Networthiness

COTS
commercial-off-the-shelf

CRD
Capstone requirements document

CTO
Certificate to Operate

DAA
designated approving authority

DITSCAP
Defense Information Technology Security, Certification, and Accreditation Process

DODAF
DOD Architecture Framework

DOIM
Director of Information Management

EPO
Enterprise Plans Office

ERP
enterprise resource planning

ESA
Enterprise Services Activity

ETL
extract, transform, and load

FDAd
Functional Data Administrator

FIPS
Federal Information Processing Standards

GES
Global Information Grid (GIG) Enterprise Services

GIG
Global Information Grid

GIG-ES
Global Information Grid Enterprise Services

GOTS
Government-off-the-shelf

ICD
initial capabilities document

IDM
Information Dissemination Management

IMA
Installation Management Activity

IMO
information management officer

IPT
integrated product team

IT
information technology.

JIM
joint, interagency, multinational

JTA
Joint Technical Architecture

LAN
Local Area Network

MDA
model driven architecture

MDEP
Management Decision Package

NCES
net-centric enterprise services

NCOW
network-centric operations and warfare

NETCOM
Network Enterprise Technology Command

ORD
operational requirements document

PDA
personal digital assistant

PEG
Program Evaluation Group

PKI
Public Key Infrastructure

PPBE
Planning, Programming, Budgeting, and Execution

RCIO
regional CIO

RS
Requirement Statement

RSAIN
Requirement Statement Audit Identification Number

SBU
Sensitive But Unclassified

SEI
Software Engineering Institute

SLA
service level agreement

SODA
services oriented development architecture

SOA
services oriented architecture

SSAA
system security authorization agreement

STAMIS
Standard Army Management Information System

TRM
technical reference model

USARC
U.S. Army Reserve Command

WAN
Wide Area Network

XML
eXtensible Markup Language

Automated data processing equipment (ADPE)
C4/IT hardware.

Automated information system (AIS)
A computer-based application; a system of software with or without dedicated hardware that supports a business process.

Army Information Technology Repository (AITR)
A database maintained by the Army CIO/G-6 that contains information on all Army AIS, which is used as the basis for networthiness and Clinger-Cohen investment decisions.

Army Knowledge Management (AKM)
The Army's strategy to transform itself into a network-centric, knowledge-based force and an integral part of the Army's transformation to achieve the Future Force. AKM will deliver improved information access and sharing while providing "infostructure" capabilities across the Army so that warfighters and business stewards can act quickly and decisively. AKM connects people, knowledge, and technologies. AKM programs pursue five goals associated with governance, best practices, infrastructure management, the Army portal, and human capital.

Army Knowledge Online (AKO)
An Army-wide Web portal and collaboration site established to provide single sign-on access to "webified" applications and collaboration capabilities to authorized users worldwide.

Army Program Element (APE)
Provides the common Department of the Army structure for programming and budgeting resources to individual or logical groups or organizational entities, major combat forces, or support programs. Army program elements are designed and quantified in such a way as to be both comprehensive and mutually exclusive, and are continually scrutinized to maintain proper visibility of Army programs.

Army Reserve Network (ARNet)
The totality of all Army Reserve-wide, metropolitan, campus, and local area networks. The ARNet is a private, non-routable Internet protocol network that connects all Army Reserve sites and connects securely to the DOD network at a limited number of points of presence.

Authority to Operate (ATO)
A document granting permission for the operation of an AIS or network, signed by a network Designated Approving Authority (DAA) under the Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

Command, Control, Communications, Computers, and Information Technology (C4/IT)
All equipment, software, and processes for the creation, collection, storage, processing, and dissemination of information for mission and administrative purposes.

Core Architecture Data Model (CADM)
A metadata model used by the Department of Defense (DOD) to document DOD Architecture Framework (DODAF) architecture artifacts in electronic form.

Component Data Administrator (CDAd)
The DOD expression for the position within a military department responsible for coordinating data administration activities across the department. Within the Army, the Army CIO/G-6 is the Component Data Administrator.

Chief Financial Management Officer (CFMO)
The financial officer for the Chief, Army Reserve.

Chief Information Officer (CIO)
An advisor to an organizational commander concerning investments in information technology. The CIO position is mandated by the Clinger-Cohen Act for Executive Departments and delegated by the Army CIO for Army major commands.

Clinger-Cohen Act
Originally known as Division E of the Information Technology Management Reform Act of 1996, the Clinger-Cohen Act mandates specific disciplines for the effective management of C4/IT investments aligned with mission requirements.

Capabilities Maturity Model (CMM)
A five-stage model of the progression of capabilities of a software development organization, developed by the Software Engineering Institute.

Course of action (COA)
An alternative developed in a decision analysis.

community of interest (COI)
The set of people with a common set of information requirements based on common or parallel subject matter and business processes. In the DOD Net-Centric Data Strategy, communities of interest will be formed around functional communities to manage data interoperability and common network services.

Certificate of Networthiness (CON)
Both a process and a result; the Army CIO/G-6 will enforce network compatibility of Army systems by requiring system owners to submit architecture documentation for examination throughout their development and operational phases. This process also includes the Certificate to Operate (CTO).

Commercial-off-the-shelf (COTS)
Standard, unmodified hardware or software products acquired from commercial sources.

Capstone Requirements Document (CRD)
An acquisition document describing the required capabilities of a collection of related systems.

Certificate to Operate (CTO)
Both a process and a result; a CTO is granted for a system to be fielded in a particular location, taking into account local support capabilities and architectural impacts.

Designated Approving Authority (DAA)
An official with responsibility for evaluating the risks associated with fielding automation solutions within a network and choosing which risks to assume consistent with accomplishment of the missions versus actual and potential costs.

Defense Information Technology Security, Certification, and Accreditation Process (DITSCAP)
A formal process required by DOD and Army guidance to assess, mitigate, and control the risks associated with automation implementations.

DOD Architecture Framework (DODAF)
A system for documenting the operational, system, and technical architecture of a C4/IT implementation and the business processes it supports, formerly called the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Framework. The data requirements of the DODAF are contained in the Core Architecture Data Model. (S*ee* CADM *above*.)

Director of Information Management (DOIM)
The position responsible for automation activities for a post, camp, or station. In the Army Reserve, the USARC Chief Information Officer also holds this position.

Enterprise Plans Office (EPO)
A division of the Enterprise Services Activity responsible for Army Reserve C4/IT planning and investment management processes.

Enterprise resource planning (ERP)
An industry term for the broad set of activities supported by multi-module application software that helps a manufacturer or other business manage the important parts of its business, including product planning, parts purchasing, maintaining inventories, interacting with suppliers, providing customer service, and tracking orders. ERP can also include application modules for the finance and human resources aspects of a business.

Enterprise Services Activity (ESA)
A special staff directorate of the U.S. Army Reserve Command responsible for C4/IT investment management processes, enterprise C4/IT planning, and management of Army Reserve-wide C4/IT services in support of Army Reserve missions.

eXtensible Markup Language (XML)
A derivative of Standard Generalized Markup Language (SGML), developed principally for use in electronic commerce applications on the Internet and now accepted as a general standard for encoding semantic information in electronic documents exchanged between parties.

Extract, transform, and load (ETL)
A set of capabilities for defining the processes of extracting data from production databases, transforming the data into a data warehouse format, and loading the data into the data warehouse.

Functional Data Administrator (FADd)
The functional proponent responsible for the data administration activities associated with a given functional area.

Federal Information Processing Standards (FIPS)
Standards and guidelines developed by the National Institute of Standards and Technology (NIST) for Federal computer systems and issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide.

Future Force
Formerly called the “Objective Force,” the concept of the future Army after transformation.

G-6
Designation for the military staff directorate responsible for information management.

G-8
Designation for the military staff directorate responsible for financial management.

Global Information Grid (GIG) Enterprise Services (GES)
The set of network-based application services that will be implemented on Department of Defense networks for use by all applications without respect to functional area or subject matter. All applications will use these services rather than implementing their own. (*See* GIG *below*.)

Global Information Grid (GIG)
The totality of all Department of Defense networks, computers, applications, and data and the people that use them.

GIG-Army
The portion of the GIG that is provisioned and supported by the Army.

Government-off-the-shelf (GOTS)
Software already owned by the Government and re-used in its unmodified state by one or more additional offices or agencies as a standard product.

Initial capabilities document (ICD)
In a "spiral development" system acquisition in which increasing functionality is delivered in distinct installments through time, the set of functional capabilities that will be delivered in the first installment of the system.

Information Dissemination Management (IDM)
A C4/IT capability being developed for the GIG that will utilize GIG Enterprise Services (*see* GES) to deliver information to combatants and supporting users on a dynamic priority basis using publish and subscribe types of delivery mechanisms.

Installation Management Activity (IMA)
The organization under the Assistant Chief of Staff of the Army for Installation Management charged with managing Army posts, camps, and stations.

Information Management Officer (IMO)
A representative of a command, unit, or functional directorate who interfaces with the supporting Director of Information Management (*see* DOIM) to obtain C4/IT services in support of mission requirements.

Infostructure
A coined word made by the contraction of the words "information" and "infrastructure;" the networks, computers, and related software that provide non-application specific C4/IT capabilities.

Investment
Within this document, a specific actual or planned expenditure of funds to acquire, operate, or maintain a designated C4/IT capability.

Integrated product team (IPT)
A multifunctional team under the leadership of a project proponent responsible for defining the requirements of an acquisition and managing the use of resources to achieve the acquisition goals.

Joint, interagency, multinational (JIM)
An operational designation that pertains to the participation of multiple military Departments (joint), Executive Agencies (interagency), or allied or coalition partners (multinational).

Joint Technical Architecture (JTA)
The technical reference model (*see* TRM) of the Department of Defense.

JTA-Army
The JTA as extended for the requirements of the Army.

Local Area Network (LAN)
A communications network typically limited to a single physical site such as a building, a floor, a department, or a work group.

Model driven architecture (MDA)
An open, vendor-neutral approach to the challenge of interoperability, building upon and leveraging established modeling standards so that platform-independent application descriptions built using these modeling standards can be realized using any major open or proprietary platform.

Management Decision Package (MDEP)
Describes a particular organization, program, or function and records the resources associated with the intended output.

Metadata
Data that describes the attributes of data including domains, ranges, consistency constraints, origins, users, types of use, and quality requirements.

Network-Centric Enterprise Services (NCES)
An acquisition program for the development of the GIG Enterprise Services (*see* GIG-ES).

Network-Centric Operations and Warfare (NCOW)
A future war fighting capability envisioned by the Department of Defense that makes optimal use of C4/IT technologies for information dissemination, collaboration, and other capabilities to improve information superiority.

Network Enterprise Technology Command (NETCOM)
A field operating agency of the Army CIO/G-6 responsible for the operation and sustainment of the Army infostructure.

Networthiness
A coined word denoting the acceptability of an automation implementation for use within Army networks considering architectural compatibility, interoperability, and sustainability. These aspects are measured in the Certificate of Networthiness process for consideration by the CIO Executive Board.

Operational requirements document (ORD)
An acquisition document that defines the operational capabilities of the system to be acquired.

Personal digital assistant (PDA)
A handheld wireless computing device.

Program Evaluation Group (PEG)
One of six groups of financial programs mandated by Title 10 of the U.S. Code for authorizing and funding the Department of Defense and the individual Services.

Public Key Infrastructure (PKI)
A set of standards-based capabilities supporting secure electronic communications between parties in which pairs of public and private keys are used to encrypt, decrypt, and digitally sign messages.

Planning, Programming, Budgeting, and Execution (PPBE)
The financial management system of the Department of Defense covering long-term mission planning through accounting for current year expenditures.

Regional CIO (RCIO)
Within the Army's new regional C4/IT management scheme, a dual-hatted individual serving as an officer of NETCOM and the Installation Management Activity (IMA). This individual is the CIO for the IMA Regional manager and provides NETCOM direction to the DOIMs within the same region.

Requirement statement (RS)
A description of a C4/IT mission need and the financial resources required to satisfy that need.

Requirement statement audit identification number (RSAIN)
A unique identifier assigned to a Requirement Statement (*see above*) and used to track records and transactions relative to a set of requirements.

Sensitive But Unclassified (SBU)
A category of information that should be protected from disclosure to the public but not sensitive compartmented or classified information.

Software Engineering Institute (SEI)
A federally funded research and development center sponsored by the U.S. Department of Defense through the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD (AT&L)). The SEI's core purpose is to help others make measured improvements in their software engineering capabilities.

Service Level Agreement (SLA)
A unilateral or bilateral contract between a service provider and one or more users detailing the services to be provided, the levels of each service, service performance measurements, and penalties and rewards associated with provider performance.

Services oriented development architecture (SODA)
An architecture and tool environment that supports the development and deployment of applications adhering to a services oriented architecture (*see* SOA).

Services Oriented Architecture (SOA)
A component-based application architecture in which all major application functions are exported as services on the network for access by users and other applications.

System security authorization agreement (SSAA)
A document produced by a system proponent detailing the functionality, architecture, configuration, operation, and support of an automation system for the purposes of identifying, eliminating, and mitigating the information security risks inherent in the system (*see* DITSCAP).

Standard Army Management Information System (STAMIS)
Any COTS or GOTS automation system provided by Army proponents for use throughout the Army.

Technical reference model (**TRM)**
A document that organizes and lists all of the technical standards that constrain C4/IT implementations within an organization.

U.S. Army Reserve Command (USARC)
The command element of the Army Reserve responsible for providing trained and ready units and individuals to mobilize and deploy in support of the national military strategy.

Wide Area Network (WAN)
A telecommunications network spanning a broad geographic area, typically (but not always) built upon the facilities of common carriers and involving connections to more than one central switching office, or requiring multi-level routing facilities.

Webified
A coined word that denotes an application that needs nothing more than a web browser for presentation on the user workstation to access the application for the first time.

XML
(See eXtensible Markup Language)

Army Reserve

Certificate to Operate

(For use of this form see USAR Reg 25-3; the proponent agency is ESA)

Proponents will submit this form to Enterprise Services Activity (ESA), Enterprise Plans Office, with attachments.

System Name:	**Date Submitted:**
Army Reserve Proponent: *(Organization)*	**System Owner:** *(Organization)*
POC: *(Rank, name, phone)*	

System includes: ☐ Hardware ☐ System software ☐ Application ☐ Office automation scripts ☐ Other: *(List)*

Attachments:
- ☐ C4IM investment decision package
- ☐ Architecture impact assessment
- ☐ Implementation plan or operations order
- ☐ Operations support plan or C4ISP
- ☐ DITSCAP SSAA
- ☐ Other: *(List)*

Hardware, software, data, and documentation provided to ESA for examination: *(List)*

Reviewed by Command IMO: *(Rank, name, phone)* ☐ *Comments attached*

Reviews completed by ESA

Enterprise Plans Office: *(Rank, name, phone)*	☐ *Comments attached*
Network Applications: *(Rank, name, phone)*	☐ *Comments attached*
Network Services: *(Rank, name, phone)*	☐ *Comments attached*
Information Management Services: *(Rank, name, phone)*	☐ *Comments attached*
Customer Services: *(Rank, name, phone)*	☐ *Comments attached*
Other: *(Rank, name, phone)*	☐ *Comments attached*
Other: *(Rank, name, phone)*	☐ *Comments attached*

Certificate to operate within Army Reserve networks is --

☐ ***Granted for the above system until*** *(date)* _____ ***or until any significant upgrade, enhancement, or configuration change to the system is to be fielded. This Certificate is subject to the following restrictions:***

☐ ***Denied for the following reasons:***

_____

(Name) ***(Title)*** ***(Signature)***

Date of issue: _____

USAR FORM 1 DEC 04 125-R

Replaces USARC Form 125-R (TEST), which is obsolete and will not be used.

Army Reserve

C4 / IT Acquisition Request

(For use of this form see USAR Reg 25-3; the proponent agency is ESA)

Date Requested: _____ *(YYYYMMDD)*

Date Received: _____ *(YYYYMMDD)*

Tracking Number: _____

Originator Name: _____ *(Rank, Name, Phone)*

Org/Directorate: _____

Estimated total acquisition value: $ _____

☐ ESA acquisition ☐ Local acquisition

MDEP: _____ **APE:** _____

☐ AKM waiver attached

Description of items or services to be acquired:

☐ Product specifications attached
☐ Statement of work attached

Business justification:

☐ C4/IT investment decision package attached

RSAIN ***(see USAR Reg 25-3, appendix G)*****:** _____

Other attachments ***(see instructions in USAR Reg 25-3, appendix F, for documentation requirements)*****:**

☐ **Acquisition strategy and plan** ☐ **Other:** _____

Signature of requesting authority: _____
(Printed name/title) *(Signature)*

REVIEWS AND APPROVAL/DISPPROVAL *[For ESA use only]*

Reviewer *(Rank, name, phone)* _____ ☐ *Comments attached*

Reviewer *(Rank, name, phone)* _____ ☐ *Comments attached*

Reviewer *(Rank, name, phone)* _____ ☐ *Comments attached*

Reviewer *(Rank, name, phone)* _____ ☐ *Comments attached*

Reviewer *(Rank, name, phone)* _____ ☐ *Comments attached*

Reviewer *(Rank, name, phone)* _____ ☐ *Comments attached*

Reviewer *(Rank, name,* _____ ☐ *Comments attached*

Reviewer *(Rank, name, phone)* _____ ☐ *Comments attached*

NOTE: All disapprovals will be accompanied by a written memorandum through the Director, ESA to the originator.

☐ Approved, with the following conditions:

☐ Disapproved.

_____ **Date:** _____
(Name/Title) *(Signature)* *(YYYYMMDD)*

Replaces AFRC Form 29-R, which is obsolete and will not be be used.

Army Reserve

C4 / IT Investment Assessment Score Sheet

(For use of this form see USAR Reg 25-3; the proponent agency is ESA)

Investment Name: _____ **Assessment Date:** _____

SECTION I - PREPARATION FOR AUTOMATION AND PROJECT PLANNING			
Assessment Criteria	**Project Scoring**	**Weighting Factor**	**Adjusted Score**
a. ***Business Process Reengineering (BPR) --*** extent to which Business Process Reengineering has been completed for the business processes supported by the investment project (0 - 2). 0 = BPR not performed, no justification provided. 2 = BPR conducted or omission justified.		3.500	0.000
b. ***Requirements Documentation --*** extent and completeness functional and operational requirements definition efforts which have been completed and documented for this investment project (0 - 2). 0 = No documentation. 1 = Incomplete documentation. 2 = Complete documentation.		4.375	0.000
c. ***Project Organization --*** extent to which project participants, roles, and responsibilities have been defined and documented (0 - 2). 0 = No defined project organization. 1 = Partial -- Roles and responsibilities not clearly defined. 2 = Roles fully defined and documented.		4.375	0.000
d. ***Project Planning --*** extent to which project objectives, tasks, timelines, resource levels, and milestones have been documented and followed in work to date (if applicable) (0 - 3). 0 = No documented project plan. 1 = Incomplete project plan or poorly followed. 2 = Well-documented project plan, no history. 3 = Well-documented plan, followed to date.		3.500	0.000
		Subtotal (Section I)	0.000

SECTION II - RISK ASSESSMENT			
Risk (probability of occurrence) + **Impact** 0 = High risk: Likely 1 = Medium risk: Possible 2 = Low risk: Remote 0 = Show Stopper 1 = Moderate Impact	**Risk + Impact = Risk Score**		
	Risk Score	**Weighting Factor**	**Adjusted Score**
Schedule risk -- the presence of significant operational or schedule dependencies that will have to be met to complete this project (0 - 4, see score legend above).		1.125	0.000
Cost sensitivity -- risk that the project will exceed reasonable /targeted cost levels (0 - 4).		1.125	0.000
Technical risk -- risk that the project will not meet its performance or operational objectives (0 - 4).		1.500	0.000
Organizational risk -- risk that the project may fail because of lack of agreement or acceptance by USAR or external organizations (0 - 4).		1.500	0.000
Process change risk -- risk that required business process changes may not be implemented to enable the benefits from this project (0 - 4).		1.500	0.000
Architectural risk -- risk that the project results will not fit with the approved USAR C4/IT architectures to minimize long-term interfacing, performance, and cost problems (0 - 4).		0.750	0.000
		Subtotal (Section II)	0.000

[NOTE: *On a separate sheet, list any other relevant risk factors based on the DOD Risk Management Framework and rate them according to the above scheme. They will be taken into account in evaluating the project risk.* ***]***

SECTION III - OVERALL BUSINESS CASE			
Assessment Criteria	**Project Scoring**	**Weighting Factor**	**Adjusted Score**
Value of the system to the business process -- degree to which the capability resulting from the investment project supports the USAR mission and supporting functional business processes (0 - 4). 0 = Does not support the USAR mission or principle lines of business or core business processes. 1 = Enhances a mission essential process. 2 = Required for the conduct of a mission essential business process. 3 = Enhances a mission critical business process. 4 = Required for the conduct of a mission critical business process.		3.500	0.000
DA and USAR Strategies Addressed -- extent to which the project addresses DA or USAR strategies in approved long range or strategic level plans (0 - 3). 0 = Conflicts with the overall organizational strategic direction. 1 = Neutral - Neither conflicts with nor promotes overall organizational strategic direction. 2 = Promotes achievement of organizational strategic direction. 3 = Critical to achieving organizational strategic direction.		3.500	0.000
Documented Return on Investment -- extent to which benefits and costs are estimated and documented to support a return on investment calculation (0 - 2). 0 = No documented estimates of benefits (cost estimates must be provided). 1 = Costs monetized, benefits quantified but not monitized. 2 = Benefits and costs monetized.		5.250	0.000
		Subtotal (Section III)	0.000

Total Score (all sections)	**Adjusted** 0.000