DEPARTMENT OF THE ARMY ER 25-1-112
U.S. Army Corps of Engineers
CECI-GAD Washington, D.C. 20314-1000

Regulation
No. 25-1-112

15 June 2014

Corporate Information
INFORMATION TECHNOLOGY ARCHITECTURE

1. Purpose. The Corps Enterprise Architecture (CeA) consists of strategic and foundational documents, a common process, and products and services to support current and transitional ways of doing business. These components are developed and used across multiple layers and mission areas within the CeA. Each layer and mission area produces its own architecture products, while reusing pertinent existing artifacts. All artifacts across the mission areas and layers are federated and aligned to provide the aggregate the CeA that is also aligned to both DoD and Federal architectures. The federation and alignment across the CeA is intended to promote integration across architectures, collaboration throughout the USACE architecture community by the Portfolio owners and reuse of existing architecture products. This in turn is intended to continually improve effectiveness and efficiency of the CeA, to allow decision-makers to:

a. Identify overlaps and gaps in capability, interoperability, standardization, duplication and supportability of integrated IT systems.

b. Provide an analytical base for strategically coordinating and sequencing capital planning and investment decisions.

c. Avoid costs associated with maintaining redundant capabilities and also greatly reduce risks to timely and affordable achievement of strategic objectives, including net-centricity, interoperability, and transition from current to future state.

d. Assist in managing USACE transformation and sequencing of the capabilities fielded in support of the USACE processes.

e. Integrate an extensive knowledgebase, so that it is accessible to the right people, at the right time, in the right way.

2. Applicability. This regulation applies to all Headquarters USACE activities, major subordinate commands (MSC), districts, centers and field operating activities and their functional areas of responsibility. Major users of this regulation are ACE-IT and IT system and software.

3. Distribution Statement. All USACE. Approved for public release, distribution is unlimited.

4. USACE Enterprise Architecture Structure. The CeA consists of three primary layers: strategic (enterprise), portfolio mission areas, and programs and solutions. The CeA defines USACE Reference Models, Target Architecture, Standards and Policy and identifies information technology within End-to-End (E2E) processes, portfolios (mission areas/domain) and the supporting IT investments. It provides a holistic view of USACE and a common view for aligning architectures (See Appendix E), priorities, and initiatives. Figure 1 shows the top down structure for the architectures described in this regulation. The Strategic (Enterprise) Architecture Layer sets the overall guidance and is controlled by the IT Executive Board. The Portfolio Architecture Layer assures technical architectures align to the Strategic Architecture layer guidance and controls the technical interfaces among the Program and Solutions layer. The lowest level, the Program and Solution Architecture Layer defines the architectures of the individual programs and solutions and is maintained by the program managers.

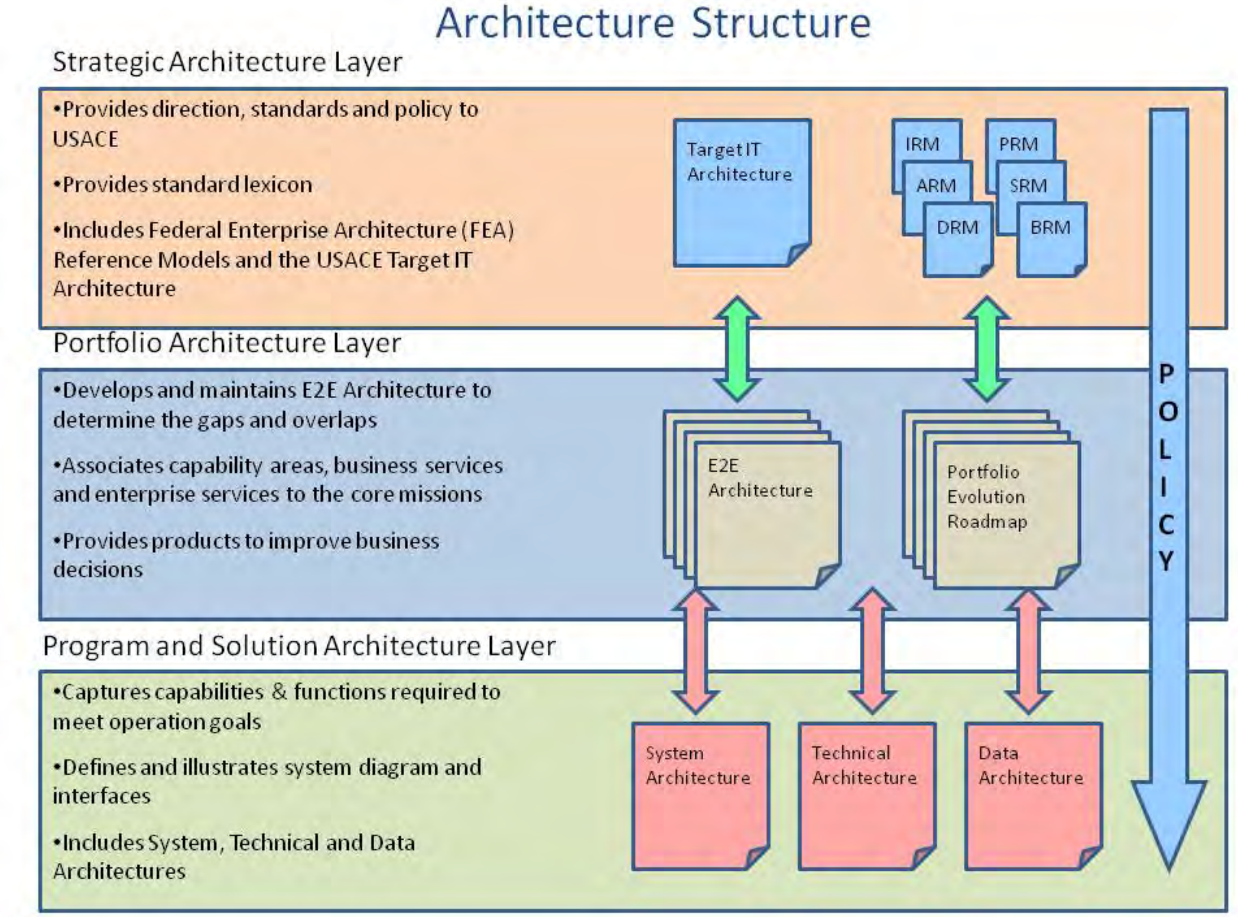

Architecture Structure
Strategic Architecture Layer
•Provides direction, standards and policy to USACE
•Provides standard lexicon
•Includes Federal Enterprise Architecture (FEA) Reference Models and the USACE Target IT Architecture
Target IT Architecture
IRM
ARM
DRM
PRM
SRM
BRM
Portfolio Architecture Layer
•Develops and maintains E2E Architecture to determine the gaps and overlaps
•Associates capability areas, business services and enterprise services to the core missions
•Provides products to improve business decisions
E2E Architecture
Portfolio Evolution Roadmap
Program and Solution Architecture Layer
•Captures capabilities & functions required to meet operation goals
•Defines and illustrates system diagram and interfaces
•Includes System, Technical and Data Architectures
System Architecture
Technical Architecture
Data Architecture
POLICY

Figure 1 USACE Enterprise Architecture Structure

5. Program & Solution Architecture Layer. Program and solution architectures define assets used to automate mission and business functions. They can be a solution in and of themselves or part of a larger capability. Architectures are developed in this layer following the current Department of Defense Architecture Framework (DoDAF) standards, as

mandated in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01F. The stakeholders are end users, developers, IT Chiefs, and Communities of Practice (CoPs).

A project is managed with a clear end date in mind and according to a set scope and budget with a single easily definable tangible output (e.g. a list of deliverables, a new system or an improved process). A particular project may or may not be part of a program. A program is a collection of two or more projects sharing a common goal. Projects/Programs require a Charter from the respective PMs. Architecture artifacts in the program and solution layer are developed for Projects and Programs and are described below.

5.1 System Architecture. The program/project system architecture is used by program managers and the IT service provider to describe the purpose, structure and interfaces associated with the program/project, to manage the interfaces between the program/project and other programs/projects, and to document compliance with the Enterprise Architecture. The system architecture is comprised of a system diagram and system description. A system diagram is the conceptual model that defines the structure, behavior, and connections of a system. A system description is a written representation of a system that is organized to support understanding about the interfaces and the internal structures of the system. Primary responsibility for the creation or development of the system architecture is the Program Manager with support from Project Managers and system developers. The stakeholders for systems architectures are the developers, CoPs and IT Chiefs.

5.1.1 System Diagram. System diagrams are used in development and in change and configuration control management. The system diagram is a graphical depiction of the internal and external interfaces between system components. See example in Appendix D. The system diagram is created during Phase 2 of the Business Capability Lifecycle (BCL), Investment Management phase and is updated when there is a change to the interfaces, databases, or system boundaries.

The system diagram includes the following information:

a. Display Internal/external interface connections.

b. Number of databases/data stores.

c. Locations of components.

d. Firewall/DMZ boundaries.

5.1.2 System Description. The system description is used to define the business needs and system functionality. The description should detail who the system owner is, who the users are (internal and/or external), what campaign goals are satisfied and which business processes it supports. See template and example in Appendix D. The system description is created during Phase 1 of the BCL, Business Capability Definition phase and is updated when there is a change to the business requirement, functionality or system change.

The system description includes:

a. Business requirements.

b. Business functions provided.

c. Functionality.

d. End Users.

e. Products.

f. Strategic goals.

g. End-to-End (E2E)/Business Processes supported.

5.2 Technical Architecture. The technical architecture defines and specifies the detailed functions, interfaces, parameters, and protocols used by the program/project. The technical architecture is used by the program/project managers, program/project development and maintenance teams and by the USACE Service Provider (i.e. ACE-IT) engineering organization to: 1) document the detailed design and 2) assure compatibility among the many programs/projects supporting the USACE mission. The technical architecture is comprised of a technical description and interface descriptions. The interface description depicts the method used to transfer data within the system and with external systems.

The Program Manager has primary responsibility for the creation or development of the technical architecture with support from Project Managers and technical developers. The stakeholders for the technical architecture are CoPs, IT Chiefs, ACE-IT engineering and architects.

5.2.1 Technical Description. A technical description defines the structure, behavior, and connections of a system and is organized to support the understanding about the interfaces and the internal structures of the system. The technical description is used to define technical functionality. See template and example in Appendix D. The technical description is created during Phase 2 of the BCL, Investment Management phase and is updated when there is a change to the functionality, technologies or standards of the system.

The technical description includes:

a. Functionality

b. Interfaces

c. Standards

d. Technologies

5.2.2 Interface Description. The interface description defines the internal and external connections to support data exchanges/transfers among hardware and software components within the system, and external data exchanges/transfers to/from other hardware and software systems. The interface description is a tabular listing of all system interfaces that indicates the type of interface, the originator/receiver, data elements and use of the data. The interface description will be used for change management, security, elimination of redundancy and enterprise data management. See template and example in Appendix D. The interface description is created during Phase 2 of the BCL, Investment Management phase and is updated when there are changes to the internal/external connections and boundaries.

The interface description includes:

a. Interface type/protocols.

b. Originator/receiver.

c. Data elements.

d. Use of data.

5.3 Data Architecture. The data architecture provides the framework to support data requirements. The availability, efficiency and effectiveness of data have an impact on the ability of portfolio owners to make informed decisions. The data architecture is comprised of two parts, a standardized logical data model that shows the relationship between the entities of a system and the systems it connects to and the data dictionary that defines the data structure of the metadata. Primary responsibility for the creation or development of the data architecture is the Program Manager with support from Project Managers and technical developers. The stakeholders for the data architecture are CoPs, IT Chiefs, ACE-IT engineering and architects. Proponents will identify and register authoritative data sources, in accordance with DoDI 8320.02 (August 2013), supplying the artifacts (data dictionary, standardized data architecture, etc.) to support mission required data needs.

5.3.1 Logical Data Model. The logical data model is represented as an entity relational diagram (ERD). The ERD is a model that depicts the intra-relationships between the data elements. ERD must adhere to policies, rules, and standards that govern the data structure and are documented in ER 25-1-110. See diagram and example at Appendix D. The logical data model is created during Phase 2 of the BCL and is updated when there is a change to the database structure or data elements.

5.3.2 Data Dictionary. A data dictionary is a data structure that stores metadata, i.e., (structured) data about data. The data dictionary contains the description for each data element found in the logical data model. See diagram and example at Appendix D. The data dictionary is created during Phase 2 of the BCL and is updated when there is a change to the data elements. All shared common data entities will be structured in a standardized format (field names, sizes, types, etc.) in accordance with reference Appendix A.w (DODI 8320.02), Sharing Data, Information, and IT Services in the Department of Defense and reference Appendix A.u ER-1-25-110, Enterprise Data Management Policy.

5.4 Roles and Responsibilities.

a. Chief IT Architect:

(1) Ensures program and solution architectures are in compliance with the enterprise architecture.

(2) Approves/disapproves program and solution architectures.

(3) Consolidates program and solution architectures within USACE architecture tool.

b. Data Architect:

(1) Provides guidance for the compliancy of data structure development and management.

(2) Approves /disapproves IT investment Data management Plans.

c. Portfolio Manager:

(1) Provides support in consolidation of program and solution architectures.

(2) Provides continuity between Program Managers.

d. ACE-IT Architect/Engineer:

(1) Provides critical review of external interfaces and compliance to the USACE IT architecture.

(2) Uses the interface descriptions to assure and control interoperability among the different IT components within the overall USACE IT architecture to include enterprise AIS's.

(3) Analyze capacity, storage, bandwidth, availability/use for applications and systems including projected growth and limitations based on IT future requirements.

(4) Ensure ACE-IT processes will support the requirements of applications.

(5) Validate system architecture artifacts.

e. Program Manager:

(1) Ensures program and solution architectures are created for each system within the program.

(2) Ensures architectures are approved by Chief IT Architect and through the formal change management process.

(3) Ensures annual review and update of architectures.

(4) Ensures architectures are stored on the USACE IT Investment SharePoint site.

(5) Define business requirements for ACE-IT support.

f. Project Manager/Development Team:

(1) Develops and maintains system and technical architectures.

(2) Submits the architecture artifacts for approval as part of the change management process.

(3) Annually reviews and updates program and solution architectures.

(4) Uploads current architecture artifacts to the USACE IT Investment SharePoint site in time to support the annual Portfolio Compliance Review.

(5) Define business requirements for ACE-IT support.

6. Portfolio Architecture Layer. A portfolio comprises an organization's IT investments required to achieve specific strategic mission objectives. The portfolio architecture layer associates capability areas, business services and enterprise services with the core missions and is focused on providing products that improve delivery of services to its customers. The portfolio architectures consist of the End-to-End (E2E) architectures and the portfolio evolution roadmaps that are aligned to the principles, structure, and processes used at the enterprise layer. The portfolio architecture provides uniform methods to align the portfolios with the USACE strategic direction, perform risk management and apply governance uniformly. These architectures provide a business perspective for an entire portfolio and are developed by the Portfolio Managers with support from the Program Managers and the IT architects. The architectures allow the Portfolio Owners to look at E2E processes and determine the impact of proposed changes to systems enabling them to assess and prioritize the evolution of systems based on required capabilities and business goals.

6.1 End-to End (E2E) Architectures. The E2E architectures are developed using the E2E business processes. The architectures assist Portfolio Owners and Portfolio Managers in performing IT optimization while examining the business processes within the portfolio from the perspective of E2E business flows. This enables the portfolio owner to identify and streamline IT from the perspective of all of the inter-related activities required to perform a business process. By streamlining IT using this approach, USACE will create consistent data models, eliminate redundancies and duplications and reduce the life-cycle costs of the business IT systems. The E2E architectures are also used in the enterprise layer to develop and maintain the Business Reference Model. The E2E architectures are created when E2E business processes are published by USACE Resources Management (CERM) and updated when there are changes to the IT Investments that impact the business processes. The E2E architecture will map the required IT to the individual steps of the process and explain what function the IT is performing at this step and its criticality to the process. See the example and template in Appendix D. The Portfolio Owners and Managers develop and use the E2E architectures to document the IT in support of the specific business activities performed. Stakeholders are the Portfolio Owners, Portfolio Managers (PfM), Program Managers (PM), enterprise architects and service providers.

6.2 Portfolio Evolution Roadmap. The Portfolio Evolution Roadmap is the depiction of planned incremental steps toward migrating a suite of IT investments to meet projected business goals. This depiction shows change over time to allow an orderly transition to the target architecture and eliminate duplicative functions and systems. The Portfolio Evolution Roadmaps enable the Portfolio Owners to plan for projected resource requirements. Evolution roadmaps are produced to illustrate different categories of change. The Portfolio Owners and Managers create and use the Portfolio Evolution Roadmaps to plan for the future. The Portfolio Evolution Roadmap is updated at the direction of the IRB to reflect transition to the target architecture. Stakeholders are the Portfolio Owners, Portfolio Managers (PfM), Program Managers (PM), enterprise architects and the service provider. See the examples in Appendix D.

6.3 Roles and Responsibilities.

a. Chief IT Architect:

(1) Provides guidance to Portfolio Owners and Managers in developing E2E architectures.

(2) Provides guidance to Portfolio Owners and Managers in planning and developing portfolio evolution roadmaps.

(3) Uploads E2E architecture documentation to the business architectural tool and provides updates to the USACE business IT view.

b. ACE-IT Architect/Engineer:

(1) Provides review of proposed deployment timelines to assure planned deployments align with other related deployments and supported infrastructure.

(2) Support portfolio by portfolio roadmap development.

c. IT Portfolio Owner:

(1) Provides direction to Portfolio Manager in developing the E2E architecture.

(2) Provides direction for their Portfolio Manager in developing portfolio evolution roadmap.

d. Portfolio Managers:

(1) Responsible for developing E2E architecture and portfolio evolution roadmap only if authorized/assigned by Portfolio owner.

(2) Coordinates with other Portfolio Managers, Program Managers and ACE-IT in developing E2E architecture and portfolio evolution roadmap.

(3) Consolidate portfolio by portfolio evolution roadmap.

7. Enterprise Architecture Layer. The enterprise layer identifies common and shared assets whether they are strategies, processes, investments, data, capabilities, services, systems, or technologies that should be reused across the Corps. It also identifies whether resources are properly aligned to USACE's mission, strategic goals and objectives. The stakeholders are headquarters staff and portfolio owners.

The enterprise layer provides the overall principles, structure and process to guide the USACE business community as outlined in the Federal Enterprise Architecture Framework (FEAF) and DoD/Army policies. Enterprise architecture products are developed to support senior leadership decisions. The enterprise architecture layer includes the Federal Enterprise Architecture (FEA) Reference Models and the USACE Target IT Architecture. This layer is based on strategic documents including Federal, DoD, Army and USACE Campaign Plans. These documents provide the principles, rules, and guidelines for managing the CeA and developing architectures across USACE. The commonality between the different architecture models are illustrated in Appendix E.

7.1 USACE Reference Model. USACE Reference models are directly aligned with Federal, DoD and Army enterprise architecture reference models. The models – performance, business, security, data, infrastructure and application – provide a common taxonomy and framework to help drive integration across USACE and among other Federal/DoD/Army elements. The reference models normalize and support vertical and horizontal integration, enable cross-enterprise analysis and collaboration of USACE investments and capabilities. This facilitates the overall USACE IT planning process, reinforces enterprise management, integration analysis and compliance, and helps to support and substantiate the development of USACE's target architecture and migration strategy. In addition to providing a common taxonomy, the reference models are key components in the overall enterprise architecture framework for enabling linkages from enterprise strategy and objectives to investments. Reference models used by USACE are listed below.

7.1.1 Performance Reference Model (PRM). Performance Reference Model (PRM) is a standardized framework to measure the performance of IT investments and their contributions to portfolio performance. The PRM has three main purposes:

a. Help produce enhanced performance information to facilitate and improve strategic and on-going decision-making,

b. Improve the alignment and better articulate the contribution of inputs to outputs and outcomes to desired results, and

c. Identify performance improvement opportunities that span traditional organizational structures and boundaries.

The PRM is composed of four measurement areas:

a. customer results,

b. processes and activities,

c. IT portfolio analysis, and

d. Technology assessments.

7.1.2 Business Reference Model (BRM). Business Reference Model (BRM) is a function-driven framework for describing the business operations of the Federal Government independent of the agencies that perform them. This business reference model provides an organized, hierarchical construct for describing the day-to-day business operations of the Federal government using a functionally driven approach. The BRM is the first layer of the Federal Enterprise Architecture and it is the main viewpoint for the analysis of data, service components and technology. The BRM is broken down into the following four areas:

a. Services for Citizens (Water Management, Geospatial, Recreation, Emergency Response, etc.),

b. Mode of Delivery (Web-based access to services, etc.),

c. Support Delivery of Services (Hand-held devices, Networks, AISs, etc.), and

d. Management of Government Resources (Environmental, Management of Federal Lands and Real Property, Financial Management, HR Management, etc.).

The Business Reference Model provides a framework that facilitates a functional (as opposed to organizational) view of the federal government’s lines of business (LoBs), including its internal operations and its services for the citizens, independent of the agencies, bureaus and offices that perform them. By describing the federal government around common business areas instead of by a stovepipe, agency-by-agency view, the BRM promotes agency collaboration and serves as the underlying foundation for the FEA and E-Gov strategies.

7.1.3 Security Reference Model (SRM). The Security Reference Model (SRM) supports architectural analysis and reporting across all of the sub-architecture views of the overall Enterprise Architecture. The SRM is taxonomy for the itemization of security controls in architecture, and the overall EA, as well as a scalable, repeatable and risk-based methodology for addressing information security and privacy requirements within and across systems, segments, agencies, and sectors. The SRM provides a common language for discussing security and privacy in the context of federal agencies' business and performance goals. The SRM:

a. provides a roadmap that assists agencies in integrating IT security/privacy with EA,

b. provides a mechanism for identifying security and privacy requirements,

c. promotes inclusion of security and privacy in business activities and processes,

d. integrates the NIST "Risk Management Framework", "Improving Critical Infrastructure Cyber security", and the organization's system development life cycle processes to ensure that relevant security and privacy requirements are integrated and continuous monitoring is implemented and

e. helps program executives understand how the Federal Information Processing Standards (FIPS) 199 of confidentiality, integrity, and availability and the eight privacy Fair Information Practice Principles (FIPPs) fit within enterprise architecture planning, while leveraging standards and services that are common to the enterprise and the government.

Federal Government organizations are mandated to implement both security and privacy protections for federal information and information systems. The SRM demonstrates how intertwined these two requirements are in the design and implementation of a federal architecture. All too often, security and privacy have been considered at the end of program development, resulting in higher costs and implementation delays. The SRM brings security and privacy requirements to the forefront of the decision-making process.

7.1.3.1 Mobile Security Reference Architecture (MSRA). The Mobile Security Reference Architecture (MSRA) provides reference architecture for mobile computing and focuses on securing the use of commodity and mobile computing devices and infrastructure used to access Federal Government resources. Mobile computing devices ("mobile devices") require a rethinking of the security models that are traditionally employed to protect information accessed by off-site/remote workers. Appropriate authentication methods, traditional security products (e.g., anti-virus, firewalls), and connectivity options may be limited, nonexistent, or require modifications to accommodate mobile devices. The MSRA enumerates these issues and describe strategies to address them. Prior to the adoption of mobile computing devices for processing sensitive information, a threat and risk assessment should be performed that is tailored to their specific mobile data threat environment and mobile services. Both policy development and the required levels of mobile device management should be considered as input to the threat and risk assessment so that the appropriate security controls can be implemented as appropriate.

7.1.4 Data Reference Model (DRM). The Data Reference Model (DRM) is the supporting foundation for the overall EA with a focus on two core questions: what information is available for sharing and re-use, and what the information gaps are, needing validation. The DRM is designed to provide a flexible common framework for effective sharing of government information across organizational boundaries, increase integration and re-use opportunities, and support semantic interoperability while respecting security, privacy, and appropriate use of that information. It enables agencies to manage information as national assets to better serve the American public and meet mission needs. The DRM acts as a catalyst to enhance the value of existing data holdings residing in “silos” through better discovery and understanding of the meaning of the data, how to access it, and how to massage or aggregate it to support performance results. The DRM provides a standard means by which data may be described, categorized, and shared. These are reflected within each of the DRM’s three standardization areas: Data Context (object/property), Data Description (representation) and Data Sharing as defined in ER 25-1-110, Information Management, Enterprise Data Management Policy. ER 25-1-110 is the high level governance for the USACE Enterprise Data Management Program (EDMP) and describes a data asset. Data assets throughout USACE include, but are not limited to, all data collected or derived by appropriated USACE funded programs, either directly by its employees or through contracts or grants, as well as data shared within and outside of USACE. This EDMP encompasses the process of designing, managing, protecting, and disseminating USACE data assets that are collected, generated, maintained, aggregated, stored and distributed within USACE while supporting business functions and goals. The EDMP governs the Data Architecture segment of the Corps’ Enterprise Architecture (CeA) within the DRM. These EDMP data requirements are harmonized at the enterprise level through the collaboration of a data stewardship program.

7.1.5 Infrastructure Reference Model (IRM) The Infrastructure Reference Model (IRM) supports architectural analysis and reporting in the host infrastructure sub-architecture view of the overall EA. The IRM is a component-driven taxonomy that categorizes the network/cloud related standards and technologies to support and enable the delivery of voice, data, video, and mobile service components and capabilities. The IRM also unifies existing agency infrastructure portfolios and guidance on standard desktop configurations by providing a foundation to advance the reuse and standardization of technology and service components from a Federal Government perspective.

7.1.6 Application Reference Model (ARM). The Application Reference Model (ARM) supports architectural analysis and reporting in the applications sub-architecture view of the overall EA. The ARM is a component-driven taxonomy that categorizes the system and application related standards and technologies that support and enable the delivery of service components and capabilities. It also unifies existing agency application portfolios and guidance on standard desktop configurations by providing a foundation to advance the reuse and standardization of technology and service components from Federal Government perspective. Aligning agency capital investments to the ARM leverages a common, standardized vocabulary, allowing interagency discovery, collaboration, and interoperability. Agencies and the Federal Government will benefit from economies of scale by identifying and reusing the best solutions and technologies for applications that are developed/provided or subscribed to support their business functions, mission, and target architecture.

7.2 Target IT Architecture. The purpose of the Target Architecture is to serve as guidance and standards to migrate the IT environment from the current architecture to the future architecture over 5 years and beyond. This will allow USACE to move into the future while meeting regulatory and technology driven changes. The benefits of using this Target Architecture include that it:

a. serves as a target allowing a smooth transition into the future, without breaking systems,

b. provides a single source to demonstrate compliance with standards and mandates,

c. strengthens portfolio management (PfM) and business system Investment Review Boards processes by specifying future standards,

d. enables rational and deliberate basis for resource allocations,

e. enables improvement and streamlines business processes using new and emerging technologies (e.g., cloud computing/mobile computing) and

f. enhances interoperability and improves timeliness of communications.

The value of aligning USACE under a common mission environment is to increase interoperability and operational relevancy and decreasing the time for development, certification and overall costs. Specifically, it will provide:

a. reduced life cycle costs through standardized applications and unity of effort,

b. enhanced cyber protection and

c. flexible infrastructure to evolve to rapidly emerging standards.

7.3 Roles and Responsibilities. The stakeholders for the Enterprise Architecture layer are HQ Staff and Portfolio Owners.

a. CECI

(1) Ensure E2E architectures are aligned with the USACE Business Reference Model and the Campaign Plan.

(2) Ensure all reference models are developed and approved.

(3) Develop BRM and DRM.

(4) Develop SRM and ARM in coordination with ACE-IT.

(5) Ensure PRM is developed and provides the necessary performance measures needed to validate success.

(6) Post reference models in the USACE architecture tool.

(7) Coordinate and develop the documents used as guidelines and standards for IT Investments:

(a) Policies and Regulations.

(b) Reference Model Standards.

(c) Target IT Architecture.

(d) Standards.

b. ACE-IT

(1) Develop IRM.

(2) Develop SRM and ARM in coordination with CECI Architects.

8. USACE Enterprise Architecture Governance. Governance is vital to ensure that USACE's investments produce desired outcomes as effectively and efficiently as possible. Effective governance is the key to enterprise architecture. Architecture governance is the key to aligning enterprise investments to business goals, cost control and providing value.

IT governance is the process that ensures the effective and efficient use of IT, enabling USACE missions. IT governance is the process by which organizations ensure the effective evaluation, selection, prioritization, and funding of competing IT investments; oversee their implementation; and extract (measurable) business benefits. IT governance is a business investment decision-making and oversight process, and it is a business management responsibility.

8.1 Governance Boards. USACE IT Architecture is governed by three boards. Governance activities within the EA life-cycle management influence and direct the policies, procedures, roles, responsibilities, schedules, and appropriate decision making bodies that govern the EA. The governance activities also ensure the EA is integrated with appropriate planning and management processes, such as portfolio management, configuration management, resource allocation, and strategic planning efforts. Governance is achieved through the following boards explained below and illustrated in Figure 2:

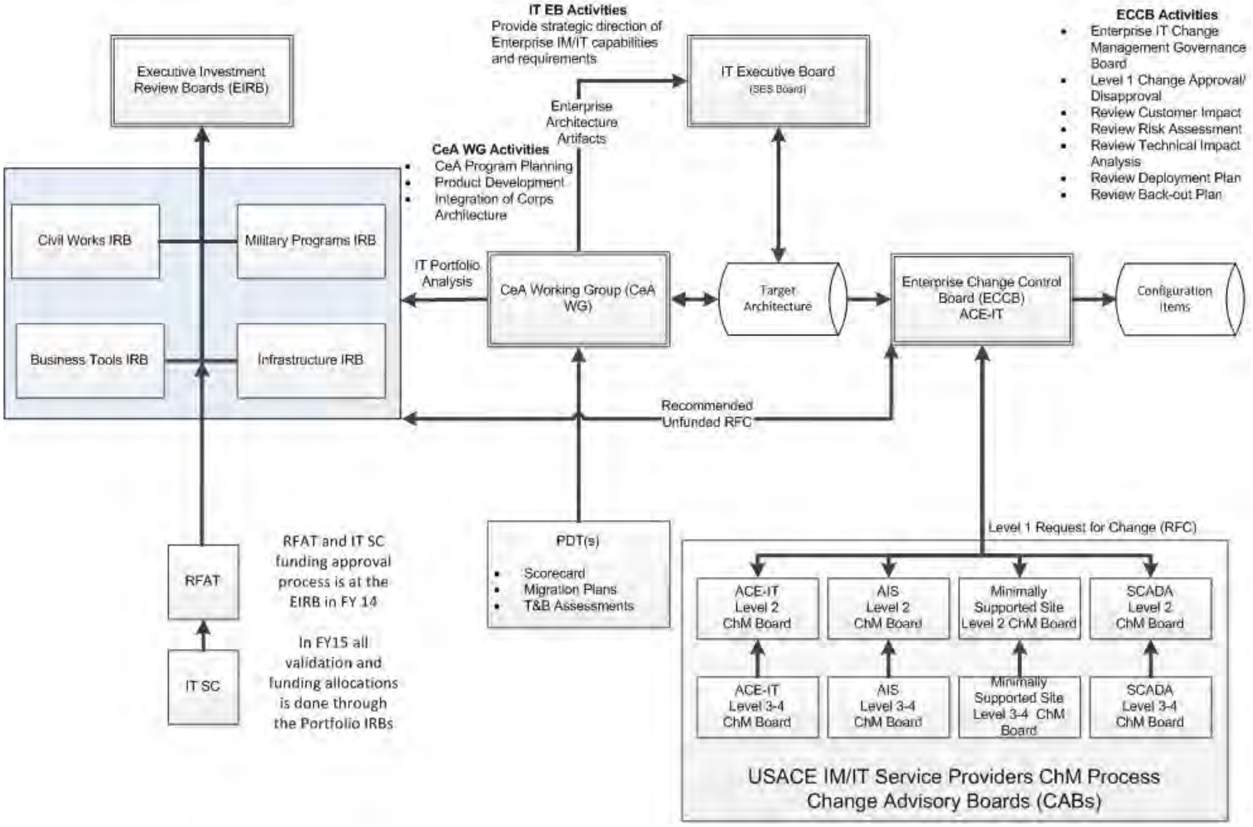

IT EB Activities
Provide strategic direction of Enterprise IM/IT capabilities and requirements
ECCB Activities
Enterprise IT Change Management Governance Board
Level 1 Change Approval/ Disapproval
Review Customer Impact
Review Risk Assessment
Review Technical Impact Analysis
Review Deployment Plan
Review Back-out Plan
Executive Investment Review Boards (EIRB)
IT Executive Board
(SES Board)
Enterprise Architecture Artifacts
CeA WG Activities
CeA Program Planning
Product Development
Integration of Corps Architecture
Civil Works IRB
Military Programs IRB
Business Tools IRB
Infrastructure IRB
IT Portfolio Analysis
CeA Working Group (CeA WG)
Target Architecture
Enterprise Change Control Board (ECCB)
ACE-IT
Configuration Items
Recommended Unfunded RFC
RFAT
IT SC
RFAT and IT SC funding approval process is at the EIRB in FY 14
In FY15 all validation and funding allocations is done through the Portfolio IRBs
PDT(s)
Scorecard
Migration Plans
T&B Assessments
Level 1 Request for Change (RFC)
ACE-IT Level 2 ChM Board
AIS Level 2 ChM Board
Minimally Supported Site Level 2 ChM Board
SCADA Level 2 ChM Board
ACE-IT Level 3-4 ChM Board
AIS Level 3-4 ChM Board
Minimally Supported Site Level 3-4 ChM Board
SCADA Level 3-4 ChM Board
USACE IM/IT Service Providers ChM Process Change Advisory Boards (CABs)

Figure 2 USACE IT Governance and Capital Planning Boards

a. IT Executive Board (IT EB). The IT EB, an SES Level Board, provides strategic direction for IM/IT capabilities and requirements and provides direction to resolve issues escalated from CeA WG and E-CCB that require senior level decision authority. Chair is USACE CIO.

b. Corps of Engineers Enterprise Architecture Working Group (CeA WG). The CeA WG's mission is to manage and implement the CeA Program objectives and approve and integrate products to foster collaboration throughout USACE that will educate and provide recommendations to decision making boards, IM/IT program managers, portfolio managers and CeA stakeholders. The CeA WG members will facilitate the CeA Program awareness throughout the represented USACE Communities of Practice (COPs), stakeholders and leadership. Chair is Chief IT Architect.

c. Enterprise Change Control Board (E-CCB). The purpose for the change control board is to assure and control interoperability among the different IT components within the USCE IT architecture. The formal change management process is used to assure individual program and solution elements are not introduced to the architecture which could adversely impacts other elements. This will ensure that systems development and/or modernization can be accomplished in such a manner that will not degrade the operation of the network. The board identifies reviews, prioritizes, and approves changes to the USACE enterprise hardware and software standards. Chair is Chief IT Architect.

FOR THE COMMANDER:

ADAM S. ROTH
COL, EN
Chief of Staff

5 Appendices
Appendix A – References
Appendix B – Acronyms
Appendix C – Glossary
Appendix D – Templates/Examples
Appendix E – Data Element Relationship

APPENDIX A

References

A-1 Federal Regulations, Laws, Guidance

a. The Common Approach to Federal Enterprise Architecture (May 2, 2012, author, Executive Office of the President of the United States)

b. Government Accountability Office Enterprise Architecture Management Maturity Framework 2.0 (GAO-10-846G, published August 5, 2010)

c. OMB Circular A–130, Management of Federal Information Resources, dated, February 8, 1996

d. Public Law 104–106, National Defense Authorization Act for Fiscal Year 1996, February 10, 1996

A-2 Department of Defense Regulations and Guidance

a. Army Information Architecture (AIA), Version 4.1, 05 June 2013, Office of the Army Chief Information Officer (CIO/G-6), Army Net-Centric Data Strategy Center of Excellence

b. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01F, dated 21 March 2012

c. Defense Business Council (DBC) & Investment Review Board (IRB), author, Department of Defense (DoD) Office of the Deputy Chief Management Officer (DCMO), dated April 8, 2013 (http://dcmo.defense.gov/governance/dbc-irb.html)

d. Department of Defense Discovery Metadata Specification (DDMS), Version 4.1. Defense 809 Information Systems Agency (DISA), Program Executive Officer, Global Information Grid 810 (GIG) Enterprise Services. 12 June 2012

e. Department of Defense Joint Technical Architecture (JTA), Version 6.0, Volume II, 3 October 2003

f. Directive-Type Memorandum 08-020, "Investment Review Board (IRB) Roles and Responsibilities", January 26, 2009, Incorporating Change 1, September 3, 2010

g. DoD Business Enterprise Architecture, author, Department of Defense (DoD) Office of the Deputy Chief Management Officer (DCMO), dated February 14, 2013

h. DoD ESI & The Joint Information Environment (JIE), DoD DISA Mission Partners Conference 2012, May 7, 2012

i. DoD Instruction 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense, 5 August 2013

j. DoD IT Defense Business Systems Investment Review Process: Guidance, January 2009

k. DoDD 8115.01 Information Technology Portfolio Management

A-3 Department of the Army Regulations and Guidance

a. AR 25–1, Army Information Technology, 25 June 2013

b. AR 25–2 Information Management Information Assurance 23 Mar 2009

c. DA Pam 25–1–1 Information Management Army, Information Technology Implementation Instructions, 25 June 2013

d. LandWarNet (LWN) 2020 and Beyond, United State Army Chief Information Officer (CIO) G-6, Version 1.0, 7 August 2013

A-4 USACE Regulations and Guidance

a. ER 25-1-106, Information Technology Capital Planning and Investment Management, 22 Jun 2006

b. ER 25-1-110, Information Management Enterprise Data Management Policy Corporate Information, 31 Jul 2013

c. USACE IT Target Architecture for 2017, CIO Policy Memo 11-017, 26 Oct 2011

APPENDIX B

Acronyms

Acronym	Title
ACE-IT	Army Corps of Engineers Information Technology
AEA	Army Enterprise Architecture
AIS	Automated Information System
APL	Approved Products List
APMS	Army Portfolio Management System
ARM	Application Reference Model
BEA	Business Enterprise Architecture
BBP	Best Business Practices
BI	Business Intelligence
BPR	Business Process Re-Engineering
BRM	Business Reference Model
CeA	Corps Enterprise Architecture
CECI-A	Corps of Engineers Corporate Information - Architecture
CIO	Chief Information Officer
CPD	Capital Planning Division
DoDAF	Department of Defense Architecture Framework
DRM	Data Reference Model
EAMMF	Enterprise Architecture Management Maturity Framework
FEAF	Federal Enterprise Architecture Framework
GAD	Governance & Architecture Division
GAO	Government Accountability Office
HQ	Headquarters
IA	Information Assurance
IM/IT	Information Management / Information Technology
ISO	International Organization for Standardization
IRB	Investment Review Board

Acronym	Title
IT	Information Technology
ITIPS	Information Technology Investment Portfolio System
IRM	Infrastructure Reference Model
LoB	Lines of Business
MOA	Memorandum of Agreement
NetOps	Network Operations
NMB	National Management Board
O&M	Operations & Maintenance
OMB	Office of Management and Budget
PfM	Portfolio Management
PgM	Program Manager
PID	Portfolio Integration Division
PM	Project Manager
PRM	Performance Reference Model
SLA	Service Level Agreement
SRM	Security Reference Model
TLA	Top-Level Architecture
TLS	Transport Layer Security
UC	Unified Capabilities
USACE	US Army Corps of Engineers

APPENDIX C

Glossary

Name	Description
Activity	An Army organization. Within the context of the AEA, a specific function that must be performed to produce, consume, or transform information. Activities are grouped into larger processes in support of accomplishing tasks and missions. Depending on the context, an activity or function is performed by an individual, unit, or prime system element. Work, not specific to a single organization, weapon system or individual that transforms inputs (Resources) into outputs (Resources) or changes their state.
Agreement	A consent among parties regarding the terms and conditions of activities that said parties participate in.
Application	Software that performs a specific task or function, such as word processing, creation of spreadsheets, generation of graphics, or facilitating email. For purposes of reporting in APMS, applications may be reported as a separate investment or included in an information system registration. If reported as a separate investment, applications will identify in the dependency tab, the host system it resides on as the parent information system.
Architecture	See enterprise architecture and Army enterprise architecture.
Army Business Enterprise Architecture	The framework of business processes and organizations that support the Army's Warfighters.
Army Enterprise Architecture	See also enterprise architecture. The AEA transforms operational visions and associated required capabilities of the business and warfighting missions into a blueprint for an integrated and interoperable set of information systems and NSS that implement horizontal information technology insertion, cutting across the functional stovepipes and Service boundaries. The AEA supports the LandWarNet and is the combined total of all the Army's operational, technical, and system architectures.
Army enterprise infrastructure	The systems and networks that comprise the LandWarNet.

Name	Description
Army Knowledge Management	The Army wide strategy to transform the Army into a network-centric and knowledge-based force to improve information dominance by our Warfighters and business stewards. It includes, but is not limited to, improving processes, technology, and work culture to collaborate, catalog, store, find, and retrieve information; and share this information with Joint, coalition, and international partners as mission needs dictate.
Army Recordkeeping Systems Management	Cost-effective organization of Army files and records contained in any media so that records are readily retrievable. Ensures that records are complete; facilitates the selection and retention of permanent records; and accomplishes the prompt disposition of noncurrent records in accordance with National Archives and Records Administration approved schedules.
Authentication	A security service that verifies an individual's eligibility to receive specific categories of information.
Authoritative data source	A recognized or official data-production source (with a designated mission statement, source, or product), which publishes reliable and accurate data for subsequent use by customers. An ADS may be the functional combination of multiple, separate data sources.
Business and functional process improvement	A systematic, disciplined improvement approach that critically examines, rethinks, and redesigns mission-delivery processes in order to achieve improvements in performance in areas important to customers and stakeholders. (See also DoDD 8000.01.)
Business enterprise architecture	The EA for DoD's business information infrastructure; includes processes, data, data standards, business rules, operating requirements, and information exchanges. The BEA serves as the blueprint to ensure the right capabilities, resources, and materiel are rapidly delivered to Warfighters by ensuring accurate, reliable, timely, and compliant information across DoD.
Capability	In the context of the AEA framework, a capability satisfies a requirement, specifically an IT requirement. For example, an Army headquarters element has the requirement to know the location of all friendly and enemy units in its area of operations. Situational awareness is the capability that satisfies this requirement. The ability to achieve a Desired Effect under specified [performance] standards and conditions through combinations of ways and means [activities and resources] to perform a set of activities.

Name	Description
Capital Planning and Investment Management	The CPIM process is to develop C4/IT investment policy and strategic direction that informs Army leaders and directly impacts their POM decisions on all C4/IT expenditures across all functional domains. The CPIM process is collaborative among C4/IT stakeholders, with a focus on C4/IT across the Army (to include all functional domains) throughout the life cycle of IT expenditures and the management of IT assets.
Command, control, communications, and computer systems	The source document that defines the Army Enterprise baseline and mission IT services provided or supported by the NEC. This list of service definitions is the foundation for the development and publishing of the customer-facing LandWarNet services catalog. The C4IM services listed as baseline are core or common user services that are the responsibility of the Army to centrally fund. Those services listed as "Mission" are the responsibility of the ACOMs/ Mission Commanders to resource. These services are not in the baseline, but are required based on the mission (for example, cell phones, pagers, personal digital assistants) and are grounded by the business processes that enable mission execution in a more efficient and effective manner. Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications.
Command, control, communications, and computers for information management services list	The source document that defines the Army Enterprise baseline and mission IT services provided or supported by the NEC. This list of service definitions is the foundation for the development and publishing of the customer-facing LandWarNet services catalog. The C4IM services listed as baseline are core or common user services that are the responsibility of the Army to centrally fund. Those services listed as "Mission" are the responsibility of the ACOMs/ Mission Commanders to resource. These services are not in the baseline, but are required based on the mission (for example, cell phones, pagers, personal digital assistants) and are grounded by the business processes that enable mission execution in a more efficient and effective manner.
Communications	See telecommunications.
Communications network	A set of products, concepts, and services that enables the connection of computer systems for the purpose of transmitting data and other forms (for example, voice and video) among the systems.

Name	Description
Communications security	Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material.
Communications systems	A set of assets (transmission media, switching nodes, interfaces, and control devices) that establishes linkage between users and devices.
Communities of interest	The inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes; and who therefore must have a shared vocabulary for the information they exchange.
Community of practice	A community of practice (CoP) is a group of people who regularly interact to collectively learn, solve problems, build skills and competencies, and develop best practices around a shared concern, goal, mission, set of problems, or work practice. CoPs cut across formal organizational structures and increase individual and organizational agility and responsiveness by enabling faster learning, problem solving, and competence building; greater reach to expertise across the force; and quicker development and diffusion of best practices. CoP structures range from informal to formal and may also be referred to as structured professional forums, knowledge networks, or collaborative environments.
Compatibility	The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference.
Compliance	A system that meets, or is implementing an approved plan to meet, all applicable TA mandates.
Configuration	An expression in functional terms (that is, expected performance) and physical terms (that is, appearance and composition).
Context	The interrelated conditions that compose the setting in which the Architectures exist. It includes environment, doctrine, and tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions.

Name	Description
Cost-effective	Describes the course of action that meets the stated requirement in the least-costly method. Cost-effectiveness does not imply a cost savings over the existing or baseline situation; rather, it indicates a cost savings over any viable alternative to attain the objective.
Data	The representation of facts, concepts, or instructions in a formal manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations, such as characters or analog quantities to which meaning is, or might be, assigned (see JP 1–02).
Data element	A basic information unit template that is built on standard semantics and structures, and that in turn governs the distinct values of one or more columns of data within a row of data within a database table or a field within a file.
Data management	The process of creating a basis for posting, sorting, identifying, and organizing vast quantities of data available to DoD
Data model	A graphical and textual representation of data needed by an organization to represent achievement of its mission, functions, goals, objectives, and strategies. A data model is represented by its entities, attributes, and relationships among its entities. In the relational model of data, entities are tables, attributes are columns, and relationships are primary and foreign key pairs. Data models may be enriched beyond data structures with both constraints and embedded processes.
Data performance plan	An organized and structured approach to the specification and collection of enterprise artifacts in support of COI objectives, and operate in a common and shared fashion. Data performance planning collects, develops, and maintains these artifacts and is of primary interest to information system professionals charged with ensuring that information systems meet the needs of the COI. These artifacts are often referred to as "metadata."
Data standards	Metadata expressed as ADSs, IESS, UIDs, and XML, and used to guide all data exchanges including those with legacy systems.
Data steward	A subject-matter expert who is under the direction of the Chief Data Officer and is responsible for developing, implementing , and enforcing Federal, Army, and the irrespective organization’s data standards, processes, and procedures.

Name	Description
Defense Business System	An information system other than a national security system operated by, for, or on behalf of the DoD. Includes financial systems, mixed systems, financial data feeder systems, and information technology and information assurance infrastructure used to support business activities, such as acquisition, financial management, logistics, strategic planning and budgeting, installations and environment, and human resource management. This includes any IT that supports generating force functions as outlined in FM 1–01 or performs functions that can be mapped to the BEA.
Desired Effect	The result, outcome, or consequence of an action [activity].
Direct-reporting unit	An operational command that reports to and is under the direct supervision of an HQDA element. A DRU executes its unique mission based upon policy established by its HQDA principal.
Domain	An area of common operational and functional requirements. The four domains are C4I, weapon systems, modeling and simulation, and sustainment.
Domain Information	Types of information within the scope or domain of the architecture.
End-to-End (E2E) process	USACE end-to-end business processes (E2E BPs) are composed of the interactions and interrelationships of activities that are carried out to provide products and services to USACE customers, thereby accomplishing USACE missions. They are cross-functional (and possibly multi-echelon) and deliver USACE business outputs. Generally the same customer or stakeholder provides inputs to the business and receive outputs from the business. (CPIM OPORD) The DoD E2E has five levels. Levels 0, 1 and 2 are generic to all organizations within the DoD. Levels 3 and 4 are organization specific, where Level 3 represents the specific type of business activity being performed by a given organization and Level 4 represents how that organization performs those business activities in a given business system environment. A term used in many business arenas referring to the beginning and end points of a method or service.
Enterprise	The highest level in an organization; it includes all missions, tasks, and activities or functions.

Name	Description
Enterprise architecture	A strategic information asset base, that defines the mission, information, and technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs. An EA includes a baseline architecture, a target architecture, and a sequencing plan (see 44 USC 3601).
Enterprise authoritative data source registry	An enterprise capability that enables a holistic view of DoD data sources, their relationships, and their responsible governance authorities. It is a Web-enabled interface with streamlined ADS registration and discovery capabilities that support the visibility of DoD data needs and the attribution of those needs to one or more authoritative bodies responsible for meeting or otherwise fulfilling those needs. For more information, see https://metadata.ces.mil.
Enterprise data	Data shared across systems, applications, and processes by organizations, branches, divisions, and other sub-units in the enterprise.
Enterprise information environment	The common, integrated computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, or assure, LANs, campus-area networks, tactical networks, operational-area networks, metropolitan-area networks and wide-area networks. The EIE is also composed of GIG organizational, regional, or global-computing capabilities. The EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the GIG. The EIE included a common set of enterprise services, called Core Enterprise Services, which provide awareness, and delivery of information on the GIG. area.

Name	Description
Enterprise network	The connection of all components, departments, organizations, and locations into a single standardized, compatible, interoperable, and secure intra-Army network. The single intra-Army network (Army enterprise network) integrates all systems in the Army (and all systems outside the Army requiring data exchange with the Army) to provide seamless information superiority that supports the Army's Joint, interagency, intergovernmental, multinational operations, and business missions. This translates to system-wide engineering, common strategy and architecture, and a single concept of operation and authority for network operations. The Army's enterprise is prescribed by the Army CIO. Enterprise network operations are under the single authority of Army Cyber Command.
Environment	The conditions (physical, political, economic, and so on) within which an architectural configuration must operate.
Exhibit documents	Exhibit 53s and 300s are reporting requirements established by the Office of Management and Budgets for an agency's IT investment portfolio.
Facility	A real property entity consisting of underlying land and one or more of the following: a building, a structure (including linear structures), a utility system, or pavement.
Federated architecture	An approach for EA development, which is comprised of a set of coherent but distinct entities or architectures, or the architectures of separate members of the federation. The members of the federation participate to produce interoperable, effectively integrated EA. The federation sets the overarching rules of the federated architecture, defining the policies, practices, and legislation to be followed; as well as the inter-federated procedures and processes, date interchanges, and interface standards to be observed by all members of the federation. Each federation member conforms to the enterprise view and overarching rules of the federation in developing its architecture. Internal to themselves, each focuses on their separate mission and the architecture that supports that mission.
Function	Within the context of the AEA framework, a synonym for activity.

Name	Description
Functional proponent	Commander or chief of an organization or staff element that is the operative agency charged with the accomplishment of a particular function(s) (see AR 5–22).
Functional Standard	Functional standards set forth rules, conditions, guidelines, and characteristics.
Guidance	An authoritative statement intended to lead or steer the execution of actions.
Information	Any communication or representation of knowledge, such as facts, data, or opinion; in any medium or form including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. Information is the state of a something of interest that is materialized -- in any medium or form -- and communicated or received.
Information enterprise	The holistic, end-to-end approach of a variety of IT activities and tasks, which include infrastructure management, DM, networking, system engineering, database and software design and management, and the administration of entire systems resulting in an Armywide capability that covers the entire life cycle of information and knowledge. IE includes matters involving information technology, network defense, and network operations contributing to the Army’s LandWarNet and DOD GIG. The Army’s IE is the core domain of the Army CIO/G–6, which includes the people, processes, and technology that resource and deliver IT services and support Armywide.
Information management	Planning, budgeting, manipulating, and controlling information throughout its life cycle.
Information requirement	The expression of need for data or information to carry out specified and authorized functions or management purposes that require the establishment or maintenance of forms or formats, or reporting or recordkeeping systems, whether manual or automated.

Name	Description
Information resources management	The planning, budgeting, organizing, directing, training, promoting, controlling, and management activities associated with the burden, collection, creation, maintenance, utilization, dissemination, and disposition of information, regardless of media. Includes the management of information and information-related resources and systems, whether manual or automated, such as records management activities, privacy and security of records, agency sharing and dissemination of information; and the acquisition and use of automatic data processing, telecommunications, and other IT.
Information system	The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. For the purposes of APMS, the terms "application" and "information system" are both IT investments describing a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (see JP 1–02).The application of IT to solve a business or operational (tactical) problem creates an information system.
Information technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used directly or is used by a contractor under a contract with the executive agency, which 1) requires the use of such equipment; or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" also includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. (Reference 40 USC Subtitle III (Clinger-Cohen Act of 1996).)

Name	Description
Information technology architecture	An integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the agency’s strategic and information resources management goals.
Information technology portfolio	A grouping of IT capabilities, systems, services, systems support services (for example, IT required to support and maintain systems), management, and related investments required to accomplish a specific functional goal.
Infrastructure	The shared computers, ancillary equipment, software, firmware, and similar procedures; and services, people, business processes, facilities (such as building infrastructure elements) and related resources used in the acquisition, storage, manipulation, protection, management, movement, control, display, switching, interchange, transmission, or reception of data or information in any format (including audio, video, imagery, or data) whether supporting IT or national security systems as defined in the CCA.
Installation	A base, camp, post, station, yard, center, or other activity, including leased facilities, without regard to the duration of operational control. An installation may include one or more sites.
Integration	The process of making or completing, by adding or fitting together into an agreed framework (architecture), the information requirements, data, applications, hardware, and systems software required to support the Army in peace, transition, and conflict.
Integrity (of information)	Assurance of protection from unauthorized change.
Interoperability	The ability of two or more systems, units, forces, or physical components to exchange and use information. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily.
Investment Review Board	Working level committee that evaluates IT investments and provides recommendations including authority levels to the Executive Investment Review Board.
Life cycle	The total phases that an item progresses through from the time it is initially developed until the time it is either consumed, in use, or disposed of as being excess.
Mission	A group of tasks and their respective purposes, which are assigned to military organizations, units, or individuals for

Name	Description
	execution.
Mission area	A defined area of responsibility with functions and processes that contribute to mission accomplishment.
Networthiness	Risk management accomplished through the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the Army enterprise.
Objectives	Quantified goals identifying performance measures that strive to improve the effectiveness or efficiency of agency programs in support of mission goals.
Operational architecture	Descriptions of the tasks, operational elements, and information flows required to accomplish or support a function.
Operational requirement	A formally established, validated, and justified need for the allocation of resources to achieve a capability to accomplish approved military objectives, missions, or tasks.
Operational view (architecture)	A description (often graphic) of the operational elements, assigned tasks, and information flows required to accomplish or support a warfighting function. OV defines the type of information, frequency of exchange, and tasks supported by these information exchanges.
Organization	A specific real-world assemblage of people and other resources organized for an on-going purpose.
Organizational Measure	A category of quality measures that address how costly a Performer is to operate and maintain.
Performance management	The use of performance measurement information to help set agreed-upon performance goals, allocate and prioritize resources, inform managers to either confirm or change current policy or program directions to meet goals, and report on the success in meeting goals.
Performance Measure	A category of quality measures that address how well a Performer meets Capability needs.
Performer	Any entity - human, automated, or any aggregation of human and/or automated - that performs an activity and provides a capability.
Planning, programming, budgeting, and execution	The process for justifying, acquiring, allocating, and tracking resources in support of Army missions.

Name	Description
process	
Platform information technology	Refers to computer resources, both hardware and software, which are physically a part of, dedicated to, or essential in real time to the mission performance of special-purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility-distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.).
Portfolio management	The management of selected groupings of IT investments using integrated strategic planning, integrated architectures, performance measures, risk management techniques, transition plans, and portfolio investment strategies. The core activities associated with PfM are binning, criteria development, analysis, selection, control, and evaluation.
Portfolio Owner	Chair of the Investment Review Board.
Portfolio Manager	Member of the CECI staff who works to support the portfolio owner and acts as the secretariat for the IRBs.
Process	A group of logically related decisions and activities required to manage the resources of the Army. A business process is a specific ordering of work activities across time and place, which also has a beginning, an end, and clearly defined inputs and outputs that deliver value to customers.
Process owners	HQDA functional proponents, ACOMs, and others who have responsibility for any mission-related or administrative work process.
Program Manager (PgM)	An individual appointed in writing by the Investment Sponsor who is responsible for providing oversight to Project Managers for related IT investments.

Name	Description
Project	A temporary endeavor undertaken to create Resources or Desired Effects.
Project Manager (PM)	The individual appointed in writing by the Investment Sponsor who is responsible for the delivery of agreed upon deliverables to the IT Investment Sponsor. A manager responsible for the resources provided and for the execution of the approved project management plan with cost, schedule and performance goals.
Proponent	An Army organization or staff that has been assigned primary responsibility for materiel or subject matter in its area of interest.
Record	All books, papers, maps, photographs, machine readable items (such as, disks, tapes, cards, printouts, aperture cards, roll microfilm, microfiche, laser disk, optical disk, optical card, other optical-recording media, film slides, transparencies, or other documentary materials regardless of physical form or characteristics) made or received by any entity of the DA as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities because of the informational value of the data.
Records management	The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with information creation, information maintenance and use, and information disposition in order to achieve adequate and proper documentation of the policies, transactions, and effective and economical management of DA operations.
Records management program	A program that includes elements concerned with the life-cycle management of information, regardless of media. Specific elements include the management of correspondence, reports, forms, directives and publications, mail, distribution, maintenance (use and disposition of recorded information), declassification of recorded information, and the implementation of responsibilities under the Freedom of Information Act and Privacy Act.
Resource	Data, Information, Performers, Materiel, or Personnel Types that are produced or consumed.
Rule	A principle or condition that governs behavior; a prescribed guide for conduct or action

Name	Description
Service	A mechanism to enable access to a set of one or more capabilities , where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description. The mechanism is a Performer. The “capabilities” accessed are Resources -- Information, Data, Materiel, Performers, and Geo-political Extents.
Service Channel	A logical or physical communication path between requisitions and services.
Service Description	Information necessary to interact with the service in such terms as the service inputs, outputs, and associated semantics. The service description also conveys what is accomplished when the service is invoked and the conditions for using the service.
Service Level	A measurement of the performance of a system or service.
Service level agreement	A formal agreement between the customer(s) and the service provider specifying service levels and the terms under which a service or a package of services is provided to the customer.
Standard	Within the context of the AEA, a document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. A standard may also establish requirements for the selection, application, and design criteria for materiel. A formal agreement documenting generally accepted specifications or criteria for products, processes, procedures, policies, systems, and/or personnel.
Standards view (architecture)	The standards view is the set of rules governing the arrangement, interaction, and interdependence of parts or elements of the architecture description.
Strategic planning	A continuous and systematic process whereby guiding members of an organization make decisions about the organization’s future, develop the necessary procedures and operations to achieve that future, and determine how success is to be measured.

Name	Description
System	An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions (see JP 1–02). Within the context of the AEA, systems are people, machines, and methods organized to accomplish a set of specific functions; provide a capability or satisfy a stated need or objective; or produce, use, transform, or exchange information. For the purpose of reporting to the Army Information Technology Registry, the terms "application" and "system" are used synonymously–a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (for example, the application of IT).
System	A functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements.
System owner	The system proponent and the agency or organization that establishes the need for the IT system. Develops requirements, provides funding, designates who will manage data entry, and aligns requirements with APMS standards.
System view (architecture)	A description, including graphics, of systems and interconnections, providing for or supporting warfighting functions. The system view defines the physical connection, location, and identification of key nodes, circuits, networks, and warfighting platforms, and specifies system and component-performance parameters. It shows how multiple systems within a subject area link and interoperate and may describe the internal construction or operations of particular systems.
Systems architect	Responsible for the integration and oversight of architecture for IT and NSS from a systems perspective.
Systems architecture	Descriptions, including graphics, for systems and interconnections providing for or supporting functions.
Task	A discrete event or action that is unspecific to a single unit, weapon system, or individual; and that enables a mission or function to be accomplished by individuals or organizations.
Technical architecture	The technical architecture provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed.

Name	Description
Technical Standard	Technical standards document specific technical methodologies and practices to design and implement.
The Army Plan	This plan is a 16-year strategic planning horizon that includes the 6-year span of the program, plus an additional 10 years. The Army Plan presents comprehensive and cohesive strategic, midterm planning and programming guidance that addresses the Army's enduring core competencies over this time period.
Thin client	The use of client-server architecture network that depend primarily upon the central server for processing activities that focus on conveying input and output between the user and the remote server. In contrast, a thick or fat client does as much processing as possible and passes only data for communications and storage to the server. Many thin client devices run only Web browsers or remote desktop software, which means that all significant processing occurs on the server.

“This Page Intentionally Left Blank”

APPENDIX D

Templates/Examples

I. System Diagram

Requirements for a System Diagram are:

a. Display Internal/external interface connections

b. Number of databases/data stores

c. Locations of components

d. Firewall/DMZ boundaries

Example System Diagram # 1: WAMAS System Diagram

The figure below illustrates how the system interfaces with the users. The system is housed in the Western Processing Center (WPC) of the USACE. It inherits the network security implemented within the USACE. The Warrant Management System is made available only within the USACE network. All users accessing this system from the USACE network can access through the web browser provided they have authority to access this system. The users outside the USACE network are not permitted to access this system i.e. user must have USACE network account to access this system. If a user needs to access this system from outside the USACE network, the user first needs to get into the USACE network through secured VPN.

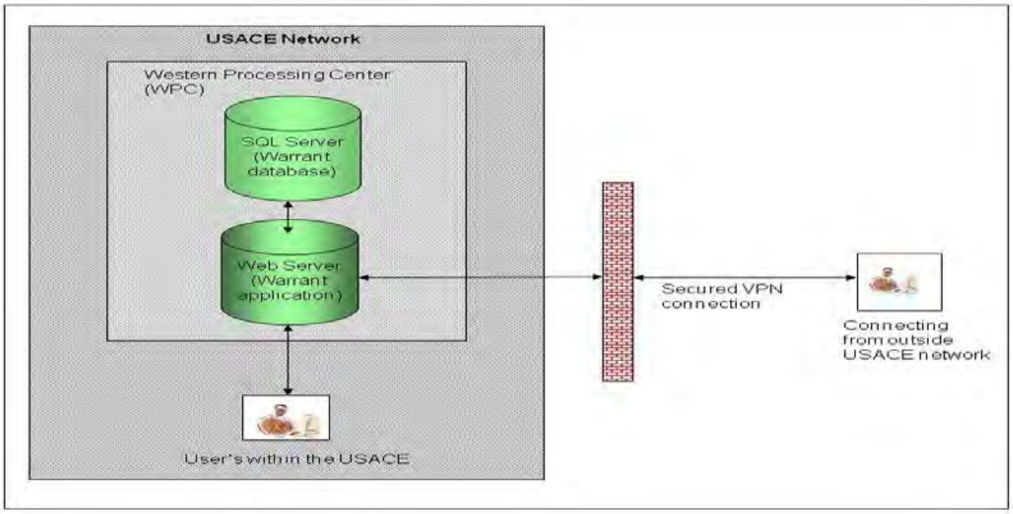

USACE Network
Western Processing Center (WPC)
SQL Server (Warrant database)
Web Server (Warrant application)
User's within the USACE
Secured VPN connection
Connecting from outside USACE network

Figure D-1 WAMAS System Diagram

Example System Diagram # 2: P2 System Diagram

The P2 system is an information system used to manage projects/programs within USACE core mission areas: military, civil works, research and development and environmental. P2 provides the following capabilities:

1. Project modeling --Work Breakdown Structures (WBS), WBS codes, calendars

2. Activity modeling (schedules, task dependencies, durations)

3. Resource and cost management (resource estimates, labor/non-labor) Project status/controls (resource leveling, earned value, % complete)

The P2 product stack also includes tools to support report generation, financial analysis, and decision support. P2 replaced legacy project management applications (e.g., P2v2); it is the sole Project Management Automated Information System (PMAIS) for the Corps.

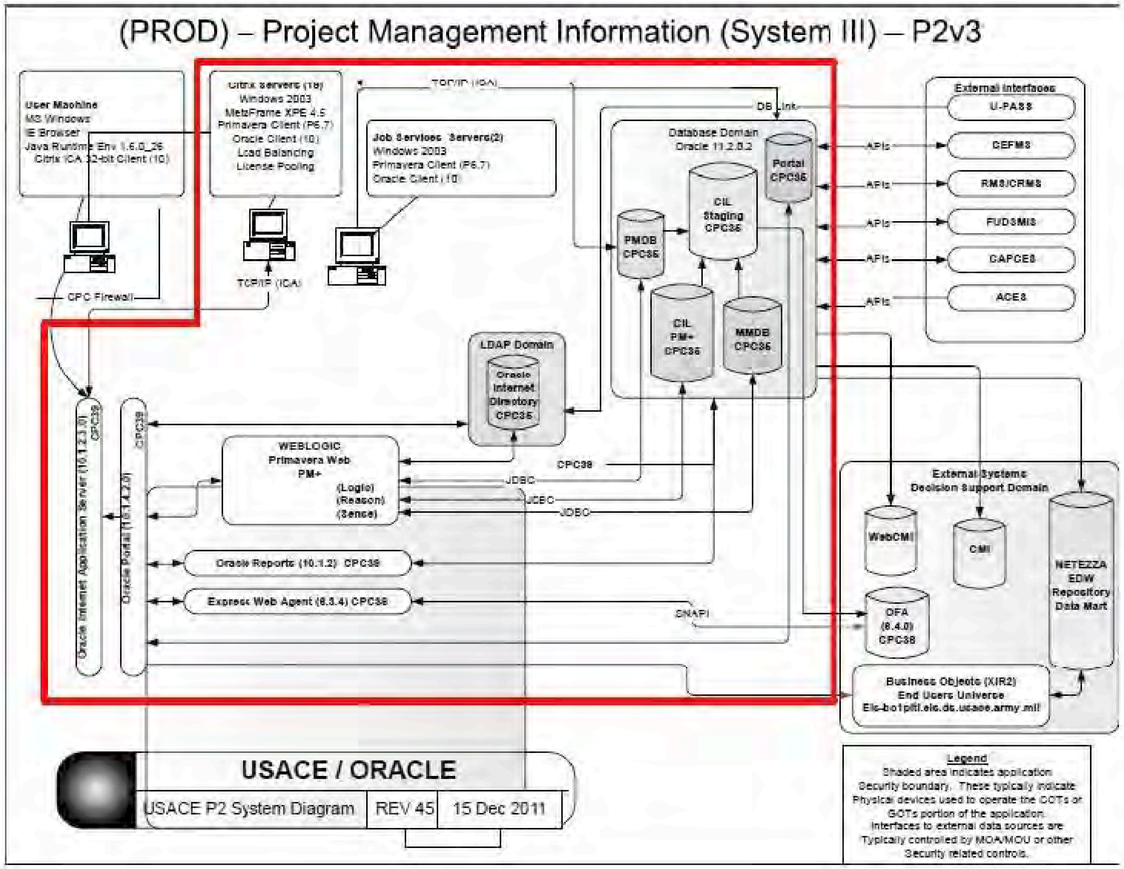


Figure D-2 P2 System Diagram

II. System Description

Requirements for System Description are:

1. Business requirements

2. Business functions provided

3. Functionality

4. End Users

5. Products

6. Strategic goals

7. End-to-End (E2E) /Business Processes supported

Generic System Description template

A concise introduction describing the business requirement(s) that are being met by the system and the problem(s) it solves. Include the strategic goals this system helps meet. (deliverables/products)

What business functions does this system perform? What E2E business processes does this system support? Who are the users of the system?

How does the system works, how does it fulfill the business requirements.

III. Technical Description

Requirements for Technical Description are:

1. Functionality

2. Interfaces

3. Standards

4. Technologies

Generic Technical Description: (How does the system work)

Introduction

Your introduction should be a concise paragraph that supplies a good sentence definition of the process to be analyzed. Like any technical document, it should state the scope and purpose of the system/application.

Brief Description

In another brief paragraph (or possibly the same one as the introduction), answer the question, "How does it happen?" This brief description should stand alone - that is, it should not refer to details, facts, or terms that aren't explained within the summary. You will probably have an easier time writing this section if you save it until you have written out the complete description. Conclude this section by breaking the process up into stages: "The principle stages of writing process are planning, drafting, revising, and proofreading." Then, focus on each step in turn.

Step-by-step Description

For each step in your description, write a miniature process description:

1. define the step

2. state its purpose (or function within the process)

3. providing the necessary context

4. technologies and standards used

5. include brief mechanism descriptions for any components that may be involved

Conclusion

Without being excessively redundant, review the major steps in the process. Walk the reader through one complete cycle, emphasizing how the completion of each stage contributes to the final overall effect.

IV. Interface Description

Requirements for Interface Description are:

1. Interface type/protocols

2. Originator/receiver

3. Data elements

4. Use of data

Example System Description: Generic Interface Description template

Interface description provides information relevant to each interface a system has with other systems. It details the reason for the interface and how it is required to be used.

			Interface Description Template	
Initiator (System)	Push/ Pull	Responding (System)	Port id/Protocol	Data Usage Description
				Data usage description, why does the receiving system need the information and what is it going to do with it.
EDW	Pull	CEFMS	Port number(id), TCP/IP	Calculate cost
EDW				

Table D-1 System Interface Description Template

V. Logical Data Model Description

Example Logical Data Model

Enterprise Data Architecture
Logical Data Model Example

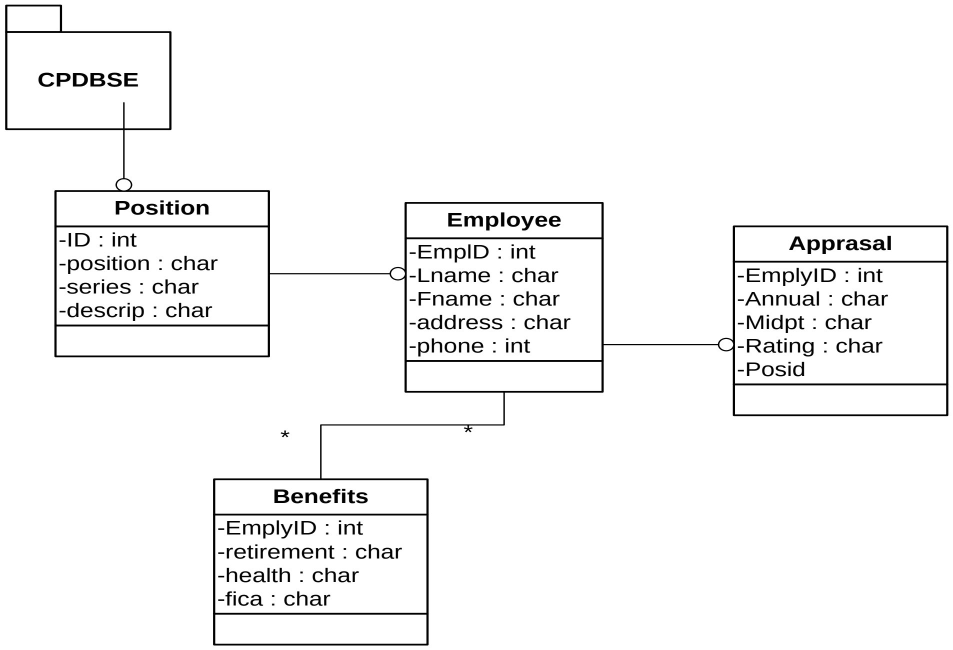


Figure D-3 Logical Data Model (Entry Relationship Diagram – ERD)

VI. Data Dictionary

Example Data Dictionary

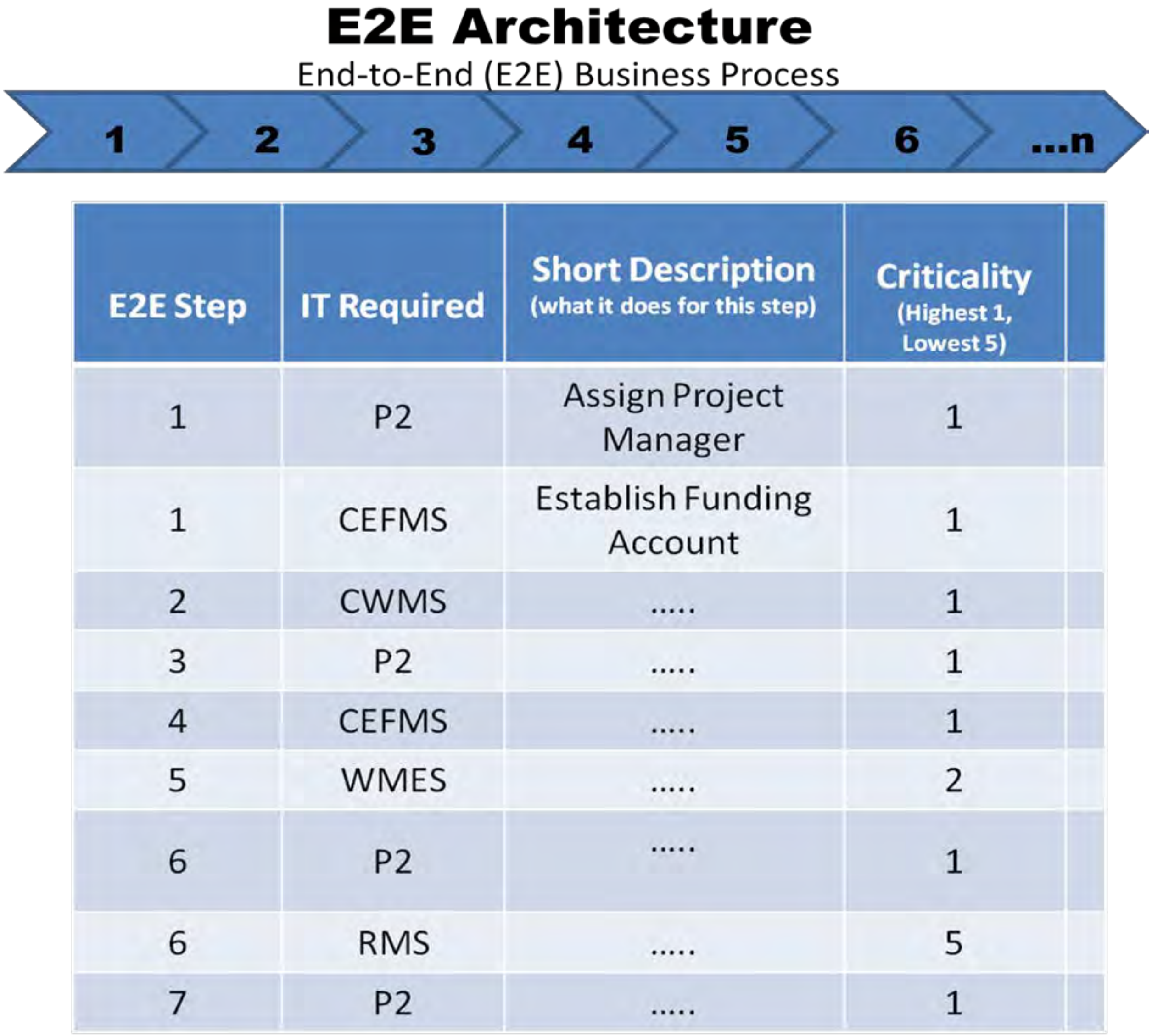
Enterprise Architecture Data Dictionary Template				
System name	Field name	Field description	char type (alpha or num)	length

Table D-2 Data Dictionary

VII. End-to-End Business Process mapping to Business Systems

Example mapping of Business system to Business processes

E2E architectures are tabular depictions that contain portfolio mission related business processes and the associated IT investments. The E2E architecture will map the required IT to the individual steps of the process and explain what function the IT is performing at this step and its criticality to the process.



E2E Architecture

End-to-End (E2E) Business Process

E2E Step	IT Required	Short Description (what it does for this step)	Criticality (Highest 1, Lowest 5)	
1	P2	Assign Project Manager	1	
1	CEFMS	Establish Funding Account	1	
2	CWMS	.....	1	
3	P2	.....	1	
4	CEFMS	.....	1	
5	WMES	.....	2	
6	P2	.....	1	
6	RMS	.....	5	
7	P2	.....	1	

Table D-4 E2E Architecture

VIII. System Evolution

1. Example Portfolio Evolution Roadmap – Mainframe to Federated Systems.

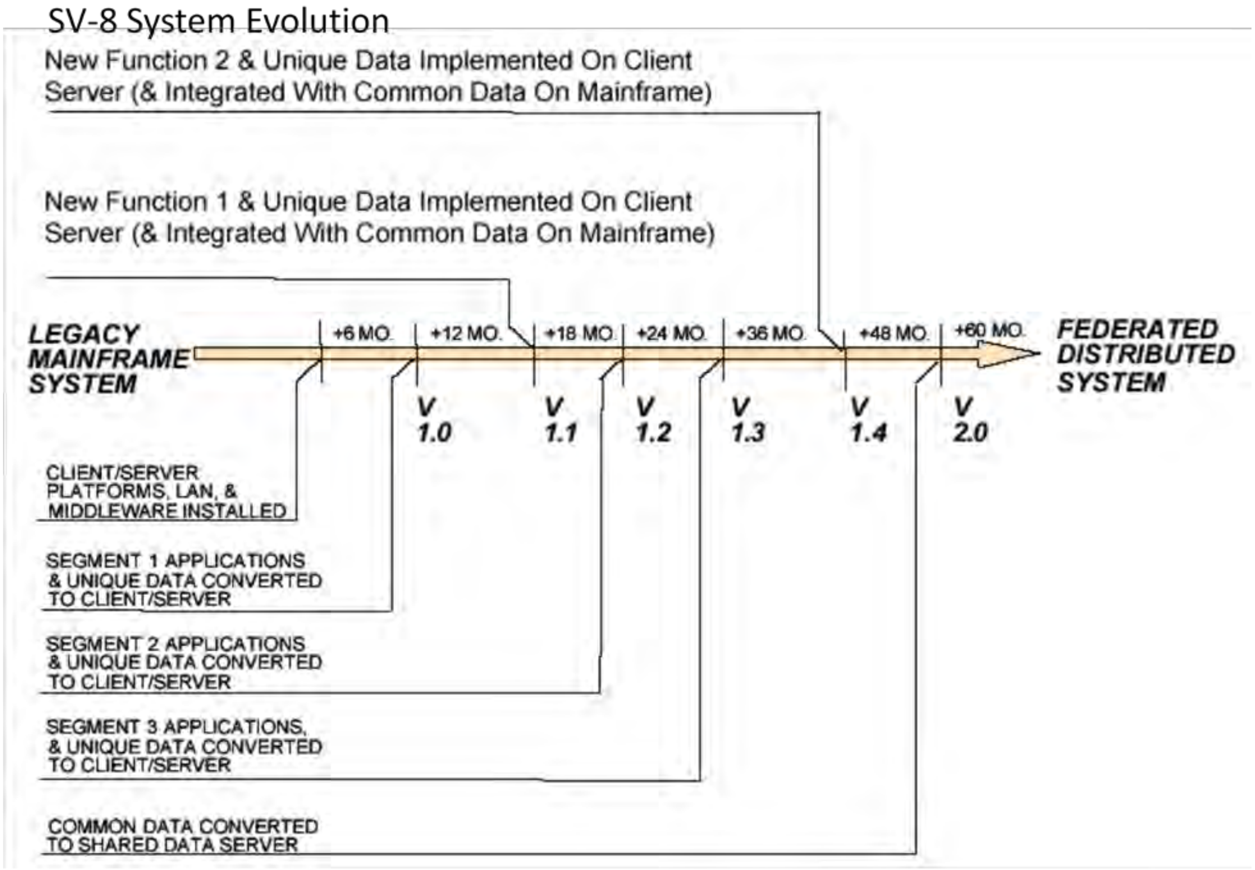

SV-8 System Evolution
New Function 2 & Unique Data Implemented On Client Server (& Integrated With Common Data On Mainframe)
New Function 1 & Unique Data Implemented On Client Server (& Integrated With Common Data On Mainframe)
LEGACY MAINFRAME SYSTEM
+6 MO.
+12 MO.
+18 MO.
+24 MO.
+36 MO.
+48 MO.
+60 MO.
FEDERATED DISTRIBUTED SYSTEM
V 1.0
V 1.1
V 1.2
V 1.3
V 1.4
V 2.0
CLIENT/SERVER PLATFORMS, LAN, & MIDDLEWARE INSTALLED
SEGMENT 1 APPLICATIONS & UNIQUE DATA CONVERTED TO CLIENT/SERVER
SEGMENT 2 APPLICATIONS & UNIQUE DATA CONVERTED TO CLIENT/SERVER
SEGMENT 3 APPLICATIONS, & UNIQUE DATA CONVERTED TO CLIENT/SERVER
COMMON DATA CONVERTED TO SHARED DATA SERVER

Figure D-5 System Evolution Graphical Description

2. Example Portfolio Evolution Roadmap –Human Resources systems

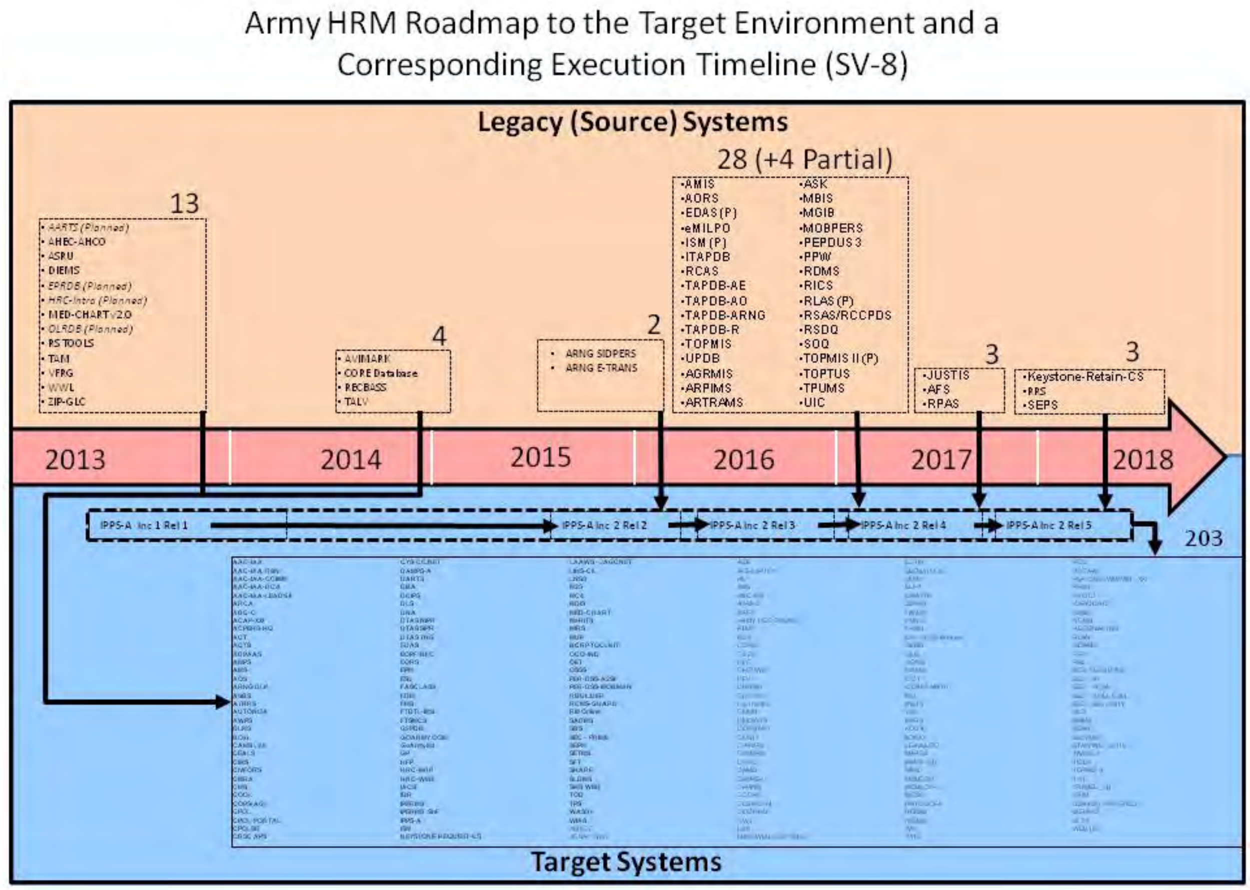
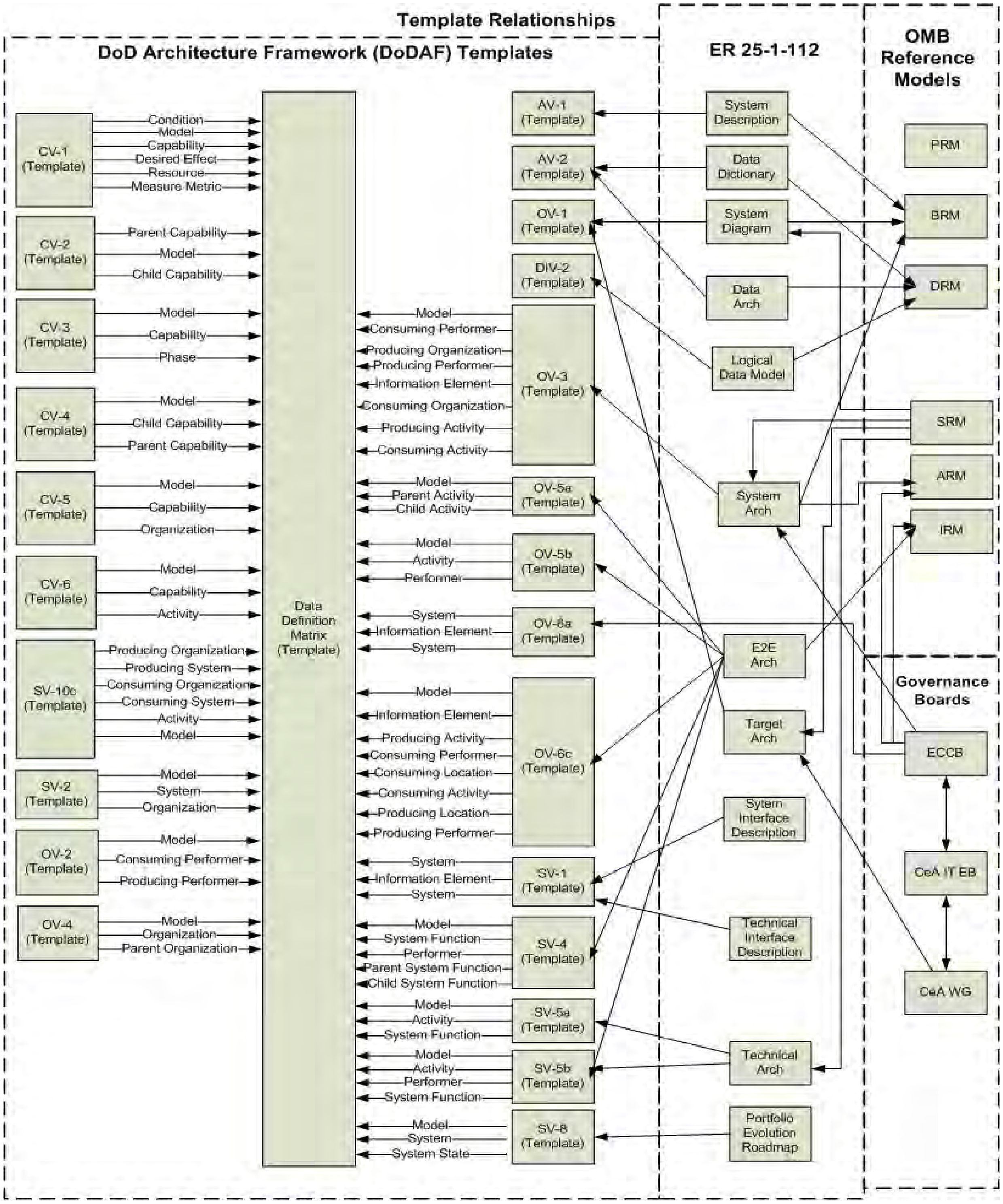


Figure D-6 System Evolution Graphical Description

APPENDIX E

Data Element Relationship



“This Page Intentionally Left Blank”