

Technical Exhibit 22

Corps Enterprise Architecture (CeA)

The purpose of this exhibit is to provide potential Service Providers insight into the scope and complexity of this mission.



US Army Corps
of Engineers®

Corps Enterprise Architecture —
May 2005



Prepared by the CeA Project Delivery Team
This Document is a Work in Progress



**US Army Corps
of Engineers®**

Corps Enterprise Architecture May 2005

Prepared by the **CeA** Project Delivery Team
This Document is a Work in Progress

Foreword

Managing our Nation's water resources; providing sustainable engineering, military construction, and environmental management; and integrating critical research and development solutions are important and complicated endeavors in the 21st century.

Clearly, the United States Army Corps of Engineers is important to America. We are unique. No other country has the capability that we bring to our citizens. Meeting sophisticated customer demands in the near future will require the highest caliber communications and collaboration throughout the organization, in tandem with our business partners.

Over the next several years, we will transform ourselves to an improved premier public engineering service by creating a virtual team that transcends organization structure and geographic boundaries. The USACE 2012 Implementation Plan will serve as the modernization blueprint for reengineering our business processes and making Information Technology (IT) investment decisions. This TWE will demand streamlined business processes and leveraging IT assets. The intent is to drive out process redundancies while encouraging us to make informed decisions about where, when, and how to invest in automated business tools.

Corps Enterprise Architecture Target 2006 provides a flexible management structure for meaningful exchange between business owners and IT professionals. This focused partnership and continued dialogue will ensure improved efficiency and serve as one more method for attaining projected, strategically derived goals and standards of product delivery to the public.

*Corps of Engineers Enterprise Architecture
Project Delivery Team*

Special Note: This Corps Enterprise Architecture document was updated on May 2005. Charts and diagrams are refreshed as necessary. Original publication date was 10 September 2003.

Table of Contents

- Foreward
- Executive Summary
- Chapter 1 – CeA Overview
- Chapter 2 – Business Reference Model (BRM)
- Chapter 3 – Performance Reference Model (PRM)
- Chapter 4 – The CeA Data and Information Reference Model
- Chapter 5 – Service Component Reference Model (SRM)
- Chapter 6 – Technical Reference Model (TRM)
- Chapter 7 – Information Assurance
- Chapter 8 – CeA Management and Maintenance

- Appendix A – Principles
- Appendix B – Communication Plan
- Appendix C – Team Members
- Appendix D – Business Functions and Subfunctions
- Appendix E – Enterprise-level IT Investments Mapped to Federal Business Functions
- Appendix F – Lines of Business Mapping to the FEA Lines of Business
- Appendix G – Functional Level ICOM
- Appendix H – Charting the Target Work Environment
- Appendix I – Performance Metrics
- Appendix J – Description of Baseline and Target Enterprise Data Environments
- Appendix K – Description of the Data Sharing Framework
- Appendix L – Detailed Description of the Data Categorization
- Appendix M – Business Reference Model
- Appendix N – Performance Reference Model
- Appendix O – Service Reference Model
- Appendix P – Technical Reference Model
- Appendix Q – Automated Information Systems (AIS)
- Appendix R – Information Assurance in the U.S. Army Corps of Engineers
- Appendix S – Federal Enterprise Architecture (FEA) Background Information
- Appendix T – CeA As-Is and To-Be Architecture Framework
- Appendix U – USACE 2012 Objective Organization
- Appendix V – Glossary

Executive Summary

The United States Army Corps of Engineers (USACE) Corps Enterprise Architecture (**CeA**) is a management tool to enhance communications between business leaders and Information Technology (IT) experts to ensure IT is effectively used to achieve current and future business needs. Specifically, the **CeA** will serve as the key to exchanging ideas, fulfilling functional requirements, and building technical solutions among business owners/managers, strategic planners, Automated Information System (AIS) developers, and the Chief Information Officer's (CIO) staff.



The main components of this architecture are the five models, (Business, Performance, etc.) or views, of the Corps and our IT and the interrelationships between the models. Each model will have a current and future state with a planned migration path to get to our target. Architecture Management and Information Assurance are also necessary components.

The approach for **CeA** is based on the Federal Enterprise Architecture Framework required by the Office of Management and Budget and generally follows the Enterprise Architecture Planning method outlined by Dr. Stephen Spewak in 1992.¹ Because of this, some aspects and terminology of the architecture such as “Value Chain” will be unfamiliar to many Corps readers.

The **CeA** collects, shares, and manages information about current (Baseline architecture) and future (Target architecture) functions, business and IT performance metrics, information and data, applications, technology, and security. With several dynamic initiatives under way (e.g., 2012), our target states will be in flux for the near future. A metaphor for this tool is to consider it an exchange where concepts and real needs will be deposited and collected, with interest, at later dates. The **CeA** Exchange therefore will contain much useful information about business and IT activities in the Baseline and Target work environments.

The **CeA** is not, however, an automated problem-solving tool. Nor is it an overarching IT governance document. Business and IT decisions will continue to be made using a wide range of methods, and rulemaking will continue to hone in on individual programmatic issues.

¹ Steven H. Spewak with Steven C. Hill. (1992). *Enterprise architecture planning: Developing a blueprint for data, applications, and technology*. John Wiley, New York.

The Project Delivery Team (PDT) that developed the **CeA** says:

*“The **CeA** is a Business Owner and IT Expert partnership established to create a focused Exchange for making informed IT asset decisions and finding best technical solutions that meet USACE Target Work Environment requirements.”*

This document serves as a high-level view of our Corps Enterprise Architecture – Target 2006. An interactive and collaborative Web site has been established to allow searching lower levels of details pertaining to the architecture. To begin using the Corps Enterprise Architecture to support your business needs, go to the **CeA** Web site at <https://cea.usace.army.mil>.

Chapter 1 – CeA Overview

1.1 CeA Components

The architectural methodology chosen for the **CeA** (Figure 1.1) is based on a set of prescribed reference models (sometimes referred to as views) that allow detailed analysis to be performed on the complex relationships between business performance and Information Technology (IT) support requirements. The five **CeA** reference models that serve as vantage points from which to conduct this relational analysis are:

- The **Performance Reference Model (PRM)**: Identifies a common set of general performance outcomes and metrics used to achieve USACE program goals and objectives. Think of this as a view of USACE Business and IT **Performance – Knowing the value of IT.**
- The **Business Reference Model (BRM)**: Describes USACE business functions and subfunctions. Think of this as a view of USACE **Business – Who we are and what we do.**
- The **Data and Information Reference Model (DRM)**: Describes the data and information that support program, support, and internal lines operations. Think of this as a view of USACE **Information – The Information we share.**
- The **Service Component Reference Model (SRM)**: Identifies and classifies horizontal and vertical IT capabilities that support business functions and subfunctions. Think of this as a view of USACE **Applications – How we get work done.**
- The **Technical Reference Model (TRM)**: Provides a hierarchical foundation to describe how technology is supporting the delivery of the application capability. Think of this as a view of USACE Information **Technology – Our business utilities and infrastructure.**

Two additional management constructs are prescribed to ensure safeguards of people/information and effective management of **CeA** resources:

- **Information Assurance**: Ensures special emphasis on safeguarding people and information in all aspects of the **CeA**. Think of this as a view of USACE **Security – keeping people and work safe.**
- **Management and Maintenance**: Provides guidance and tools that will be provided to assist users in locating and analyzing information and technical specifications. Think of this as a view of USACE **CeA Management – Our focus and style.**



Figure 1.1. **CeA** architectural methodology

1.2 CeA Value to USACE

Enterprise architecture planning and management can be a significant contributor to the corporate decision-making process. Good business management practices must ensure that IT initiatives are derived from architecture-based parameters, filters and analysis. The outcome will be improvements in IT asset management decisions and quicker response times in solving technical problems associated with Automated Information Systems (AIS) development.

The **CeA** establishes a high-level framework for information exchanges between business owners and IT specialists by identifying corporate cross-cutting business functions, data requirements, and opportunities for measuring and controlling costs and efficiencies. Examples of potential benefits that will come from developing the **CeA** are listed in Table 1.1.

Table 1.1. **CeA** Potential Benefits

Short-Term Benefit	Long-Term Benefit	Beneficiary
Enable informed decisions to be made about selecting, ranking and resourcing IT investments	Improvement to the Capital Planning and Investment Decision Process	Business Owners, Customers, Stakeholders
Analyze sources (beyond P2) for project-related data and information throughout the PMBP process	Increased accuracy and timeliness of data and information related to program and project planning	Project Managers, Business Owners, District Commanders, Senior Leaders, Project Review Boards, Customers, Stakeholders
Identify potential electronic government (e-Gov) initiatives	Leverage IT investments by collaboration with other Federal agencies	Federal Agencies, Customers, Stakeholders
Identify potential opportunities for consolidation in business processes, applications, information, or technology.	Reduce redundant IT initiatives	Business Owners, District Commanders, Senior Leaders, Project Review Boards, Customers, Stakeholders

Short-Term Benefit	Long-Term Benefit	Beneficiary
Analyze sources for data and automated processes in the pre-development stage of AIS development	Reduced time and cost to upgrade or deploy new AIS	Customers, Stakeholders, Business Owners, System Developers, CIO Staff
Standard vocabulary to articulate expectations between business owners and AIS developers	Improve communication among the business organizations and IT organizations	Business Owners, System Developers, CIO Staff
Provide architectural views that communicate the complexity of large systems	Facilitate improvements to managing extensive, complex computing environments	Business Owners, System Developers, CIO Staff
Increased focus on the strategic use of emerging technologies to better manage the enterprise information	Improved ability to consistently insert new technologies into the enterprise	Strategic Planners, Business Owners, System Developers, CIO Staff
Discover opportunities for building greater quality and flexibility into applications without increasing cost	Consolidation of applications at the functional level, providing ability to expedite integration of legacy AIS – reducing number of AISs over time	Business Owners, System Developers, CIO Staff
Effectively link information technology investments to USACE strategic goals, objectives and plans, as well as to USACE business functions	Improve consistency, accuracy, timeliness, integrity, quality, availability, access, and sharing of IT-managed information across the USACE enterprise	Strategic Planners, Business Owners, System Developers, CIO Staff, Customers, Stakeholders
Effectively link USACE business functions to other Federal Government business functions	Improve consistency, accuracy, timeliness, integrity, quality, availability, access, and sharing of IT-managed information across the Federal Government	Strategic Planners, Business Owners, System Developers, CIO Staff, Federal Agencies, Customers, Stakeholders
Make common, reliable data available for sharing throughout USACE	Faster access to information for decisions and business activities	Strategic Planners, Business Owners, System Developers, CIO Staff, Federal Agencies, Customers, Stakeholders

1.3 CeA Principles

Decisions made about USACE IT assets and initiatives have important consequences to the USACE strategic goals, particularly the “Process” goal, which challenges the organization to “operate as One Corps, regionally delivering quality goods and services.” These decisions are based on available information and sound professional guidance. Corps Enterprise Architecture (**CeA**) principles were established by the Project Delivery Team (PDT) to provide universal constraints that narrow the parameters of success in applying **CeA** concepts for aligning IT assets with business requirements. The Principles identified in Appendix A will serve as common threads throughout the development and use of the **CeA**.

Examples of **CeA** Principles include:

- The **CeA** is business driven, delineating business functions and subfunctions.
- Systems developers use the **CeA** to promote the efficiencies and effectiveness of individual IT products and services as they evolve.
- Changes to the **CeA** will include input from stakeholders to ensure improvement in work force productivity.
- New Standards are approved, controlled, planned, tested, financially justified, documented iteratively, and add value to business function.
- Structured and unstructured data are treated as a corporate resource in support of business operations.

1.4 CeA Development

The schedule for completing the **CeA**, to the point it allowed business and IT professionals to use it as a tool, was constrained to the last 6 months of FY03 (Figure 1.2). The PDT took advantage of parallel organizational and business analysis that was underway within USACE in order to use these parts for the **CeA** and prepare the FY05 budget submittal to the Office of Management and Budget (OMB).



Figure 1.2. Schedule for completing the **CeA**

1.5 Strategic Communications

The **CeA** project started with a kickoff meeting the first week of May to begin the PDT collaboration process. A series of briefings were conducted to senior Headquarters staffs at various meetings and to USACE Information Managers in June. In-Progress Review (IPR) briefings and discussions will continue with senior staff and the field as opportunities present themselves.

The **CeA** Web site (<https://cea.usace.army.mil>) will serve as the primary source for **CeA** information. See Appendix B for Strategic Communications Plan.

Primary Audiences: The following communities of practice are primary users of the **CeA** Web site:

- Business Owners
- Strategic Planners
- System Developers
- CIO Staff
- **CeA** Team Members

The PDT would hope the resounding message would be:

*“The **CeA** is an information exchange for making informed decisions and solving technical problems associated with aligning IT to business needs.”*

A **CeA** interactive Web site, <https://cea.usace.army.mil>, provides collaboration and discussion forums as a single point of entry to the **CeA** Exchange (Figure 1.3).

1.6 The CeA Project Delivery Team

A multifunctional PDT (Figure 1.4) was established to include full representation from the business community and IT experts in Headquarters and the field. The sophistication of the **CeA** requires a dedicated, diverse, and creative team. Team members have come together from diverse functional areas to contribute to goals and objectives, while applying critical thinking skills. A full list of team members is available in Appendix C. Appendices V & W provide information about contractor expertise used for **CeA** development.



Figure 1.3. CeA-interactive Web site

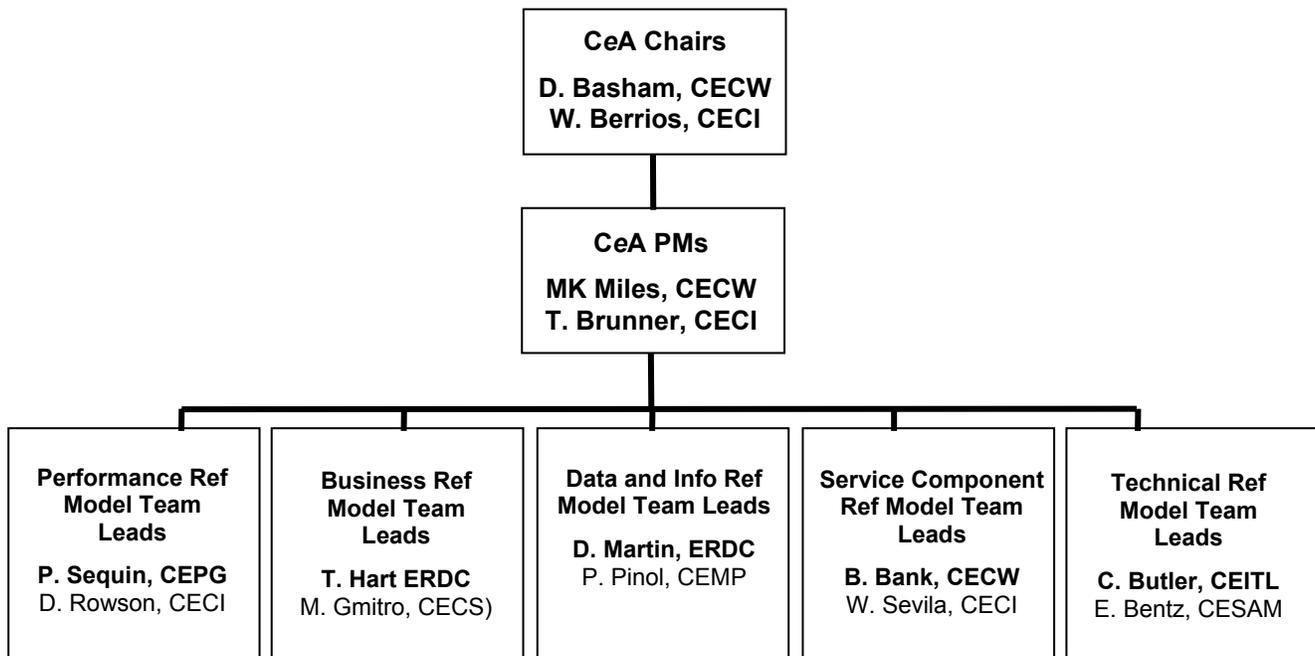


Figure 1.4. CeA PDT organization chart

1.7 Relation of CeA to the USACE Capital Planning Investment Control Process

Governance provides a formal process for defining who has the power to make technology decisions and how those decisions should be made. It addresses the problem of decision making in an environment where IT responsibilities are decentralized, and it deals with the processes needed to manage both the acceptance of the architecture and follow-up assessments and planning. A governance structure determines the responsibilities of the various parties involved in IT decision making and includes a framework for resolving disputes. It balances the common good and individual liberty by defining what is of central importance and what is local. Adherence to this principle will enable USACE to share responsibility for the deployment, operations, and management of technology with all components and stakeholders. It will also ensure business unit participation in evaluating and making IT investment decisions using consistent criteria and will maximize the use of IT resources across the enterprise. One of the main functions of the USACE **CeA**, in fact, is the support of the IT investment review process by providing an architectural framework against which all IT projects can be evaluated. The governance process provides USACE staff with the policies, procedures, and tools needed to make sound IT purchase and development decisions for the future.

It will be important for USACE to make short-term investment decisions related to activities that sustain current operations at acceptable levels (e.g., legislative mandates), while pursuing the architectural goals concurrently. Guiding principles and processes have been established to help the **CeA** Technical Architecture Working Group (TAWG) and Capital Planning Investment Control (CPIC) Committee make decisions about the necessary trade-offs and compromises when faced with mitigating circumstances, permitting progress toward the target **CeA**. Architectural Alignment and Assessment (AAA) is an integral element to keep focus on the Target Work Environment (TWE) (Figure 1.5). For additional information on the TAWG or CPIC, see the **CeA** Web site.

IT Portfolio Management

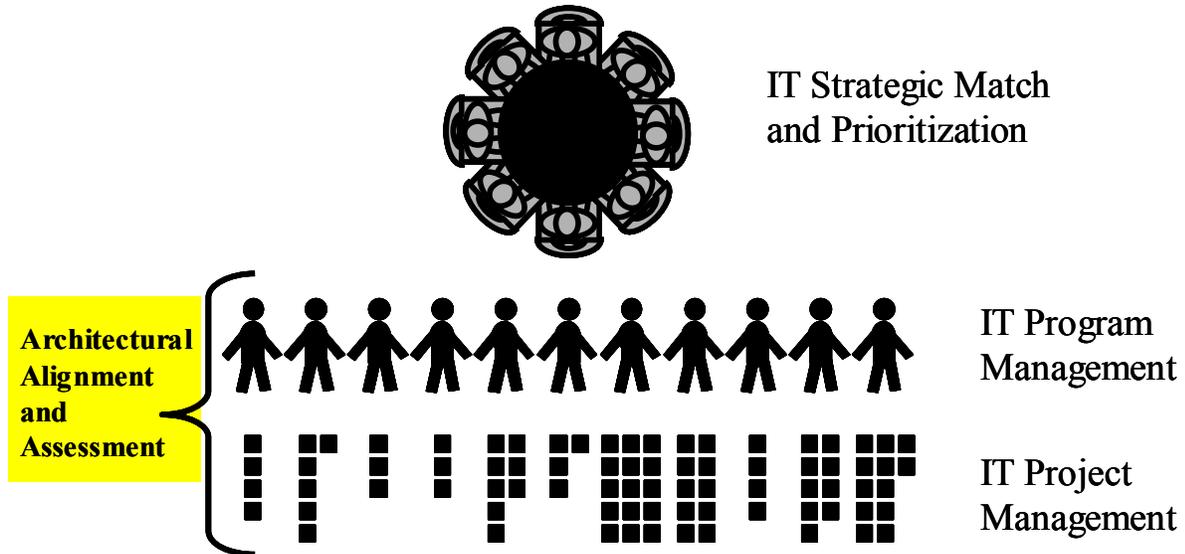


Figure 1.5. IT Portfolio Management

Chapter 2 – Business Reference Model

The **CeA** BRM is a function-driven framework for describing USACE business operations and the organizational elements that perform them. While many existing sources for information are available about



“how” (regulations and operating manuals) and “where” (formal organizational structure) work is getting done, the BRM focuses on the basic relationships between “*who we are and what we do*” with respect to the Baseline and Target work environments. The **CeA** PDT put it this way:

*“The BRM provides business owners, strategic planners, system developers and CIO staffs with an organized, hierarchical construct for exchanging critical information about the **Target Work Environment**.”*

BRM work products (Figure 2.1) should be used as reference points in motion that help to make informed choices that contribute to forward progress toward the USACE TWE. Functional and organizational information collected and sorted for example, is considered accurate without an attempt to achieve 100 percent validation from individual offices. Functions and organizations are in constant motion. The PDT felt their energy was better used in understanding the business function needs for the TWE than getting the present/past work environments 100 percent accurate. Adjusting the BRM work products, however, will be an ongoing task.

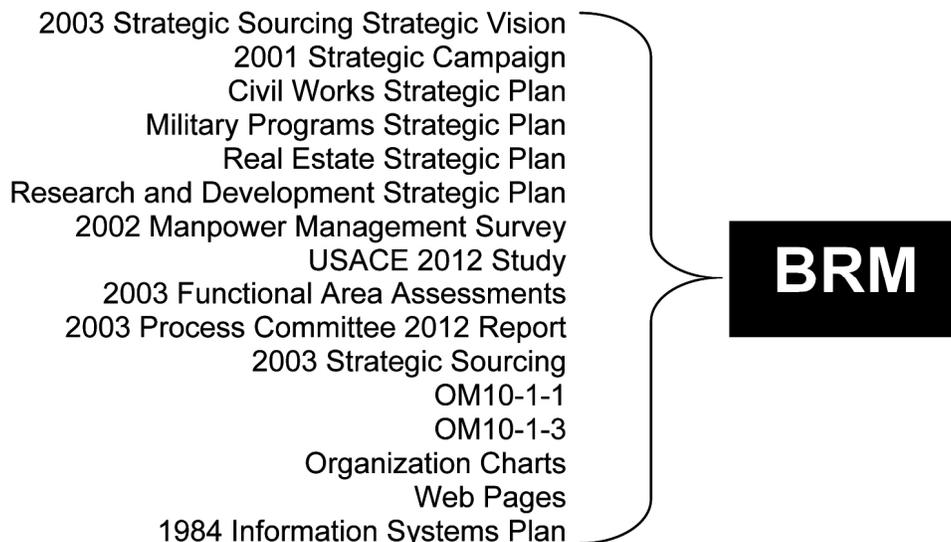


Figure 2.1. BRM work products

2.1 USACE Enterprise Statement and Value Chain

The **CeA** PDT employed a Value Chain method to ensure proper understanding of USACE business from the Washington Headquarters office to the lowest field levels. The Value Chain in Figure 2.2 depicts the relationship of the USACE Enterprise Statement (Agency Purpose), Primary Mission Areas, Core Competencies, Mission Support Functional Areas, and Internal Support Functional Areas.

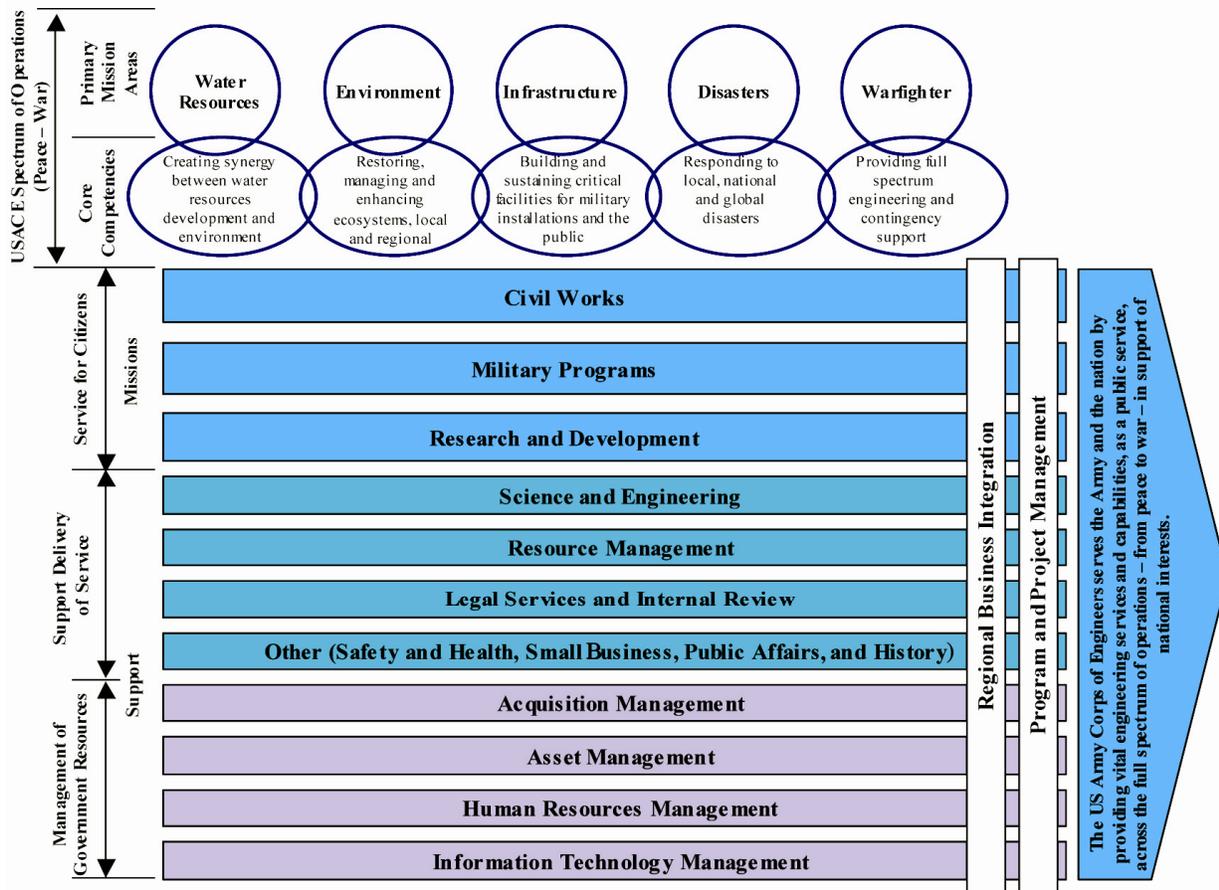


Figure 2.2. USACE Target Work Environment enterprise statement and value chain

The *Enterprise Statement* succinctly states why USACE exists. The five *Primary Mission Areas* and reinforcing *Core Competencies* speak to the assignments and capabilities that have earned USACE worldwide recognition as a premier public engineering organization. The thirteen functional areas, shown as bars on the chart, provide the foundation for understanding the TWE.

USACE **Missions** of *Civil Works*, *Military Programs*, and *Research and Development* (also considered primary functional areas) directly provide *Service for Citizens* (OMB term), which includes the delivery of citizen-focused products and services on behalf of the United States Government. The Real Estate Business Function becomes a

subfunction of Military Programs in the TWE. Two **Crosscutting Business Functions** (*Regional Business Functions* and *Program and Project Management*) are integrated throughout the other eleven business functions.

The next four Functional Areas, known as the **Support** Functional Areas, or *Support Delivery of Services* (OMB term), refer to the functions that provide the critical policy and programmatic and managerial underpinnings that facilitate USACE delivery of services to citizens.

The final four Functional Areas, known as the internal support functional areas, or *Management of Government Resources* (OMB term), encompass the activities that must be performed for USACE to operate effectively.

2.2 Business Reference Model (BRM) Components

Figure 2.3 shows the components of the BRM (see Appendix M for readable version).

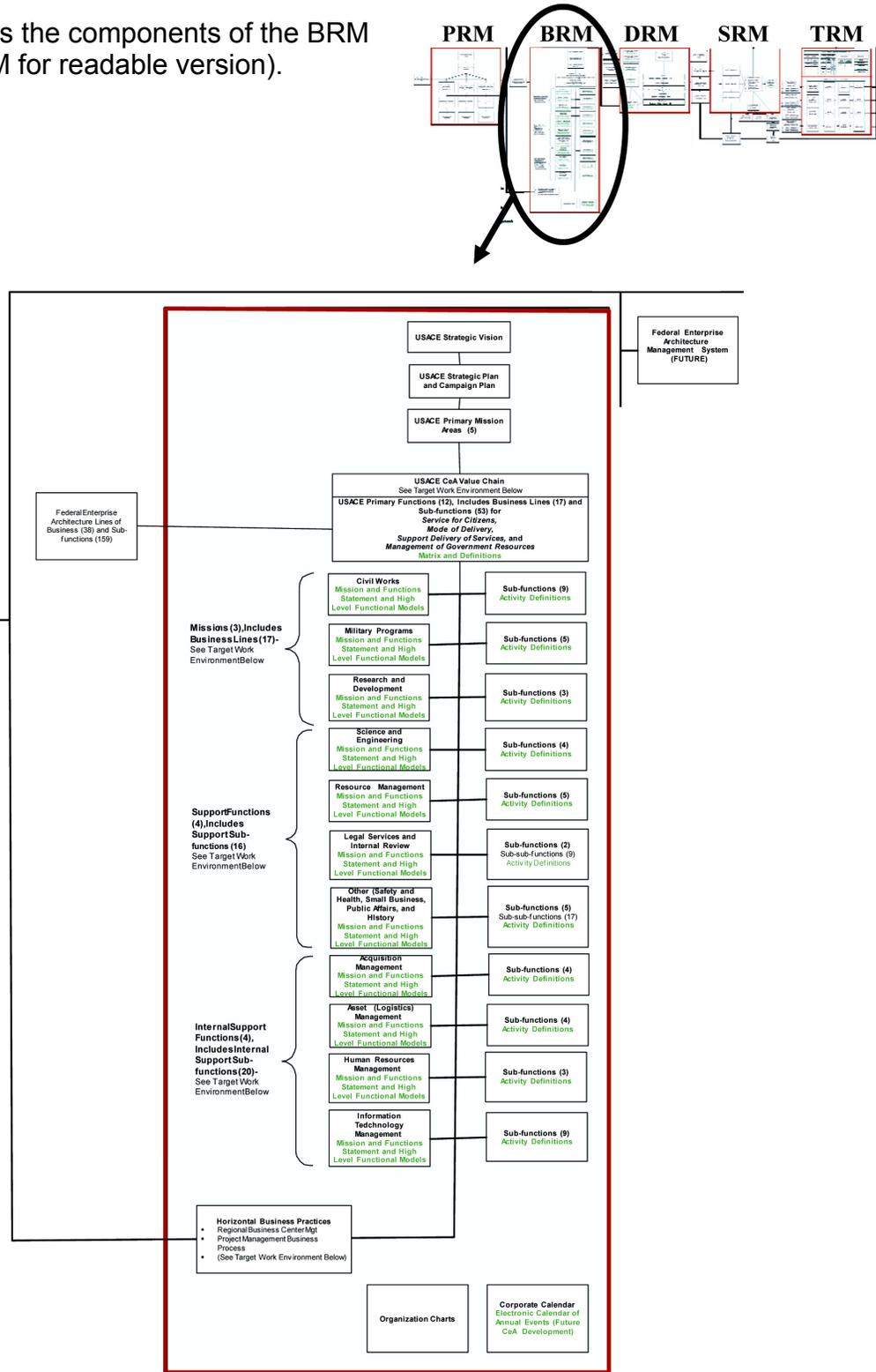


Figure 2.3. BRM components

2.3 USACE Business Functions and Subfunctions

The PDT reviewed the 39 business functions defined in the 1984 Information Systems Plan (ISP) and compared them to the information provided in the Functional Area Assessment (FAA) team, current OM 10-1-1, 2002 Manpower Management Survey, and USACE Web sites to decompose and synthesize USACE business functions and subfunctions. The Hierarchy diagram in Figure 2.4 (see Appendix D for easy-to-read version) depicts the functional decomposition of the primary business areas (2003 snapshot).

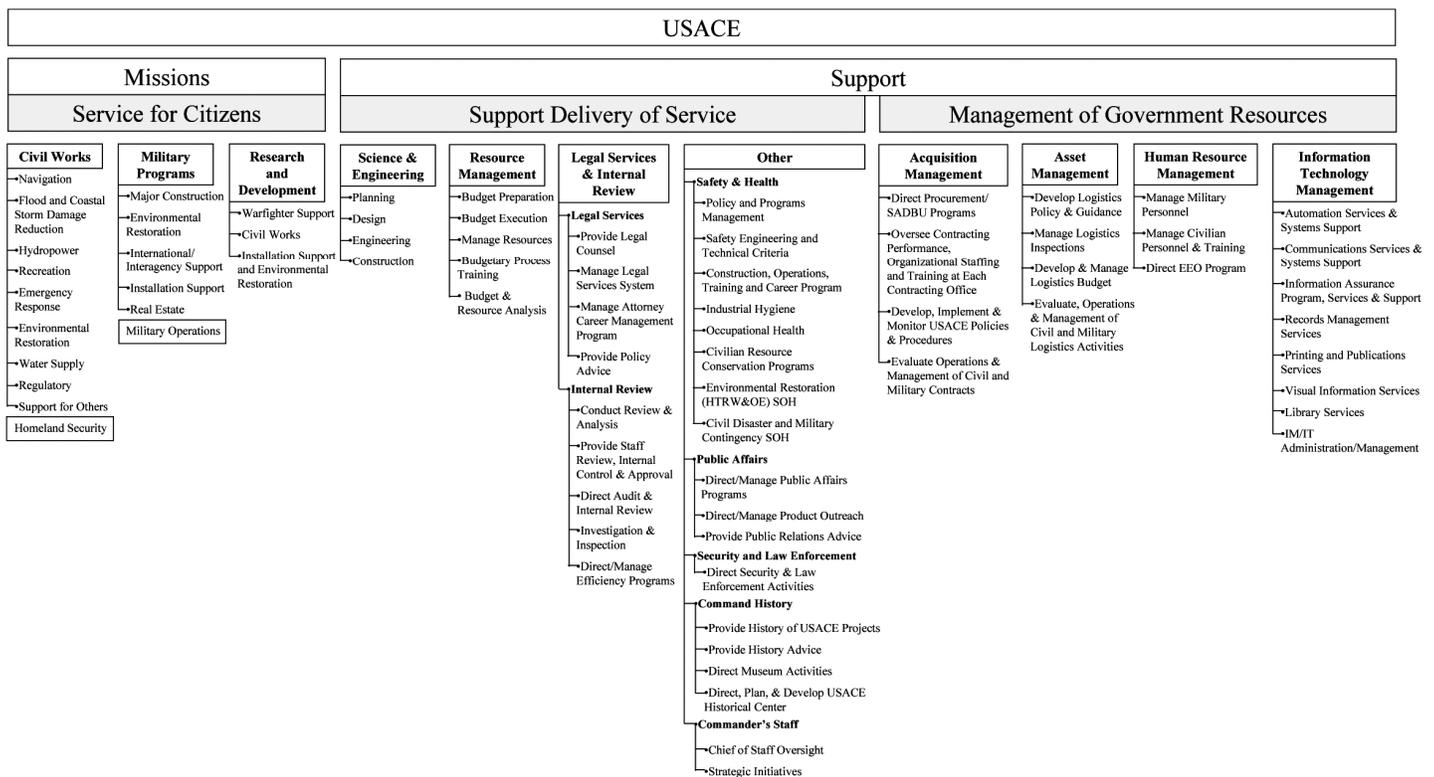


Figure 2.4. Hierarchy diagram

2.4 Understanding the Evolution of Business and Organization Structure

The USACE BRM in the TWE reflects an enterprise-centric approach to program and project management through Regional Business Centers (RBC). Civil Works, Military Programs, and Research and Development will continue to be official USACE missions (also referred to as primary business functions) as depicted in Figure 2.3. Each of these missions will additionally include Business Lines (sometimes referred to as Lines of Business) not shown in Figure 2.4. All remaining Business Functions are Support Functions (sometimes referred to as Support Services).

2.5 Articulating Future Information Technology Requirements and Migrating to the Target Work Environment (TWE)

The **CeA** PDT identified 13 business practices as expressions of end states for the TWE. These 13 end states are known directives extrapolated from the USACE vision, strategic and tactical business initiatives. The TWE end states are in alignment with the **CeA** guiding principles established as parameters for developing the evolving target architecture. Sculpting and migrating to the TWE will always be a growing and changing process. The descriptions provided here are considered high-level, minimum definitions, which are intended to provide general direction on IT investment decisions. More detailed analysis and considerations will be conducted as IT investment decisions are made at the enterprise, regional, and local levels.

2.5.1 USACE Target Work Environment

The TWE focuses on business functions and subfunctions that transcend organizational structure and work location in the future. The optimal USACE organizational structure will evolve through senior-led growth and analysis of the following seven elements: Structure, Strategy, Systems, Shared Values, Stakeholder Values, Style of Leadership, and Skills. For detailed information, refer to the discussion of the Seven S Model and the Objective Organization Design in “USACE 2012: Aligning the U.S. Army Corps of Engineers for Success in the 21st Century,” at <http://www.hq.usace.army.mil/stakeholders/Final.htm>.

The following 13 TWE end states are the linchpin to a successful **CeA**:

1. Enterprise (Corporate-level) Program Asset Management
2. Regional Watershed and Installation Management
3. Protection of USACE Military and Civil Critical Infrastructures
4. Integrated Emergency Management and Homeland Security
5. Enhanced Communications and Information Access Throughout USACE
6. Enhanced Management of Business Processes (Example: Online Applications)
7. Enterprise Management of Manpower Resources
8. Enterprise and Regional Acquisition Strategy
9. Enterprise Management of Knowledge That Includes Best Practices, Registry of Skills, Customer Feedback, Lessons Learned, Corporate Issues Management, etc.
10. Enterprise Processes to Manage Technology and Data
11. Methods for Data Exchange with Government and Industry Partners
12. Internal and External Virtual Teaming
13. One-Stop Web Access to USACE Public Information

2.5.2 CeA TWE End States and Description Summaries

2.5.2.1 Enterprise (Corporate-level) Program Asset Management

TWE Summary: Business practices in the TWE associated with *Enterprise Program Asset Management* will require IT investments that improve analytical modeling capabilities and collaboration/communications between USACE and other Federal agencies.

2.5.2.2 Regional Watershed and Installation Management

TWE Summary: Business practices in the TWE associated with *Regional Watershed and Installation Management* will require IT investments that improve USACE enterprise-level AIS interoperability, data sharing, collaboration and communications between USACE and other Federal, State, local and tribal organizations, as well as such trusted partners as universities and private industry.

2.5.2.3 Protection of USACE Civil and Military Critical Infrastructure

TWE Summary: Business practices in the TWE associated with *Protection of USACE Civil and Military Critical Infrastructure* will require IT investments that improve USACE current capabilities for Federal-level data sharing, detection, warning, alert systems, and analysis of potential terrorist attacks.

2.5.2.4 Integrated Emergency Management and Homeland Security

TWE Summary: Business practices in the TWE associated with *Integrated Emergency Management and Homeland Security* will require IT investments that improve Geographic Information Systems (GIS), cross-agency data sharing/application interoperability, mobile communications, TeleEngineering, intra-agency modeling, response simulations, and other information especially related to watersheds.

2.5.2.5 Enhanced Communications and Information Access Throughout USACE

TWE Summary: Business practices in the TWE associated with *Enhanced Communications and Information Access Throughout USACE* will require IT investments that improve enterprise-level interoperability among USACE AIS, data warehousing, data transport, collaborative tools, security, and decision support tools.

2.5.2.6 Enhanced Management of Business Processes (Example: Online Applications)

TWE Summary: Business practices in the TWE associated with *Enhanced Management of Business Processes* will require IT investments that improve AIS component-level interoperability for internal and external users (examples include single sign-on or on-line applications).

2.5.2.7 Enterprise Management of Manpower Resources

TWE Summary: Business practices in the TWE associated with *Enterprise Management of Manpower Resources* will require IT investments that ensure state-of-the-art science and engineering automated tools, standard practices, and treatment of data as a corporate asset (data warehousing) in support of virtual teaming.

2.5.2.8 Enterprise and Regional Acquisition Strategy

TWE Summary: Business practices in the TWE associated with *Enterprise and Regional Acquisition Strategy* will require IT investments that maintain and improve regional acquisition-related AIS.

2.5.2.9 Enterprise Management of Knowledge That Includes Best Practices, Registry of Skills, Customer Feedback, Lessons Learned, Corporate Issues Management, etc.

TWE Summary: Business practices in the TWE associated with *Enterprise Management of Knowledge That Includes Best Practices, Registry of Skills, Customer Feedback, Lessons Learned, Corporate Issues Management, etc.*, will require IT investments that consolidate current AIS and system components currently providing similar services.

2.5.2.10 Enterprise Processes to Manage Technology and Data

TWE Summary: Business practices in the TWE associated with *Enterprise Processes to Manage Technology and Data* will require IT investments in the IT infrastructure to bring state-of-the-art computing capabilities to the desktop, and implement a clear path to increased access/use of corporate data via shared data repositories.

2.5.2.11 Methods for Data Exchange with Government and Industry Partners

TWE Summary: Business practices in the TWE associated with *Methods for Data Exchange with Government and Industry Partners* will require IT investments that improve data collection, analysis, and dissemination for internal and external information users.

2.5.2.12 Internal and External Virtual Teaming

TWE Summary: Business practices in the TWE associated with *Internal and External Virtual Teaming* will require IT investments that promote standard science and engineering tools and processes for internal and external team members to support virtual project management.

2.5.2.13 One-Stop Web Access to USACE Public Information

TWE Summary: Business practices in the TWE associated with *One-Stop Web Access to Public Information* will require IT investments that reduce reporting burdens, streamline business transactions, and provide automated support to decision making through an aggressive migration to Web-based electronic mechanisms.

2.5.3 Prescribed IT Focus for Supporting the TWE

- Improve communications capabilities between USACE and other Federal, State, university, tribal organization, and other trusted partners.
- Improve data collection, analysis, and sharing between USACE and other Federal, State, university, tribal organization, and other trusted partners – particularly in areas of watershed management, infrastructure protection, homeland security, and GIS.
- Improve collaboration and virtual teaming capabilities – particularly in the area of science and engineering tools/practices standardization.
- Improve USACE analytical modeling capabilities.
- Improve intra-agency modeling and response simulations, especially related to watersheds.
- Bring IT infrastructure state-of-the-art computing capabilities to the desktop.
- Consolidate current USACE AIS and system components providing similar services.
- Improve enterprise-level interoperability among USACE AIS.
- Improve AIS component-level interoperability for internal and external users (examples include single sign-on or on-line applications).
- Reduce reporting burdens, streamline business transactions through an aggressive migration to Web-based electronic mechanisms.
- Improve mobile communications.
- Improve TeleEngineering capabilities.
- Provide decision support tools.
- Maintain and improve regional acquisition-related AIS.

2.5.4 Examples of Specific IT Initiatives Supporting the TWE

- Improvements in data management (standards, access, etc.).
- Select data marts warehouses (GIS, homeland security, watershed management, etc.) for internal and external access.
- Increase in Web-based collaboration tools.
- Increase in regional/national IT contracts; decrease in local IT contracts.
- AIS consolidation at system and component level (Computer-Aided Design and Drafting (CADD)/GIS, business, lessons learned, etc.).
- e-Corps (single sign-on, knowledge management horizontal portal, lessons learned, etc.).

- Standard suite of S&E tools to support virtual engineering.

2.5.5 Migration to Target Work Environment (TWE) Analysis

The Baseline Work Environment (Figure 2.5) is a snapshot taken of USACE business activity at the end of the 3rd Quarter, Fiscal Year 2003. Information sources used by the PDT to establish the baseline as a reference point included operating manuals, organization charts, and various management studies that had been recently conducted. The PDT observed many effective business activities within functional areas and some efforts to improve operational efficiencies across organizational borders. One clear example of how to achieve collaboration while maximizing available corporate resources is the recent USACE Project Management Business Process (PMBP) initiative. After review, observations, and discussions of the various BRM input sources, the PDT concluded the baseline offers much evidence of functional areas and at a variety of locations, with success in collaboration across traditional functional and geographic area boundaries.

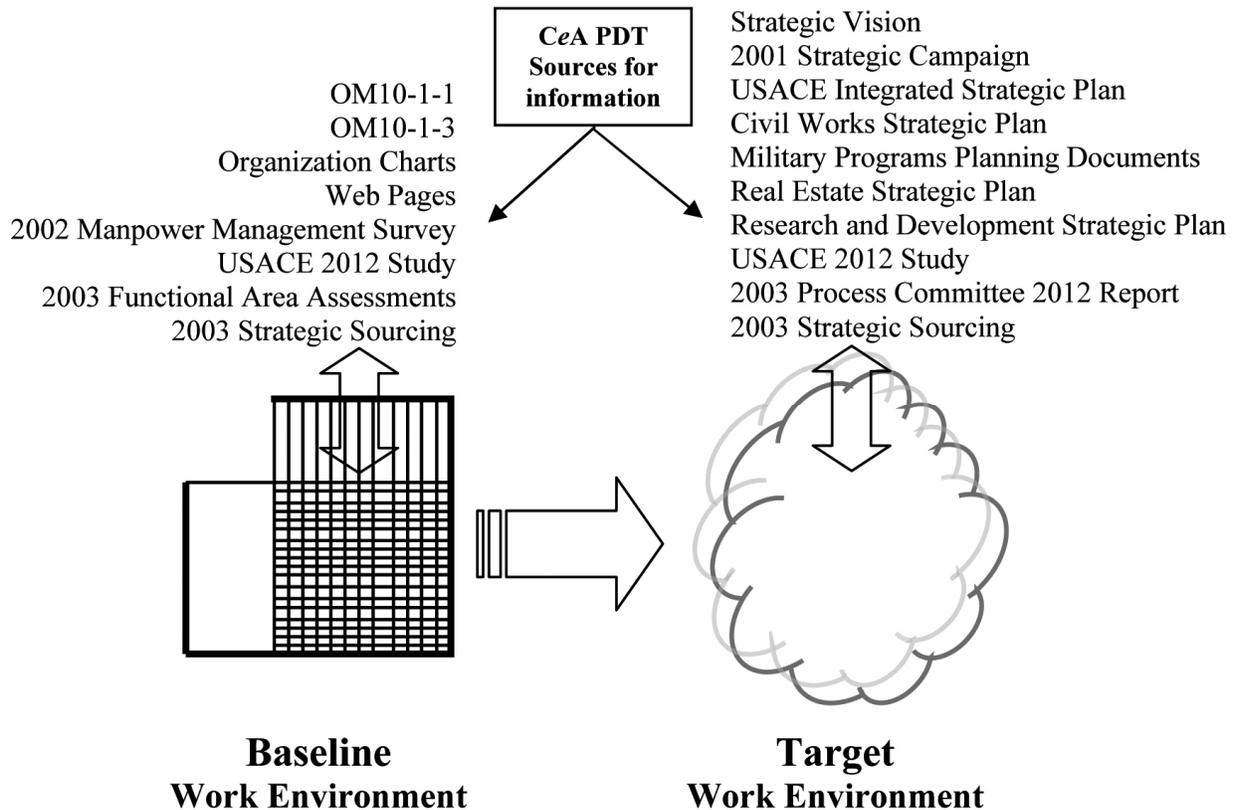


Figure 2.5. TWE analysis

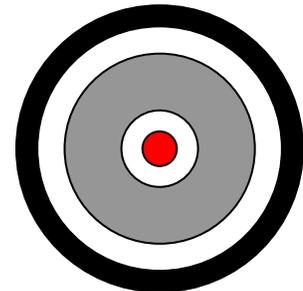
The TWE (Figure 2.5) can be painted from Strategic Plans developed by the Program Areas of Civil Works, Military Programs, and Research and Development. The USACE 2012 Process Committee Report and Strategic Sourcing Plan are also reliable indicators of changes in business functions in the near future. Critical thinking applied to

the various inputs about the TWE revealed that the initiatives outlined in the strategic plans were the most critical elements to monitor and support. These initiatives are the areas where the organization rises above the normal operational mode to improve efficiencies and/or customer satisfaction. The PDT states that:

“The Target Work Environment focuses on business functions and subfunctions that transcend organizational structure and work location.”

2.5.6 USACE IT Investments Supporting Migration to the TWE

The Chief Information Officer (CIO) focuses on a select group of enterprise-level IT Investments to enable a smooth migration to the TWE. For budget year 2005, the CIO requested IT Program Managers to prepare business cases that clearly mapped the following eight IT investments to the President’s Management Agenda and USACE Strategic Plan:



- Acquisition Services Program
- Asset Management Services Program
- Business Management Tools Program
- Consolidated IT Infrastructure/Office Automation/Telecommunications
- Emergency Preparedness and Response Program
- Financial Management Services Program
- Real Estate Management Program
- S&E Technology Program

For budget year 2006, the CIO expanded the breadth and depth of this mapping/migration requirement to increase granularity of investment details related to 16 individual IT projects (business cases) within the eight programs established for FY2005. The following list and rest of the main text of this report provide general discussion and migration strategy; state assumptions; present contributions toward USACE Strategic Goals; demonstrate support of the President’s Management Agenda; and clearly demonstrate how this investment will reduce costs or improve efficiencies.

- Architect-Engineer Contract Administration Support System and Construction Contractor Appraisal Support System (ACASS/CCASS)
- Asset Management Services Program (AMS)
- Automated Personal Property Management System (APPMS)
- Consolidated IT Infrastructure/Office Automation/Telecommunications (I/OA/T)
- Corps Enterprise Architecture (**CeA**)
- Corps Water Management System (CWMS)

- Emergency Preparedness and Response Program (EPRP)
- Financial Management Services (FMS)
- Knowledge Management Environment (KME)
- Operations and Maintenance Business Information Link (OMBIL Plus)
- Project Management Information System II (P2)
- Real Estate Management Program (REMP)
- Resident Management System (RMS)
- Science and Engineering Technology (SET) Strategy - Common Delivery Framework (CDF)
- Science and Engineering Technology (SET) Strategy - Enterprise Geospatial Information Systems (eGIS)
- Science and Engineering Technology (SET) Strategy – Modeling Tools

2.5.7 Budget Year 2006 Architectural Alignment and Assessment

An Architectural Alignment and Assessment of Major Enterprise-level IT Investments was conducted in August 2004. Sixteen business cases were studied to validate IT support to USACE business needs (Reference Civil Works Strategic Plan, dated March 2004, http://www.usace.army.mil/civilworks/hot_topics/cw_strat.pdf) and support to the President's Management Agenda (Reference President's Management Agenda, 2000, http://www.whitehouse.gov/omb/budintegration/pma_index.html). Figure 2.6 illustrates where these 16 business cases are considered valuable contributions to reaching Civil Works Strategic Goals and business objectives.

The **CeA**, in tandem with USACE 2012, is the modernization blueprint for mapping IT investments to business needs.

More detailed mapping of IT Investments can be found at Appendix I. Table 2.1 provides a sampling of data.

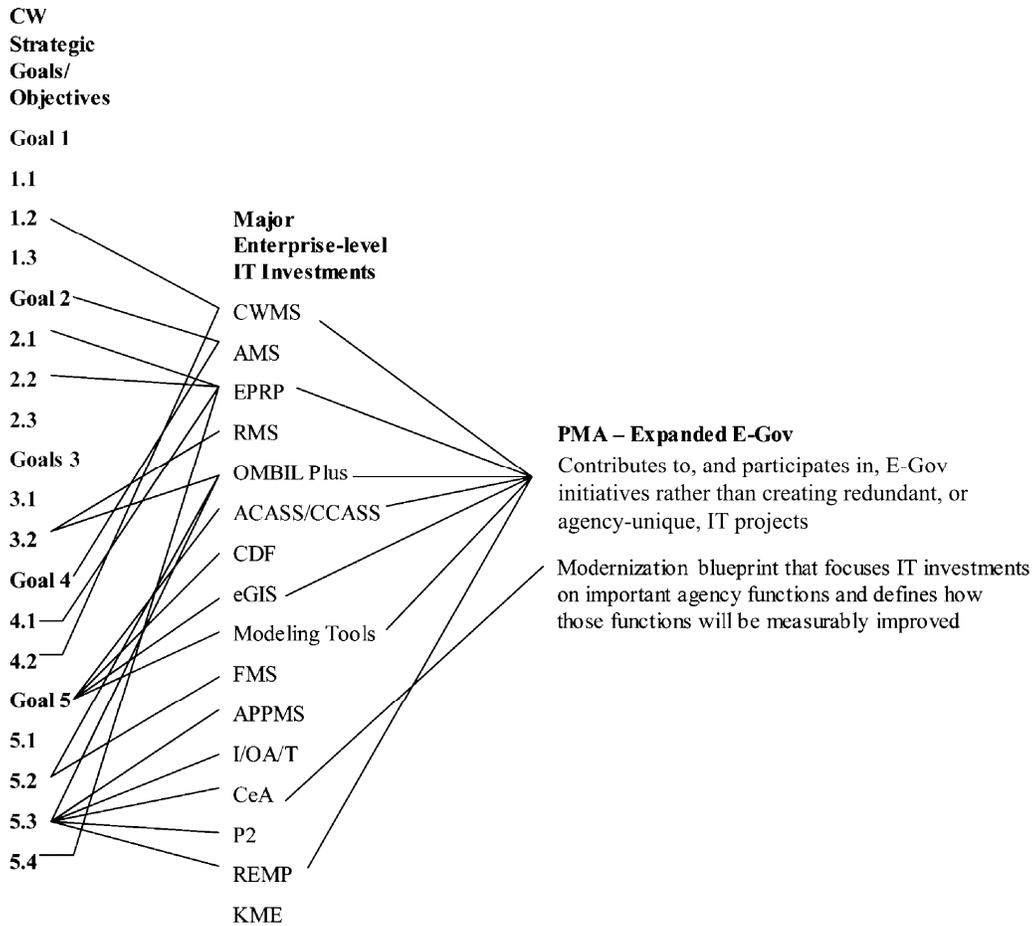


Figure 2.6. Contributions of IT business cases to Civil Works Strategic Goals/Objectives

Table 2.1. Excerpt of IT Investment Mapping

CW Goals and Business Objectives	Supporting, Major Enterprise-level IT Investments	IT Investment Support to President's Management Agenda
Objective 1.2. Support the formulation of regional and watershed solutions to water resources problems.	Corps Water Management System (CWMS) is a Web-enabled decision-support and analysis tool, used to support USACE water control management staff. This automated information system makes decision data readily available to chain of command, public input process for 700 reservoir and lock and dam projects. CWMS is required to operate 24/7 to meet the authorizing legislation and administration policies.	CWMS supports the President's Management Agenda goal, "Expanded Electronic Government," specifically addressing two objectives: 1. "Share information more quickly and conveniently between the Federal and State, local, and tribal governments." CWMS provides Web-based, Internet-accessible standardized water management information of river flows, stages, and reservoir operation plans; 2. "Automate internal processes to reduce costs internally, with the Federal government, by disseminating best practices across agencies." CWMS outputs have been designed for joint exchange and use among Federal agencies, including the National Weather Service, U.S. Bureau of Reclamation, U.S. Geological Survey, Tennessee Valley Authority, and several other Federal agencies.

2.5.8 USACE Data and Information Migration Plan for Achieving the Target Work Environment

TWE implementation efforts will focus initially on strategic business needs that can benefit from developing integrated databases that reside within an inner core. A common interface layer surrounding the managed database core will enable legacy applications to access the data using standardized, flexible, and reusable software modules designed specifically for this universal purpose. Program management and regional customer service are two key business areas that will potentially benefit from this approach.

As mentioned earlier, the TWE focuses on business functions and subfunctions that transcend organizational structure and work location. The Target Value Chain combines Civil Works, Military Programs, and Research and Development into a single primary business function called Missions.

The primary difference between the Baseline BRM and Target BRM is in the business practices. The Baseline BRM business practices are defined and implemented vertically by primary business function where each USACE organization controls and maintains the information produced with limited information sharing across the enterprise.

The following USACE business initiative listing provides an example of how TWE business processes and IT investments will be implemented around business functions and not organization structure:

- **Strategic Plan**
 - Program Management (PMBP)
 - Business Information
 - Inventory
 - Watershed
 - Environment Support for Military Installations
 - Vulnerability and Loss Reduction
 - Corporate Issues Management Process
 - Communications
 - Regulatory Process
 - Financial Budgeting
 - Streamline Acquisition Process
- **Information Technology**
 - IT Infrastructures
 - Technology Insertion
 - Information Assurance
 - IT Investment Portfolio Mgmt
 - e-Government
- **Knowledge Management**

- **Human Resource Mgmt**
 - Manpower
 - Skill Registry
 - Recruitment Service
 - Lessons Learned
 - Career-long Learning
 - Mentoring/Coaching

- **Science and Engineering**
 - World-Class Public Engineering

After the establishment of this target architecture, USACE developed a series of program-level IT migration plans and held discussions to consider cross-cutting impacts and considerations. Those discussions are summarized in the following paragraphs. Program and project milestones and strategies can be studied in more detail from the **CeA** Web site (<https://cea.usace.army.mil>).

The Migration Plan is intended to provide the azimuth and general management parameters for the TWE. The individual paths and methods to reach the TWE will be left to the discretion of the IT Program Managers with responsibility to provide oversight to all IT investments.

All IT initiatives in the near term should contribute toward creating an IT environment that is more responsive to the demands of changing business needs, able to store and manipulate dramatically larger volumes of data; adopts to new and more efficient technologies with minimal disruption; and provides adequate technology for administering new USACE programs.

Migrating from current USACE systems environment and infrastructure to the TWE will necessitate IT program and project implementation planning, coordination, and diligence in execution to ensure success. This migration will be phased in over a multi-year time horizon, based upon an evolutionary implementation plan. The PDT recognizes that implementing a target **CeA** is an evolutionary process, and that it must continually balance conflicts that will inevitably arise between meeting ongoing business needs with immediate technology solutions in the current environment and the long-term **CeA** goals.

2.5.9 Data Migration Considerations

Tomorrow's USACE worker and customers must access information where they work. Their workplace may be in the field, in a telecommute environment, home, or while on travel. As workers locate further out from the standard office environment, the need for collaborative means is of paramount importance. Further, USACE workers and customers need timely access to accurate information in support of their work, and they need accurate, timely, and complete responses to submitted work, requests for service, and information exchange.

The PDT envisions a **CeA** that manages data as the corporate resource. All operational business functions can be seen as data operations, whether the function is engineering, civil works, military programs, financial management, or scientific research queries. By optimizing information management, the **CeA** will improve the efficiency of all processes dependent on information flow. This optimization depends upon structuring the data so that searches through the data are rapid, and upon structuring the interfaces to the data so that communication of data to and from business functions is efficient and well defined. This results in an information-centric model, and allows for future collaborative initiatives for USACE and the Federal Enterprise Architecture Framework (FEAF).

The **CeA** conceptual enterprise data model (see Chapter 4, Data and Information Reference Model) is one based on universal data model concepts. These concepts are designed to produce standard and flexible models that are not drastically affected by enterprise business changes. The model is structured in a manner that permits the integration of USACE enterprise data efficiently in support of all of the USACE business operations, knowledge and content management, unstructured and structured, data and geospatial functions and data. The means required to transition to this type of structure and its underlying principles are as follows:

- a. **Identify and define enterprise data objects.** All of the data objects required to perform USACE enterprise functions must be defined and mapped to specific locations, organizational structures, and applications.
- b. **Establish a data management presence.** Policies and procedures to manage data as an enterprise asset need to be established, promoted, and maintained. These data management functions cover data definitions, naming, data retention, data accessibility, data retirement, etc. These should also address the process of data conflict resolution in the USACE data environment.
- c. **Identify data users and stewardship.** All of the users and stewards of any data object should be defined and identified with specific roles associated at any time during the life cycle of the data object.
- d. **Develop the enterprise data model.** This data model needs to be extensive enough to cover all of the data used by USACE, sourced either externally or internally. This data needs to cover “back office” data, geospatial data, and all types of USACE unstructured data.
- e. **Develop data quality processes and procedures.** These are policies and procedures that define and test, on an ongoing basis, data content and data management policies and procedures. These policies and procedures must be supported with metrics for data consistency, accuracy, timeliness, completeness, and validity.

- f. **Define and select enterprise support tools.** Consistent with the concept of maximizing the database structure for flexibility, appropriate support tools (data modeling, database build, quality measurement tools, etc.) need to be evaluated, selected, and implemented.
- g. **Define the enterprise data migration strategy.** An enterprise data migration is an iterative, ongoing process that builds a universal data model to meet all USACE data needs.
 - Rank and select the functional area of greatest Return on Investment (ROI) to USACE.
 - Forward engineer the enterprise database.
 - Alternatively, establish one of the current systems as the enterprise data and plan the long-term migration of that enterprise database to the constructs and principles embodied in the USACE enterprise data model.
- h. **Implement the migration strategy.** The migration strategy must be carefully planned and designed for implementation, over time, as USACE legacy databases are retired.

2.5.10 Risk Management During Migration

The need is clear for standardization of USACE business practices and asset management, particularly as it moves toward the objective organization. Risks and problems in transitioning workloads between contractors decrease with increased standardization in business methodologies.

Strategic and tactical planning of the business, technical, and organizational aspects of implementing a **CeA** has been ongoing throughout the **CeA** effort. No change occurs without risk, and change of the magnitude needed to implement a **CeA** fully is not without its share of risks to the business, the technical aspects, the environment, and personnel. Deliberate and ongoing planning, analysis, execution, and evaluation of the effort using a phased approach to implementing the target **CeA** permits the PDT to anticipate and manage risk. Its plans will be subject to continual refinement as the PDT considers outcomes and implications of subsequent phases for the changing business and IT environment. Progress toward achieving the target environment, changes in the strategic outlook driven by dynamics in the business environment, and details of the tactical steps will be reflected in each annual submittal of USACE Exhibit 300 budget submissions to the OMB.

2.5.11 Inputs for Defining the Target Work Environment

These **CeA** PDT researched and analyzed a wide variety of strategic direction documents and other information sources to arrive at the 13 TWE end states mentioned earlier. References included but were not limited to:

- USACE Integrated Strategic Plan
- CW Strategic Plan FY 04-09
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- **USACE 2012 Implementation Plan**
- CEEIS Modernization Planning
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps Project Management Plan (PMP)
- DoD Joint Technical Architecture
- Principal Assistant Responsible for Contracting (PARC) Web Page

The USACE 2012 Implementation Plan (“USACE 2012: Aligning the U.S. Army Corps of Engineers for Success in the 21st Century,” <http://www.hq.usace.army.mil/stakeholders/Final.htm>) serves as the modernization blueprint for reengineering business processes and making IT investment decisions. The paragraphs that follow are excerpts from the 2012 Implementation Plan:

- **Act as “One Corps”:** Align and operate as one Corps with the primary responsibility, authority, tasks and activities at each echelon commensurate with the appropriate role. Promote the concept of mutual-interdependence throughout the organization while aligning expertise with the work.
- **Act as “One Headquarters”:** HQUSACE and the Division echelons are aligned and operate seamlessly as one headquarters and issues are resolved after only one staff level review. The lowest level possible is empowered to action. Functions at each level add value and eliminate redundancies. Program oversight and integration occur at the Washington Headquarters and program management takes place at the Regional level.
- **Washington Headquarters Focus:** Washington Headquarters is focused primarily on strategic learning, planning and direction, national relationships, policy development and creating conditions for success of the entire organization.

- **Division Office Focus:** Division Offices are focused on creating conditions for success that enable the achievement of missions within the RBC through the accomplishment of Command and Control, Regional Interface, Program Management, Quality Assurance and operational planning and management of the RBC.
- **Actualize the RBC:** The RBC is used to effectively and efficiently utilize regional resources and expertise through the concept of mutual-interdependence.

2.5.12 Major Process Changes (Excerpts from 2012 Implementation Plan)

- **National and Regional Program Management:** Appropriations are managed at the national level and regions manage regional programs and funds.
- **Checkbook Funding:** Funding should be provided to enable offices to purchase necessary expertise and services when there is an insufficient requirement for a continuous level of effort or service.
- **Eliminate certification of DD1391:** The Assistant Secretary of the Army (Installations and Environment) (ASA-I&E) direction to conduct planning charrettes for all Army Military Construction (MILCON) projects included in the Program Objective Memorandum (POM) creates a redundant requirement for DD1391 certification. DD1391 certification can still be accomplished at the District level for those projects that have not been programmed based on a planning charrette.
- **Army MILCON Design Directives:** Regions will issue design directives on all Army MILCON projects.
- **Army MILCON Reprogramming:** Regions will request MILCON reprogramming authority and approval directly from Office of the Assistant Chief of Staff for Installation Management (OACSIM). Washington level HQs will be informed the action is occurring but will not be in the process flow.
- **Regions Manage Army MILCON Project Funds:** Regions will obtain project funds directly from HQs Washington level Directorate of Resource Management. This includes construction and Planning and Design (P&D) funds. Washington level HQs will manage at the appropriation level and the regions will manage at the project level. P&D funds will be allocated by Washington level HQs on a regional basis. The Regions will allocate and manage on a District basis.
- **Regional Support Centers:** Many of the support functions recommended the establishment of Regional Support Centers for their specific function. This concept has merit on a broad scale and Regions are encouraged to evaluate the concept for all Regional functions, support and mission. It appears that regional processes could be streamlined significantly in some functional areas.
- **Programmatically Fund the “Reconnaissance Phase” of the Civil Works Planning Process:** Establish reconnaissance studies similar to the current Continuing Authorities Program. Congressional action will be required.

- **Provide 100 Percent Federal Funding for the Feasibility Phase of Project Implementation:** Seek Congressional Modification of WRDA 86 to remove the feasibility study cost sharing requirement.
- **Build and Defend the Civil Works Program around Business Lines:** In FY 05, the Corps of Engineers is developing its budget based on the nine water resources business lines. This initiative should be continued.
- **Reconstitute Project Cooperation Agreements (PCAs) as Partnering Agreements executed at the District Level:** This would eliminate months, if not years, from the civil works process and address the number one partner and customer complaint about our civil works process.
- **Actualize the Regional Business Center:** Focus Washington Headquarters and Division Offices on their appropriate missions and align resources to truly actualize RBCs.

2.5.13 Organizational Design Concepts (Excerpts from 2012 Implementation Plan)

- **Regional Business Center (RBC):** The Corps is moving toward the RBC objective state defined in the RBC 2012 Concept Paper, March 24, 2003. The basic premise is that the Corps will operate more interdependently within each region. Each district will no longer need to perform every function; the Corps will have technical centers, regional metrics, regional support functions that serve multiple districts, and one CEFMS database. For example, one CEFMS database for each region is necessary to actualize the RBC, as it will allow direct charging to projects within a region, streamline internal funds management processes, and promote collaboration. As the Corps defines what it does within each functional area, it is essential that the evolving "doctrine" be recognized, particularly as defined in the role of the RBC. Both Washington Headquarters and Major Subordinate Command (MSC) Headquarters processes must be designed to maximize support of district tactical level work, while efficiently leveraging all available resources of the Corps.
- **Regional Support Teams:** Significant cultural changes and minor structural changes are necessary to break the existing three-echelon and competing-stovepipe paradigms necessary to operate as One Corps and One Headquarters. Cultural changes will take place over time as we stop competing internally between programs and begin to behave as "One agile team, capable of operating virtually as a learning organization." The structural change that will support the cultural change is the creation of Regional Support Teams (RSTs), which will link the Washington and Regional Headquarters into one and create synergy among all programs. RSTs will be focused on the execution of programs for major Corps mission areas including Civil Works, Military Construction, Installation/Interagency/International Support, Environmental, Real Estate, and Research and Development. The teams will be assigned to the Washington level HQs and will be duty stationed in Washington, but they will represent the voice, concern, and conscience of the Regions. They will be empowered to work issues

with any level of the USACE organization necessary to resolve the issue in an expeditious and timely manner.

- Support Functions:** In the context of Executive Direction and Management (ED&M), "mission" equates to direct program oversight, and "support" is the indirect services that facilitate that program oversight. For purposes of this analysis, the General Expense (GE) & Operations and Maintenance (OMA) ED&M resources assigned to Military Programs, Civil Works, Real Estate, and Research and Development are assumed to be direct "mission" assets. All other functions are defined as "support."

Utilizing USACE 2012 considerations listed above, two primary organizational models for support functions (Figure 2.7) were developed:

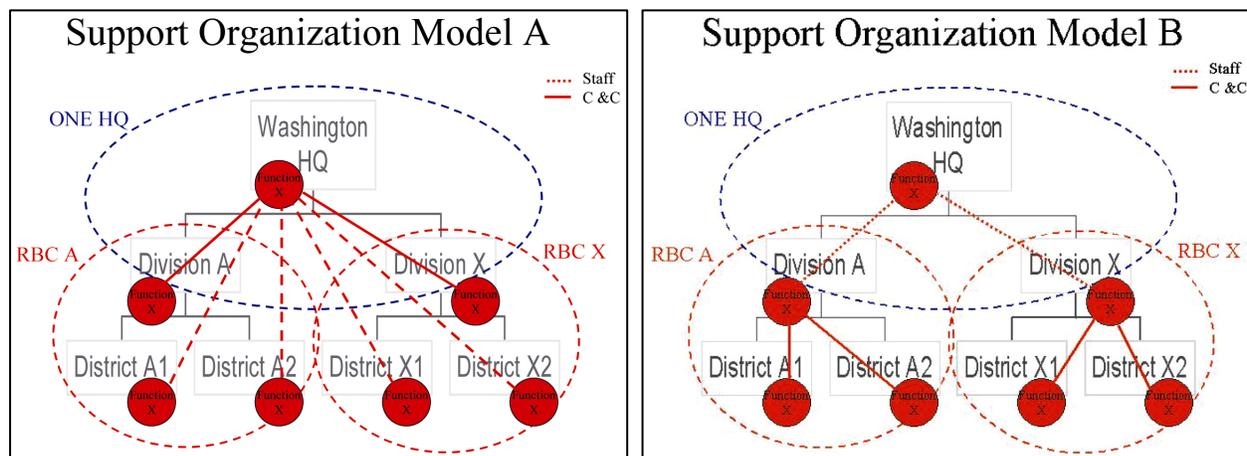


Figure 2.7. Organizational Models for Support Functions

- Support Organization Model A (National Focus)** was designed to provide support services that can most effectively be provided at the national level, utilizing centrally managed national assets. Under this concept, individuals and their work assignments would be managed by the functional lead located in the Washington Headquarters. This model requires all personnel to be included in the Washington level HQs manning document. Individuals would be forward deployed to other locations as needed. There may or may not be a physical presence at each location.
- Support Organization Model B (Regional Focus)** was designed to provide support services that are best provided regionally, that are part of the "business of doing business" in the RBC. Under this concept, individuals and their work assignments would be coordinated by and be under the oversight of the functional lead located in the RBC Headquarters. Only ED&M personnel would be physically located in the RBC Headquarters. Most assets would be forward deployed to serviced locations. Supervisory relationships between the functional lead and the serviced organization can be tailored depending upon the specific function being performed. The functional lead in the RBC would generally report

to the Deputy Division Commander. The functional lead in the RBC would retain a staff-to-staff relationship with the functional lead in the Washington HQ, much as it is today. For example, this type support organization is currently functioning in the U.S. Army Engineer Research and Development Center (ERDC), although the funding is less complicated as there is no differentiation between ED&M and other funding sources. There is one Chief, Resource Management (RM) responsible for providing support to all of ERDC's seven laboratories. Functional team members are present at each of the locations although they do not all perform the same functions at each location. There is a direct reporting relationship between the Chief of Resource Management and the director of ERDC and a staff relationship between the ERDC Chief of RM and the USACE Director of RM.

2.6 USACE Functions and Subfunctions Mapping to the FEA Business Reference Model

The OMB requires all Federal agencies to map their individual Lines of Business (LOB) and subfunctions to the Federal Enterprise Architecture (FEA) LOB and subfunctions. USACE BRM business functions directly map to the FEA BRM at the USACE 2nd level subfunctions (not shown in Figure 2.7). Table 2.2 provides a representative sampling of the subfunction mapping to FEA subfunctions. This list also shows the information source used to make this determination. As shown, the PDT referred to the USACE 1984 Information Systems Plan (ISP), which was the last time enterprise-level business processes were identified and validated by business owners. The 2003 USACE Strategic Sourcing was also used as a reference point to consider present-day subfunctions being conducted. The Strategic Sourcing Work Breakdown Structure (WBS) was particularly useful to understand subfunctions at the District level. See Appendix E for full listing and subfunction crosswalk.

As mentioned in the previous paragraph, OMB requires all Federal agencies to map their individual LOB and subfunctions to the FEA LOB and subfunctions. Table 2.2 shows the direct mapping of USACE subfunctions to FEA subfunctions. The LOB is the higher-level crosswalk between individual Federal agencies business and the general crosscutting LOB at the Federal level. The PDT has developed the chart in Figure 2.8 as the starting point for aligning USACE LOB with the OMB FEA-prescribed LOB. It should be noted that this LOB crosswalk is notional at best until validated by USACE senior leaders. This work will continue to ensure USACE business owners have a good reference point for work being done by USACE in comparison to work being done by other Federal agencies.

Table 2.2. Sampling of Subfunction Mapping to FEA Subfunctions

FEA Business Area (BA)	FEA Line of Business (LOB)	FEA BA Code	FEA LOB Code
Services For Citizens		1	
Community and Social Services		1 01	
Correctional Activities		1 02	
Defense and National Security		1 03	
Disaster Management		1 04	
Economic Development		1 05	
Education		1 06	
Energy		1 07	
Environmental Management		1 08	
General Science and Innovation		1 09	
Health		1 10	
Homeland Security		1 11	
Income Security		1 12	

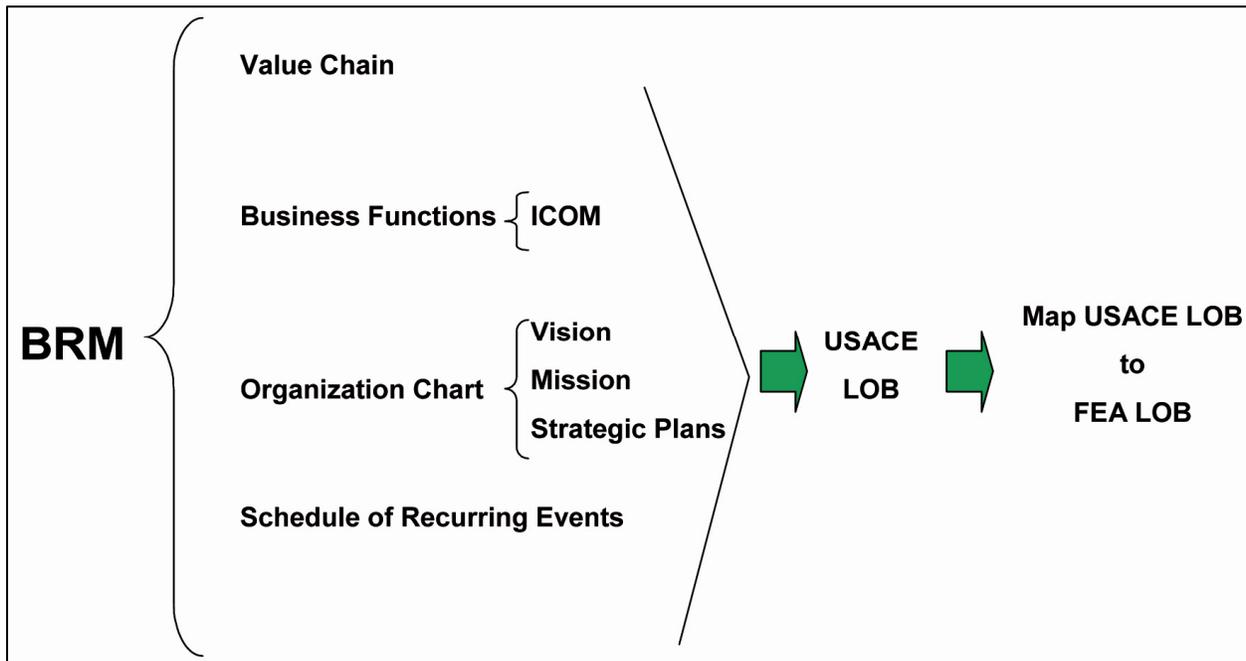


Figure 2.8. Chart for aligning USACE LOB with FEA LOB

OMB has established four specific FEA BRM Business Areas that require mapping from individual Federal agencies:

- Services for Citizens (the purpose of government)
- Mode of Delivery (the mechanisms the government uses to achieve its purpose)
- Support Delivery of Services (the support functions necessary to conduct government operations)
- Management of Government Resources (the resource management functions that support all areas of the government's business)

Figure 2.8 shows the mapping process. Figure 2.9 shows the PDT's best effort at aligning USACE LOB to FEA LOB. See Appendix F for full LOB listing and subfunction crosswalk.

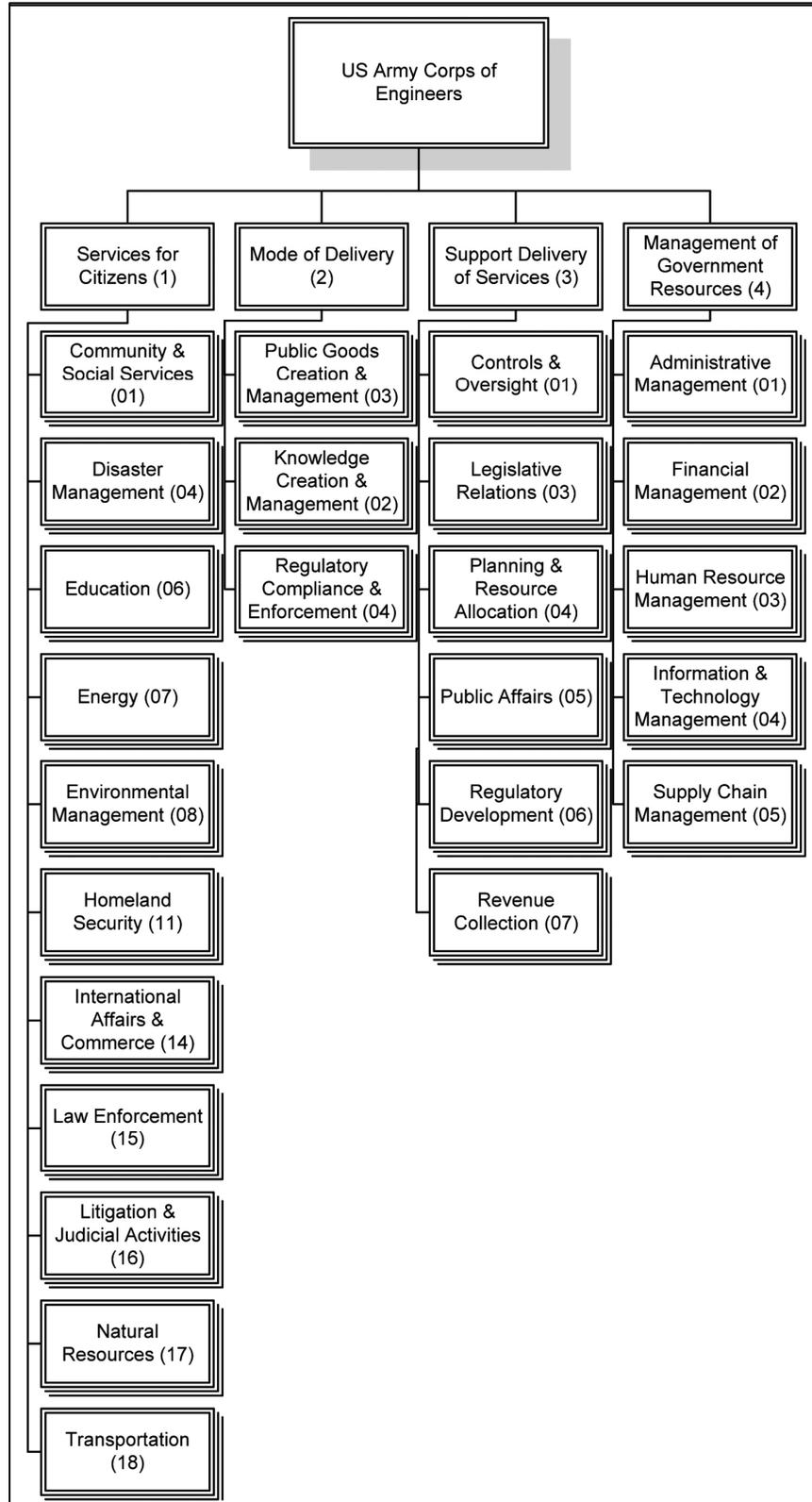


Figure 2.9. USACE Lines of Business Mapping to the Federal Enterprise Architecture Lines of Business

2.7 USACE Business to Information Technology Support Context

Depicting USACE LOB and subfunctions, and mapping them to the FEA are helpful but not the main purpose for developing the USACE BRM. To understand and improve the way IT supports USACE vision, missions, and business functions requires mapping at the sub-subfunction (or activity) level. The PDT puts it this way:

“Comprehending the consequences of choices being made about USACE business functions and IT support requires mapping relationships of inputs, outputs, controls and mechanisms at the activity level.”

The PDT developed a series of diagrams to illustrate inputs, outputs, controls, and mechanisms (ICOM) at various operational levels to ensure closer examination at the lowest level was done in concert with higher level ICOM. The charts describe the ICOM process for the USACE primary business functions. Figures 2.10 and 2.11 reflect the ICOMs affecting USACE and their impact on a single business function (between Baseline Work Environment Primary Business Function of Civil Works, Military Programs, and Research and Development Programs). Validation has been accomplished with most, but not all business owners. This work will continue. See Appendix G for full-size, easy-to-read versions of ICOM charts.

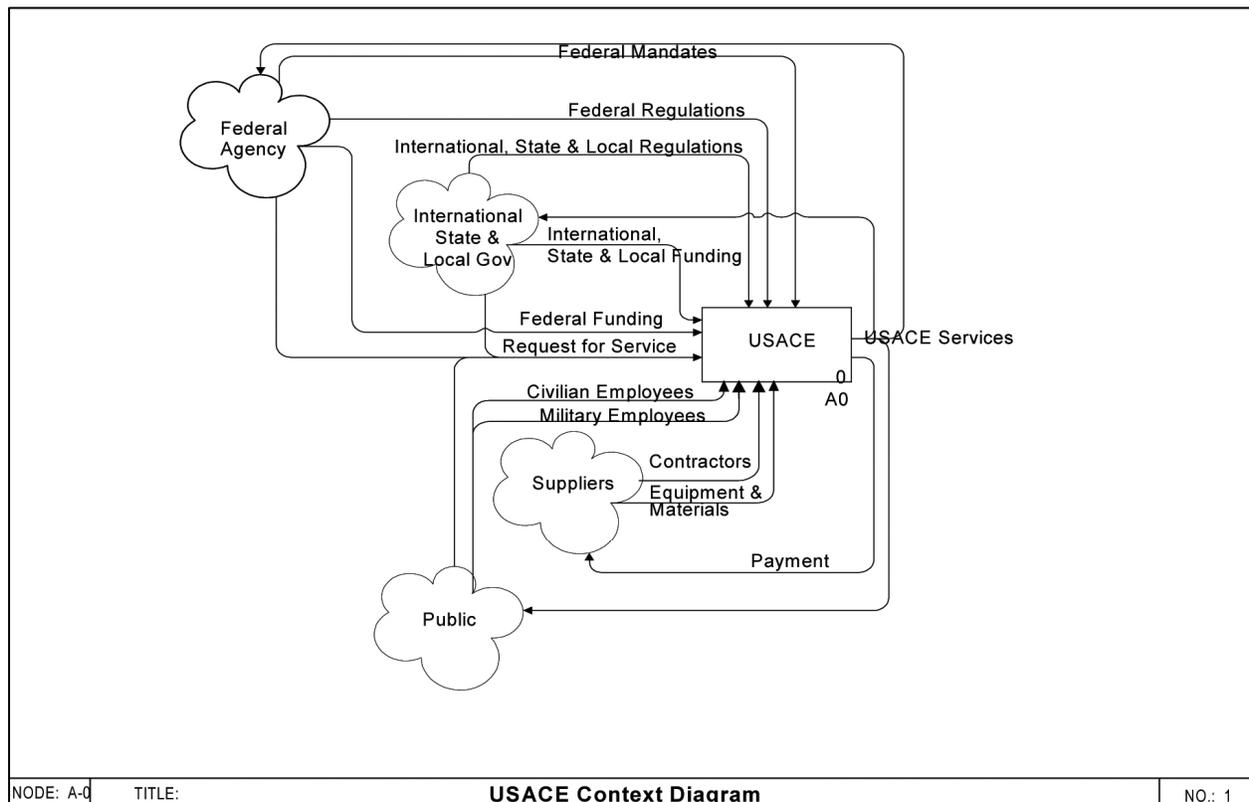


Figure 2.10. ICOMs affecting USACE

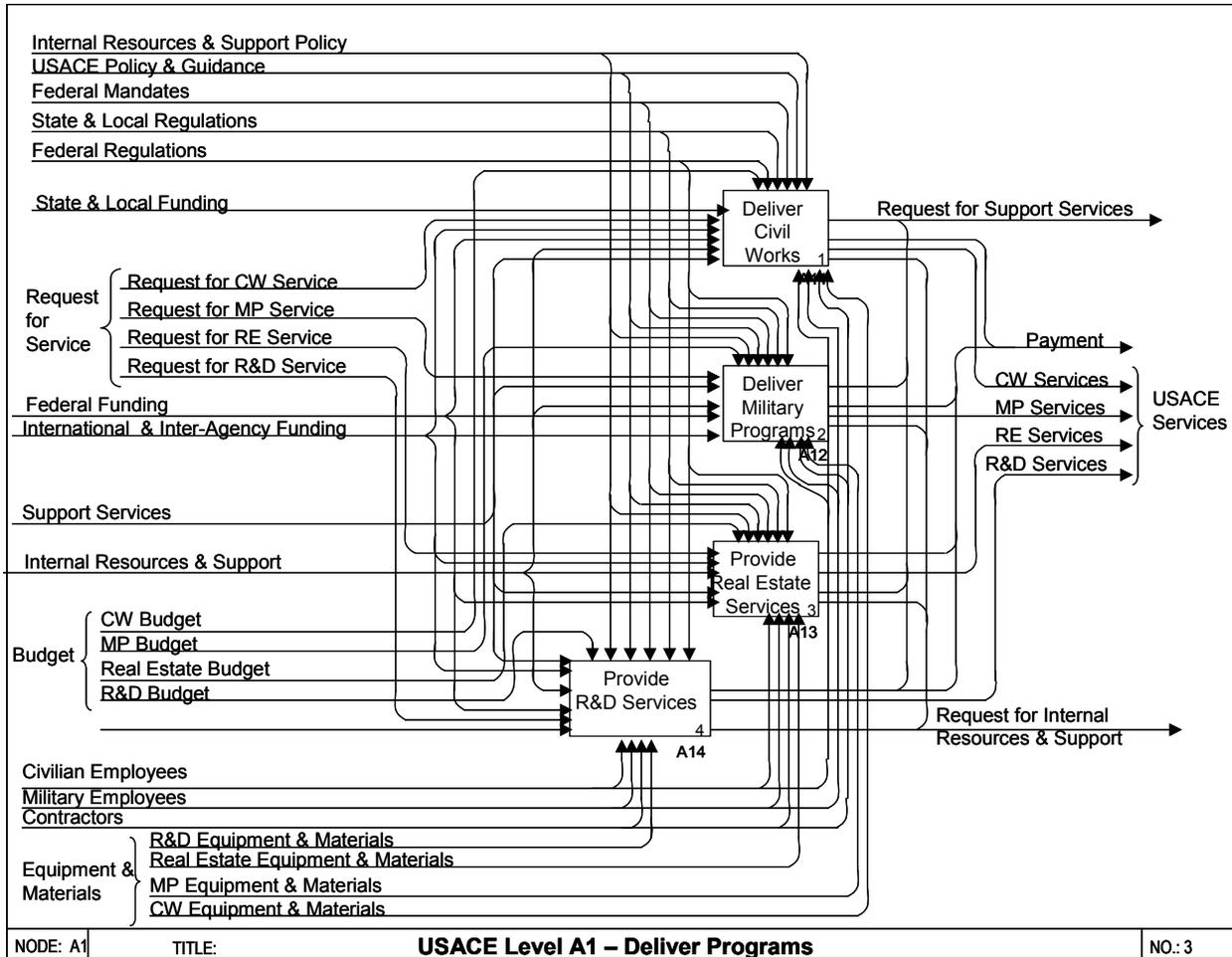


Figure 2.11. Impact of ICOM on a single business function

Figure 2.11 shows ICOM exchanges between Civil Works, Military Programs, Real Estate and Research and Development Programs (see Value Chain diagram in Figure 2.2).

2.8 USACE High-level Business Functions Inputs, Controls and Mechanisms

The high-level functions ICOMs are the lowest level scope for the initial **CeA** development task. Additional levels of understanding about ICOMs at lower levels are necessary and will be continued in later **CeA** development efforts. Figure 2.12 shows one example of one functional area identified on the Value Chain. See Appendix G for full-size chart and ICOM spreadsheets of remaining functional areas.

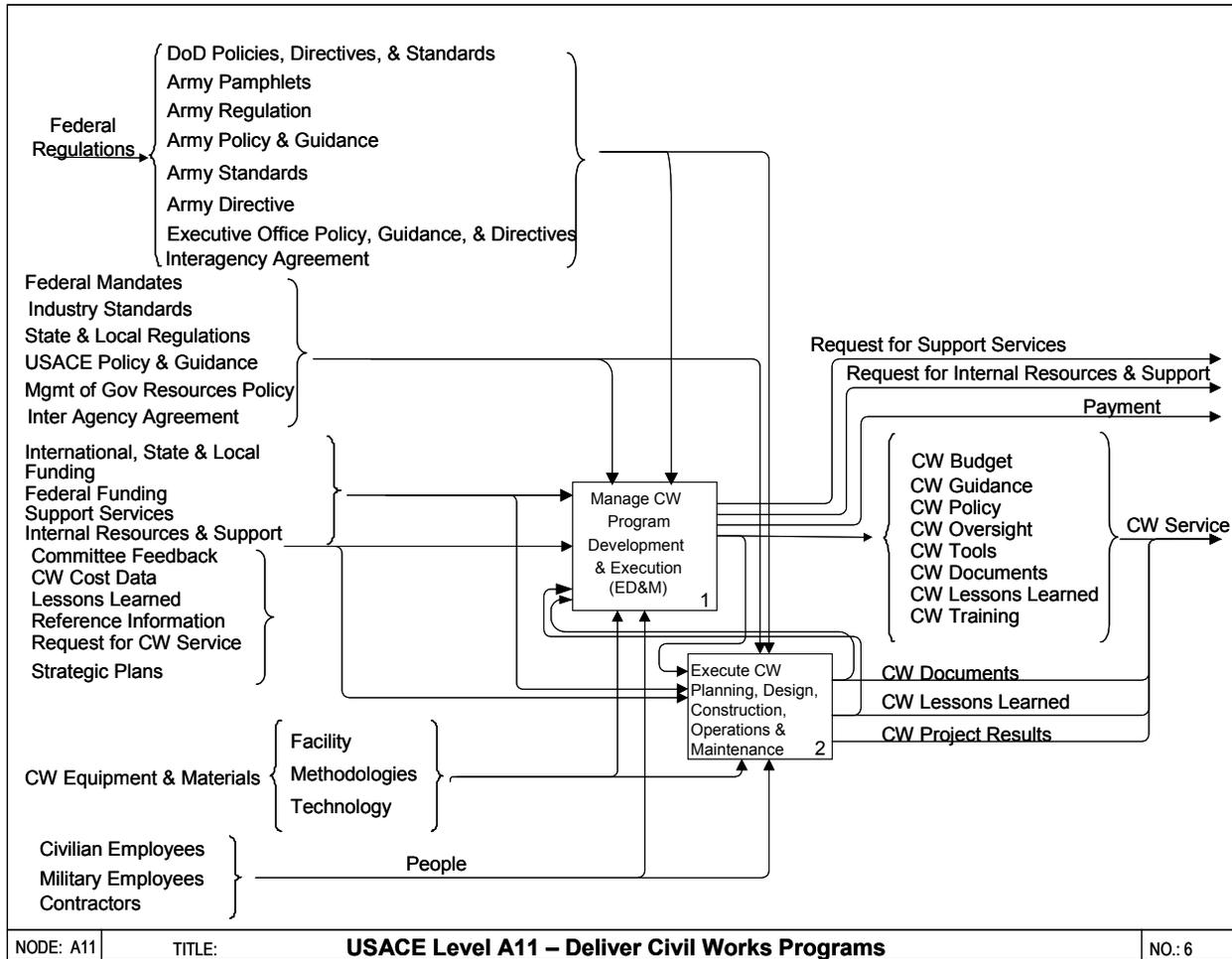


Figure 2.12. Example of one functional area identified on the Value Chain

2.9 The Target USACE Work Environment Worksheet

The TWE worksheet (Table 2.3) was used to focus on business functions and subfunctions that transcend organizational structure and work location. It was observed that the USACE Value Chain and BRM will remain very similar to the Baseline work environment except that the Target Value Chain will combine Civil Works, Military Programs, Real Estate, and Research and Development into a single primary business function called “Programs.”

The primary difference between the Baseline BRM and Target BRM is in the business practices. The Baseline BRM business practices are defined and implemented vertically by primary business function where each USACE organization controls and maintains the information produced with limited information sharing across the enterprise.

The worksheet in Table 2.3 provides a sample of USACE initiatives that move the organization closer to the TWE. See Appendix H for full listing.

Table 2.3. TWE Worksheet for Business Functions and Subfunctions

Primary Business Function	Initiative	Source Document	Source Document Section	As-Is	To-Be
Programs	Program Management (PMBP)	USACE Campaign Plan	Process, Strategy 1.2 & 1.3	by Project (PROMISE)	by Enterprise (P2 and Regional Management Board)
		MP 2012, May 2003	Goal 6		
		CERE 2012, April 2003	Process, Objectives 1.1,1.2, 4.1, 3.2-5 Communication Objective 2.2		
	Business Information	USACE Campaign Plan	Process, Strategy 2.3	by Enterprise (OMBIL-+)	by Enterprise (OMBIL-+)
	Inventory	USACE Campaign Plan	Process, Strategy 2.3	by functional area (FEM, NID, REMIS, etc.)	Enterprise Asset Management
	Watershed	USACE Campaign Plan	Process, Strategy 3.1	by project	managed Watershed Solutions (Regional Watershed Planning Tool)
		CW Strategic Plan FY 2004-2009 <i>(note: plan details As-Is and To-Be as well as implementation strategy)</i>	Strategic Goal 1-3, Section 4 (Goals and Objectives), Section 5 (Implementation & Evaluation)		
	Environmental Support for Military Installations	USACE Campaign Plan MP 2012, May 2003	Process, Strategy 3.3 Goal 3	limited support by project	regional, holistic assessments leading to projects
	Vulnerability and Loss Reduction from Natural and Man-made disasters, including terrorism	CW Strategic Plan FY 2004-2009 <i>(note: plan details As-Is and To-Be as well as implementation strategy)</i>	Strategic Goal 4, Section 4 (Goals and Objectives), Section 5 (Implementation & Evaluation)	by project	1) Integrated life-cycle management of emergency management programs 2) Provide critical infrastructure protection for Civil Works facilities and seamless infrastructure protection within the Corps
	Corporate Issues Management Process	USACE Campaign Plan	Communications, Strategy 4.2	ad hoc issues identification & Resolution	Corporate Issues Management Process
Improve Communications with External Partners, stakeholders, & Customers	USACE Campaign Plan	Communications, Strategy 3.1 & 3.2	Ad hoc Communications	Enterprise-wide Communications Process	
	CERE 2012, April 2003	Process, Objective 1.5, 2, 4.2, 4.4, 4.5 Communication Objective 2			
Regulatory Process (simpler, transparent, consistent)	USACE Campaign Plan	Process, Strategy 3.2	Duplicate Permit & Mitigation Requirements imposed on non-Federal O&M Sponsors	eliminate duplicate permit and mitigation requirements imposed on non-federal O&M Sponsors; increase using Special Area Management Plans	

References Used in Developing Baseline and Target Work Environment

- USACE Strategic Vision: <http://www.hq.usace.army.mil/cepa/vision/vision.htm>
- USACE 2001 Strategic Campaign: <https://corpsinfo.usace.army.mil/mp/n/50th/CampaignPlanUpdate8May01.pdf>
- Program Area Strategic Plans —
 - Civil Works: <http://www.iwr.usace.army.mil/iwr/strategicplan.htm>
 - Military Programs
 - Real Estate Strategic Plan
 - Research and Development Strategic Plan
- Organization Charts
- Human Resource Requirements to Execute the Mission
 - USACE 2012
 - 2003 Functional Area Assessments
 - 2003 Process Committee 2012
 - 2003 Strategic Sourcing

- 2002 Manpower Management Survey
- **CeA** PRM
- FEA BRM: <http://www.feapmo.gov/feaBrm2.asp>

BRM work products (sometimes referred to as artifacts) developed by the PDT to better understand the Baseline and Target work environments include

- USACE Enterprise Statement and Value Chain Diagram
- Graphic and Narrative for the Baseline and Target Work Environments
- USACE Business Functions and Subfunctions
- USACE Subfunctions Mapping to **CeA** PRM Metrics (Currently under development)
- USACE Functions and Subfunctions Mapping to the FEA BRM
- Calendars of **CeA**-related Events
- **CeA** Governance and Management Tools

Chapter 3 – Performance Reference Model (PRM)



The PRM provides a standard performance measurement framework designed to

- Enhance available performance information
- Better align inputs with outcomes
- Identify improvement opportunities across organizational boundaries.

The **CeA** PDT is prescribing the FEA PRM framework recently released to Federal agencies. The PRM uses standard IT performance indicators, which can be new or coincide with those already in use, and can be tailored or “operationalized” to the specific environment.

DRAFT PERFORMANCE REFERENCE MODEL (PRM)

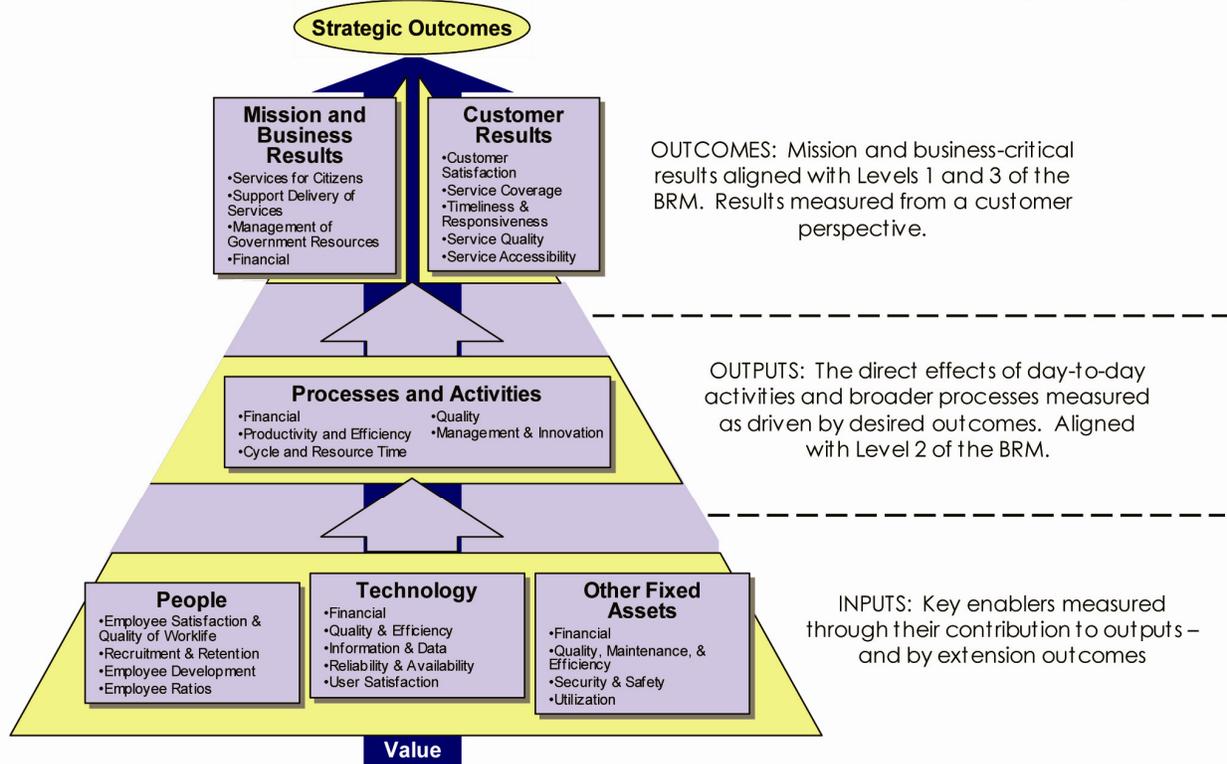


Figure 3.1. Draft PRM

The PRM components are shown in Figure 3.2 (see Appendix N for readable version).

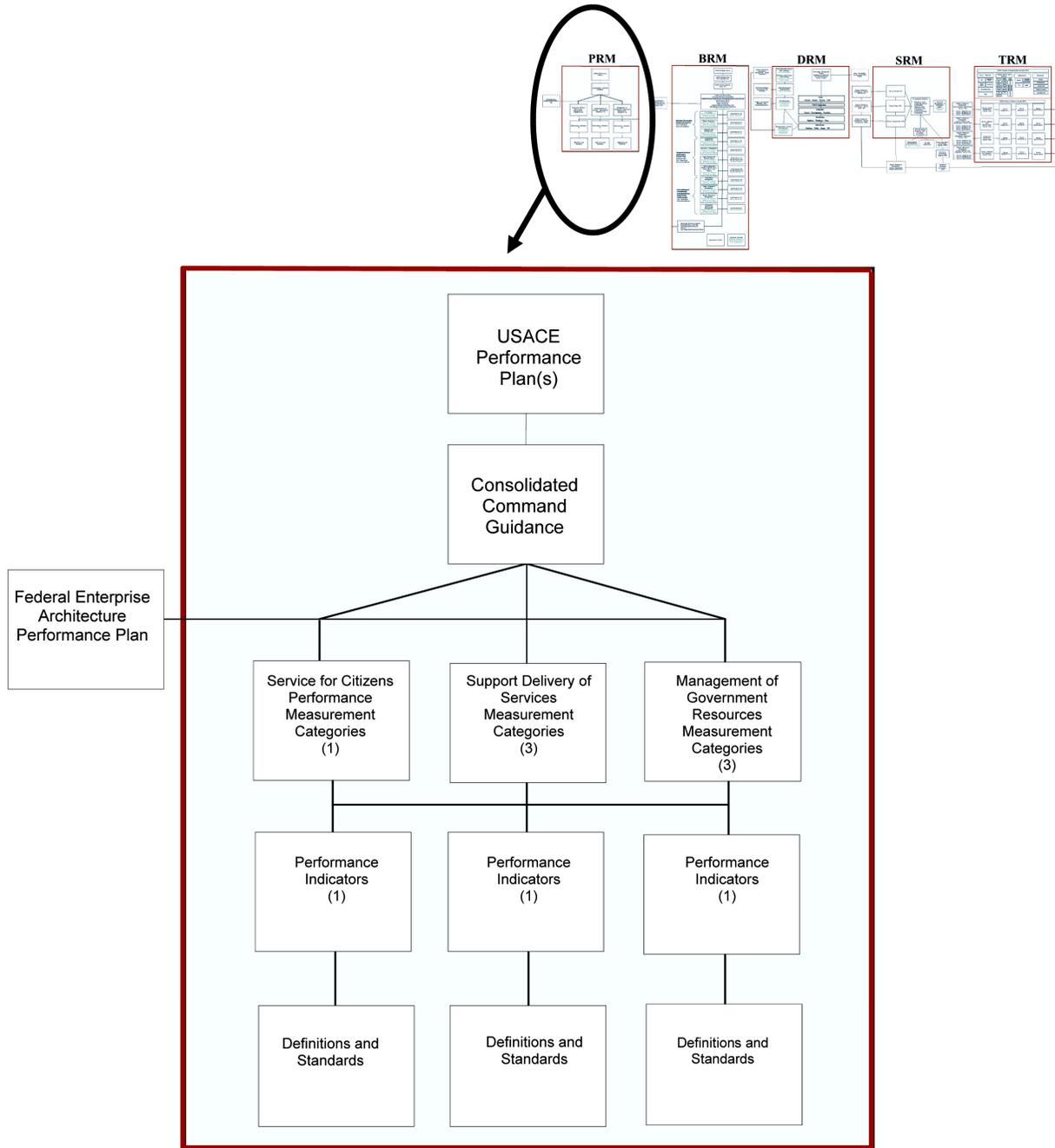


Figure 3.2. PRM components

3.1 Baseline Performance Reference Model

The current USACE PRM version covers the performance measurement for business subfunctions and their results. USACE Baseline architecture identified twelve primary

business functions: Civil Works, Military Programs, Real Estate, Research and Development, Legal Service and Internal Review, Information Technology Management, Resource Management, Others, Acquisition Management, Logistics Management, Human Resource Management, S&E. As of September 2003, only Civil Works, Military Programs, Real Estate, and Research and Development will be implemented. Tables 3.1 and 3.2 show two USACE business areas: Business subfunctions and Business sub-subfunctions (as described in the BRM):

Table 3.1. PRM Business Subfunctions

Primer Business Function	Subfunctions
Civil Works	Manage Civil Works Program Development & Execution
	Direct Civil Works Operations & Maintenance
Military Programs	Military Construction
	Installation Support
	Environment Restoration
	Interagency and International Support
	Direct Real Estate Activities
	Provide Real Estate service for Natural Disaster Relief
Research and Development	Directs the Research and Development Programs

Table 3.2. PRM Business Sub-subfunctions

Primer Business Function	Subfunctions	Sub-subfunctions (Also referred to as business lines)
Civil Works	Manage Civil Works Programs Development & Execution	Provide Strategic Direction
		Direct Civil Works Policy/Planning
	Direct Civil Works Operations & Maintenance	Navigation
		Flood Control
		Emergency Management
		Environment
		Regulatory
		Recreation
		Water Supply
		Hydropower
Works for Others		

One of the key PRM work products will be a chart mapping the performance metrics to business functions, as shown in Table 3.3. See Appendix I for a readable version.

Table 3.3. Chart Mapping Performance Metrics to Business Functions

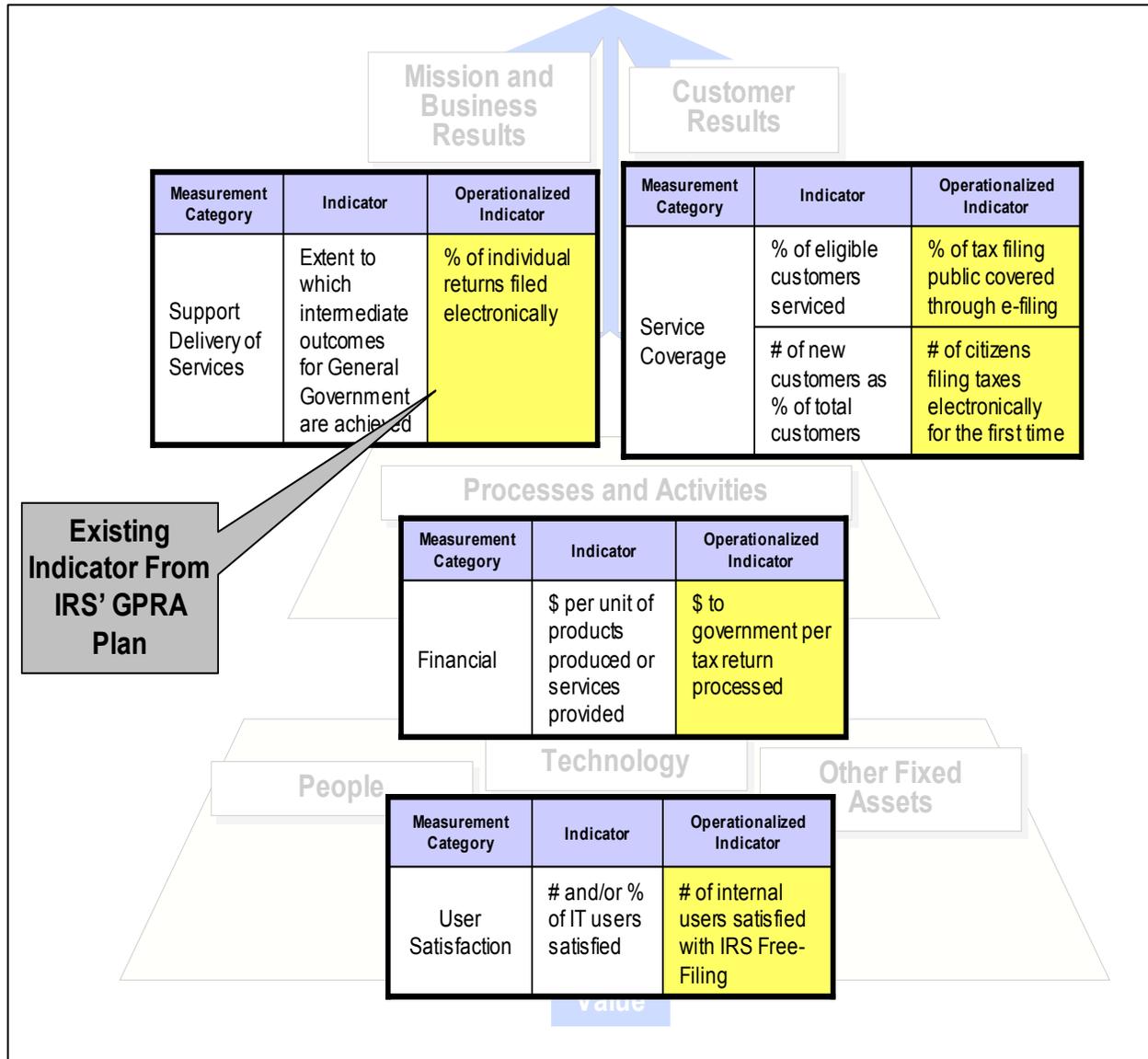


Figure 3.3. Overview of PRM

The ultimate goal of the Target PRM is to align performance information properly for development, modernization, and enhancement of IT investments with the PRM in “Performance Goals and Measures.”

A second important work product coming out of the PRM will be a clearly articulated cause and effect chart that shows relationship between IT inputs, process outputs, and ultimately business and customer outcomes. A notional example is provided in Table 3.4.

Table 3.4. Sample Cause and Effect Chart

Fiscal Year	Measurement Area	Measurement Category	Measurement Indicator	Baseline	Planned Improvements to the Baseline	Actual Results
2005	Mission & Business Results	Support Delivery of Services	Percent of individual tax returns filed electronically	41%	Increase to 44%	TBD
2005	Customer Results	Timeliness & Responsiveness	Time citizens save by filing electronically	TBD	TBD	TBD
2006	Mission & Business Results	Support Delivery of Services	Percent of individual tax returns filed electronically	TBD	TBD	TBD

Chapter 4 – The CeA Data and Information Reference Model (DRM)



The Data and Information Reference Model (DRM) describes, at an aggregate level, the data and information that support USACE programs and business lines of operation.

The initial scope of the DRM is to identify and exchange information about enterprisewide data and information activities. While there are thousands of actions where data is generated and used each business day, it is rare that users ask the questions, “Is the required data available somewhere already?” or “Could someone else take advantage of the data being generated for a perceived unique requirement?”

The U.S. Army Corps of Engineers (USACE) relies on interactive computer-based systems to identify and assess alternatives, make decisions, solve problems, and conduct business in general. Data is the principal component that drives the decision-making process and the quantified representation of information. Data becomes information when meaning is applied to it. The terms data and information will be used synonymously in this document. Information is a corporate asset. In fact, it is information that drives our business process, not applications and technology. Applications are developed or purchased to manipulate and create new information. Technology is the enabler that supports applications and the ability to store and deliver information. It is important that all automation efforts focus on information use and not just technology. Thus, it is important to manage data according to certain basic principles:

- Avoid duplication in data acquisition. Share data wherever possible via networks and partnership.
- Look for existing data sets before performing data collection.
- Adhere to existing government and industry data content, access, and delivery standards.
- Manage data to maximize its use by multiple processes.
- Manage data at the owner level and negotiate access arrangements.
- Require the use of metadata for every data set.

This document provides the reference model for managing USACE data according to these principles. A reference model is a framework for understanding significant relationships among the entities of some environment, and for the development of consistent standards or specifications supporting that environment. Based on a small

number of unifying concepts, a reference model is a generally accepted abstract representation that allows users to focus on establishing definitions, building common understandings and identifying issues for resolution. The **CeA** DRM provides a mechanism for identifying the key issues associated with enterprise information portability, modularity, scalability and interoperability.

The primary objectives of the DRM are to

- Describe, at an aggregate level, the data that support program and business line operations
- Establish a commonly understood classification of USACE data
- Facilitate the identification of duplicative data resources
- Streamline data exchange processes internally, government to government, government to business, and government to citizen

The DRM is organized in three main sections:

- Baseline and Target Data Environment for selected mission-critical AISs
- Data Sharing Framework
- Categorization of Data

4.1 Baseline and Target Data Environment for Mission-critical AIS

Both a Baseline Data Environment and a Target Data Environment were defined based on a review of the data environments for eight mission-critical AIS.

4.1.1 Baseline Data Environment for Mission-critical AIS

Initially, a USACE Baseline Data Environment was identified based on the data associated with eight mission-critical systems plus GIS data objects:

- REMIS
- CEFMS
- RMS
- FEMS
- ENGLink
- CWMS
- P2/PROMIS
- OMBIL Plus
- GIS

More detailed information about each of these systems is provided in Appendix J, Section J.8.

The intent was to establish a commonly understood classification for USACE data and begin to identify duplicative data resources, data anomalies, and inefficient structures. For each of these systems, the following efforts were completed:

- Identified the data types (from the reviewed database structures) used
- Provided a high-level general description of the data and database objects
- Indicated the location and number of instances of these data objects
- Provided some indication of the nature of the data sharing, replication, or extraction of data between the data types

The data models for these eight systems plus geospatial data were reviewed for 1) consistency of structure, 2) application of standards that might have been applied, 3) common data structures and attributes, 4) common relationships, and 5) unnecessary complexity or size. In addition, data was gathered from the location where the data objects appeared and/or were interfaced, replicated, or exchanged. Details of this review are provided in Appendix J.

The review showed that data for the eight mission-critical systems plus geospatial data are highly consistent in terms of use of common structures and definitions, which implies that standards and data management policies and procedures were employed at one point. In addition, there is a substantial amount of “shared” data between the database systems.

Several key data issues or observations that seem to be generally characteristic of the baseline environment are worth noting:

- Redundant data in the environment.
- Unusually large numbers of tables within key databases (e.g., CEFMS, REMIS).
- Dissimilar data within key databases.
- Noninterfaced geospatial data to USACE operational data (e.g., REMIS data related to geospatial data).
- Seemingly unnecessary replication of data across Districts.
- Significant data synchronization concerns.
- Data access and availability issues for key databases.

4.1.2 Target Enterprise Data Environment for Mission-critical AIS

A three-step process was used to define the Target Enterprise Data Classes:

- First, USACE defined the 64 Baseline USACE Data Classes and rolled them up to a “true” enterprise level. The result was that less than 30 data classes, on an aggregate, spoke to “types of data” at the enterprise level.
- Second, with both of these columns represented in a spreadsheet, a comparison was made to the Civil Works business area ICOM model to ensure that data could be reasonably associated with the data represented as being used on the ICOM models. The idea was to be able to identify any gaps (missing components) in either the functions/subfunctions or the high-level data objects. The result to date is a nonvalidated mapping of USACE Target Enterprise Data Classes to USACE Baseline Data Classes.
- The third step involved adding definitions to the new USACE Enterprise Data Classes for presentation, validation, approval, and use in work products such as the USACE Target Enterprise Data Model (the validation is in progress).

The chart provided in Appendix J, Section J.6, depicts the mapping of USACE Baseline Data Classes to the Target Enterprise Data Classes.

The USACE Target Enterprise Data Model is a “notional” data model in that given the strategic plans available, it seeks to establish some basic concepts and principles that can be associated with building and managing data objects in the environment. As such, it is not geared toward meeting an atomic data and processing requirement. That will come later when more detail on processes and data have been determined. This model, in conjunction with the strategic plans, is meant to be used to facilitate the establishment of principles and guidance in this arena. The data model is provided in Appendix J, Section J.7.

4.2 Data Sharing Framework

The Data Sharing Framework (DSF) (Figure 4.1) is described in terms of technical layers whereby each layer provides specific functionality required to make data/information usable across USACE.

The top level of the framework is the set of USACE applications that require access to the data. These applications range from simple desktop screening level tools to commercial GIS software operating on a shared server, to multidimensional models operating in a supercomputing environment. The challenge is to develop a framework that will support data accessibility by all of these applications. The layers that compose the framework are described in Appendix K. Technical standards and guidelines for system development and acquisition are provided in the **CeA-TRM**.

This framework is intended to provide a description of the elements that should be considered when access to a data source is required by multiple USACE applications. The Data Categorization section, Section 4.3, should be consulted to determine if a corporate data access solution already exists.

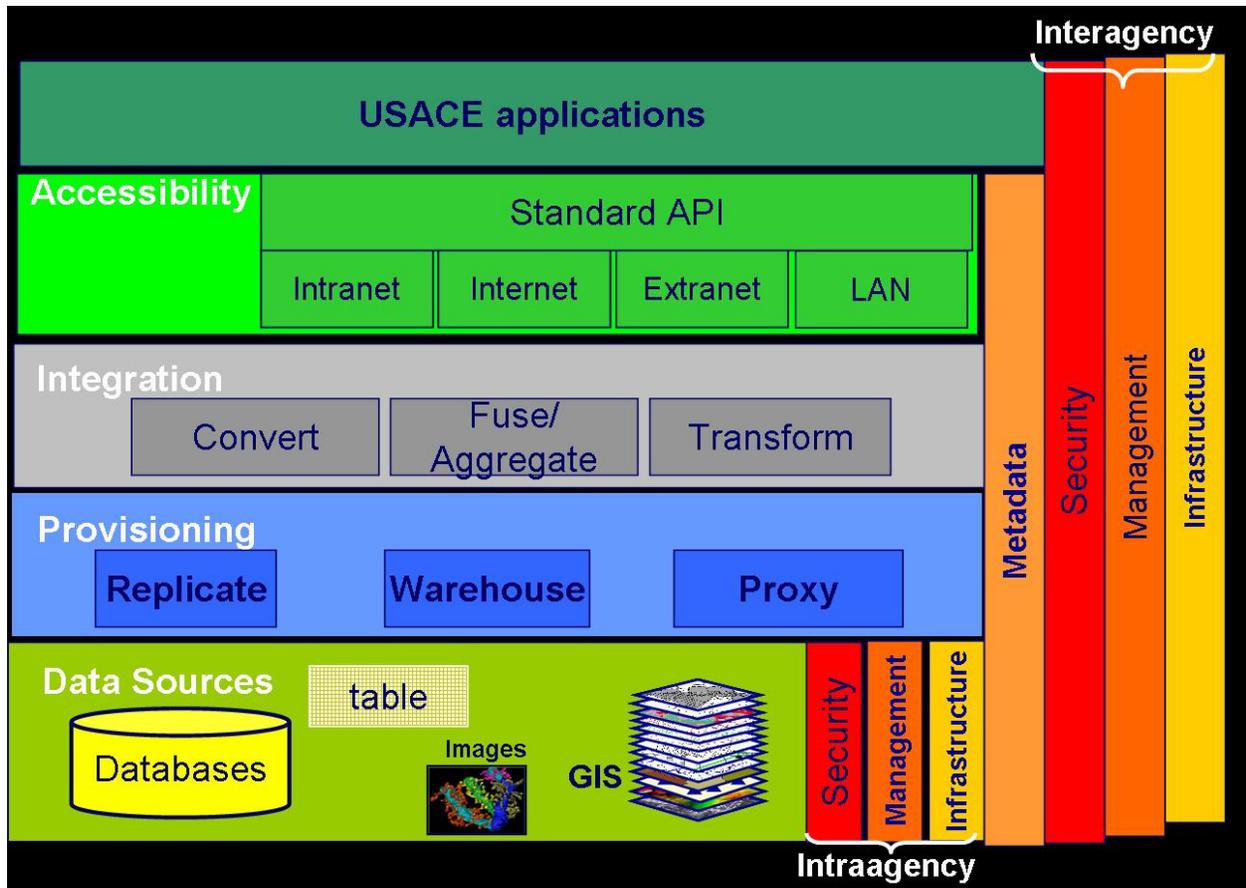


Figure 4.1. Data Sharing Framework

4.3 Categorization of Data

Digital data is used by USACE to support S&E, Asset Management, Emergency Operations, Business Management, Acquisition Management, Real Estate, and Financial Management. This section describes at an aggregate level the data that support USACE programs and business line operations, establishes a commonly understood classification of USACE data, and facilitates the identification of existing data resources. While there could be many different categorization schemes for USACE data, this categorization was based loosely on the 2005 organization of USACE Business Cases for OMB. It is expected that the categorization will evolve as users provide feedback regarding its usefulness. The basic categorization is provided in Table 4.1. The details of each data category are provided in Appendix L.

Table 4.1. Basic Categorization of Data

Primary Category	Subcategory
Science & Engineering	Cost engineering
	Structural engineering
	Construction specifications
	Design
	Hydro
	Environmental
	Infrastructure
	Climate
	Soils
	Landform
	Land use/vegetation
	Maps/imagery
Real Estate	Appraisal
	Planning and control
	Acquisition
	Leasing
	Management
	Disposal
	Relocation Assistance
Financial Management	Contracts
	Labor
Emergency Operations	Project-specific
	Scientific
	Financial
	Geospatial
	Personnel
Asset Management	Facilities and Equipment
	Personal Property
	Infrastructure
	Vehicles
Acquisition Management	Construction/engineering contracting
Business Management	Project Management
	Civil Works Operations and Maintenance
	Construction

Chapter 5 – Service Component Reference Model (SRM)



The Service Component Reference Model (SRM) will be used to assess automated information systems and other service components like IT production and management tools in use through the organization. The **CeA** PDT put it this way:

“USACE Applications and IT tools must be business-driven, but to understand their relative importance they must be sorted in some sort of functional framework with subclassifications, in line with USACE business and/or performance objectives.”

The SRM will also be used in the development of USACE IT capital investment business cases the USACE submits to OMB each year as part of the Civil Works budget submission. As part of each business case, the USACE will map the IT initiative to the appropriate USACE Service Domain(s), Service Type(s), and Component(s). A description of how the initiative supports the line of business and subfunctions identified within the BRM will also be included in the business case.

- **Service Domains** – Represent the highest level of the SRM. They provide a high-level view of the services and capabilities that support enterprise and organizational processes and applications.
- **Service Types** – Represent a “drilled-down” view of the Service Domains. The Service Types further categorize and define the capabilities of a Service Domain. They are intended to define the second level of detail that describes a business-oriented service.
- **Components** – Represent the lowest level of the organization as described within the Service Domain and are depicted visually within the Service Type. Per the OMB Federal Enterprise Architecture Program Management Office (FEAPMO) SRM, a Component is defined as “a self-contained business process or service with predetermined functionality that may be exposed through a business or technology interface.”

The SRM components are shown in Figure 5.1 (see Appendix O for readable version).

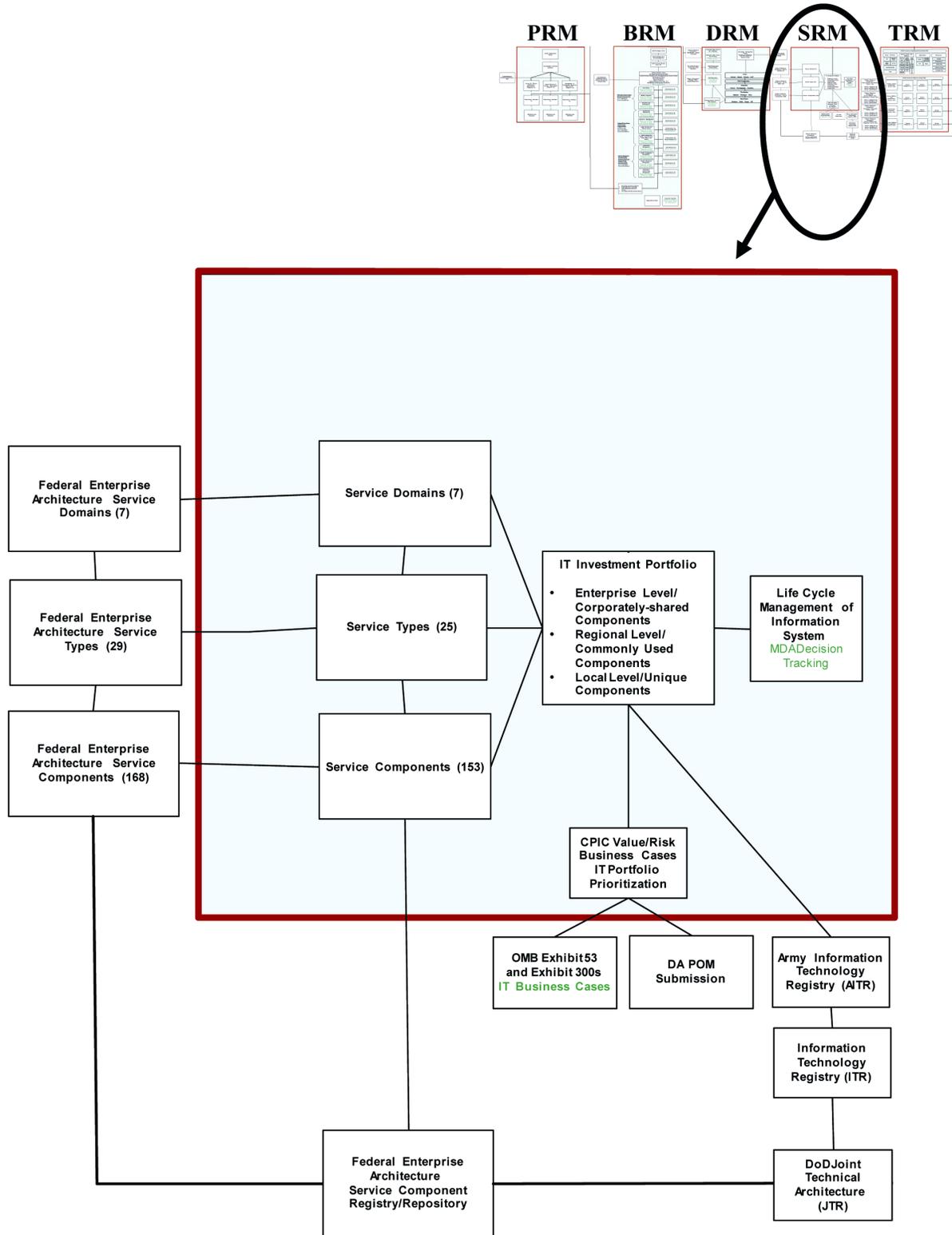


Figure 5.1. SRM components

The SRM is constructed as a hierarchy of Service Domains, Service Types, and Components as shown in Figure 5.2.

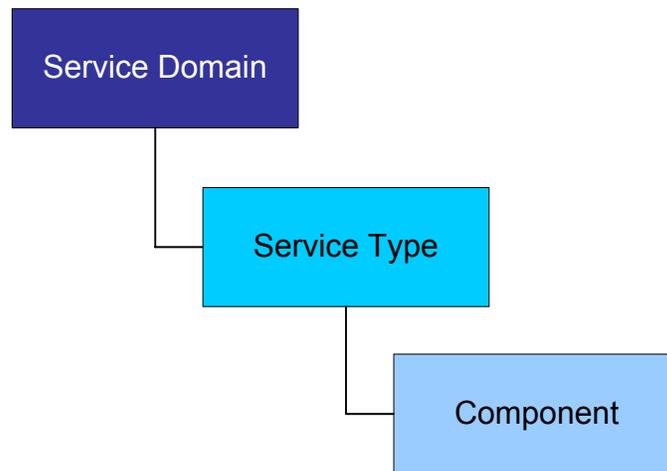


Figure 5.2. SRM hierarchy

The SRM is designed to be independent of the USACE business functions. This allows it to be applicable horizontally across service areas providing a leverageable foundation for reuse of applications, application capabilities, components, and business activities. The SRM outlines the following seven main Service Domains of the Federal Government, was used by USACE to develop the **CeA** SRM:

- **Customer Services Domain** – Consists of the capabilities that are directly related to the end customer, the interaction between the business and the customer, and the customer-driven activities or functions. It consists of 3 Service Types and 21 Components.
- **Process Automation Services Domain** - Consists of the capabilities that support the automation of process and management activities that assist in effectively managing the business. It consists of 2 Service Types and 5 Components.
- **Business Management Services Domain** - Consists of the capabilities that support the management and execution of business functions and organizational activities that maintain continuity across the business and value-chain participants. It consists of 4 Service Types and 20 Components.
- **Digital Asset Services Domain** - Consists of the capabilities that support the generation, management, and distribution of intellectual capital and electronic media across the business and extended enterprise. It consists of 4 Service Types and 25 Components.
- **Business Analytical Services Domain** – Consists of the capabilities that support the extraction, aggregation, and presentation of information to facilitate decision analysis and business evaluation. It consists of 4 Service Types and 19 Components.

- **Back Office Services Domain** - Consists of the capabilities that support the management of enterprise planning and transactional-based functions. It consists of 6 Service Types and 47 Components.
- **Support Services Domain** - Consists of the cross-functional capabilities that can be leveraged independent of Service Domain objective or mission. It consists of 6 Service Types and 31 Components.

These 7 Service Domains comprise a total of 29 Service Types and 168 Components as illustrated on the following pages. See Appendix J for more detailed information on Service Types and Components that apply to USACE.

5.1 Customer Services – Service Domain

The Customer Services Domain consists of the capabilities that are directly related to an internal or external customer, the interaction of the business with the customer, and the customer-driven activities or functions. The customer Services domain represents those capabilities and services that are at the front end of a business, and interface at varying levels with the customer. Figure 5.3 illustrates the USACE Service Types and Components for the “Customer Services” Domain, described as follows:

- **Customer Initiated Assistance Service Type.** Defines the set of capabilities that allow customers to seek assistance and service proactively from an organization.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Customer Services Domain and Customer Initiated Assistance Service Type:

- Real Estate Management Program
- Corps of Engineers Financial Management Services Program

- **Customer Preferences Service Type.** Defines the set of capabilities that allow an organization’s customers to change a user interface and the way that data is displayed.

None of the FY05 Business Cases address this Service Type.

- **Customer Relationship Management Service Type.** Defines the set of capabilities that are used to plan, schedule, and control the activities between the customer and the enterprise both before and after a product or service is offered.

Applicable FY05 Business Cases. The following business case submitted for FY05 funding pertain to the Customer Services Domain and Customer Relationship Management Service Type:

- Real Estate Management Program

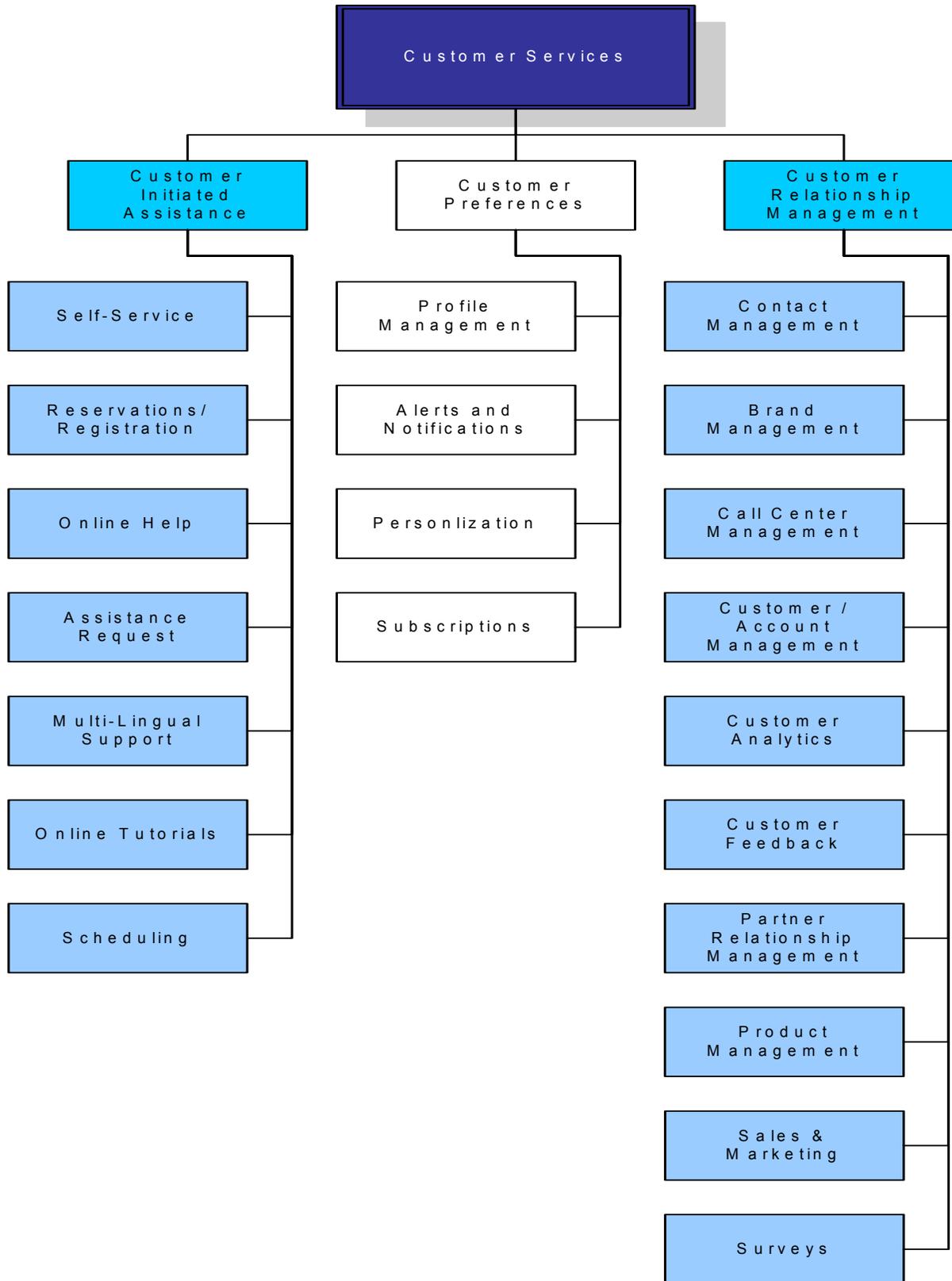


Figure 5.3. Customer Services Domain

5.2 Process Automation Service Domain

The Process Automation Services Domain consists of the capabilities that support the automation of process and management activities that assist in effectively managing the business. The Process Automation Services domain represents those services and capabilities that serve to automate and facilitate the processes associated with tracking, monitoring, and maintaining liaison throughout the business cycle of an organization. Figure 5.4 illustrates the USACE Services Types and Components for the “Process Automation Services” Domain, described as follows:

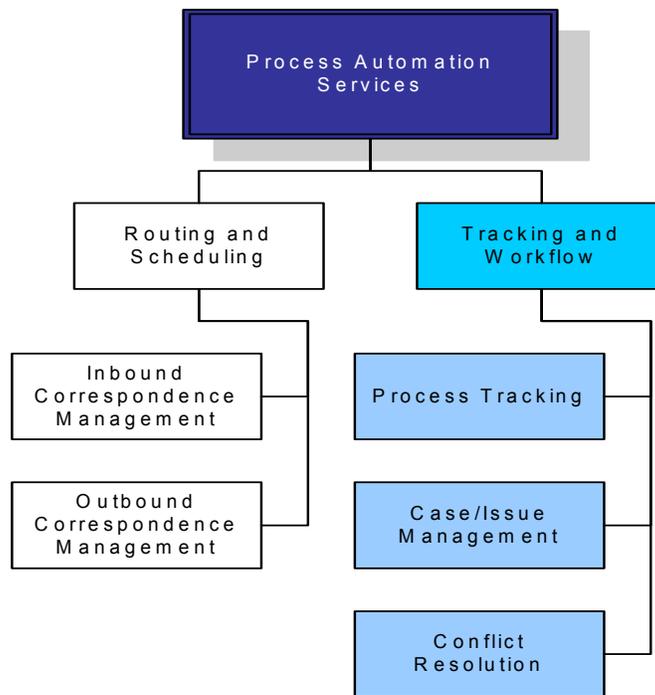


Figure 5.4. Process Automation Services Domain

- Routing and Scheduling Service Type.** Defines the set of capabilities for the automatic directing, assignment, or allocation of time for a particular action or event.

None of the FY05 Business Cases address this Service Type.

- Tracking and Workflow Service Type.** Defines the set of capabilities for automatic monitoring and routing of document to the users responsible for working on them to support each step of the business cycle.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Process Automation Services Domain and Tracking and Workflow Service Type:

- Asset Management Services Program
- Business Management Tools Program

5.3 Business Management Services Domain

The Business Management Services Domain consists of the capabilities that support the management and execution of business functions and organizational activities that maintain continuity across the business and value-chain participants. The Business Management Services domain represents those capabilities and services that are necessary for projects, programs, and planning within a business operation to be successfully managed. Figure 5.5 illustrates the USACE Service Types and Components for the “Business Management Services” Domain, described as follows:

- **Investment Management Service Type.** Defines the set of capabilities that manage the financial assets and capital of an organization.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Business Management Services Domain and Investment Management Service Type:

- Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
- Real Estate Management Program via REMIS
- Business Management Tools Program

- **Management of Process Service Type.** Defines the set of capabilities that regulate the activities surrounding the business cycle of an organization.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Business Management Services Domain and Management of Process Service Type:

- Science, Engineering and Technology
- Real Estate Management Program
- Asset Management Services Program
- Business Management Tools Program

- **Organizational Management Service Type.** Defines the set of capabilities that support both collaboration and communication within an organization.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Business Management Services Domain and Organizational Management Service Type:

- Business Management Tools Program

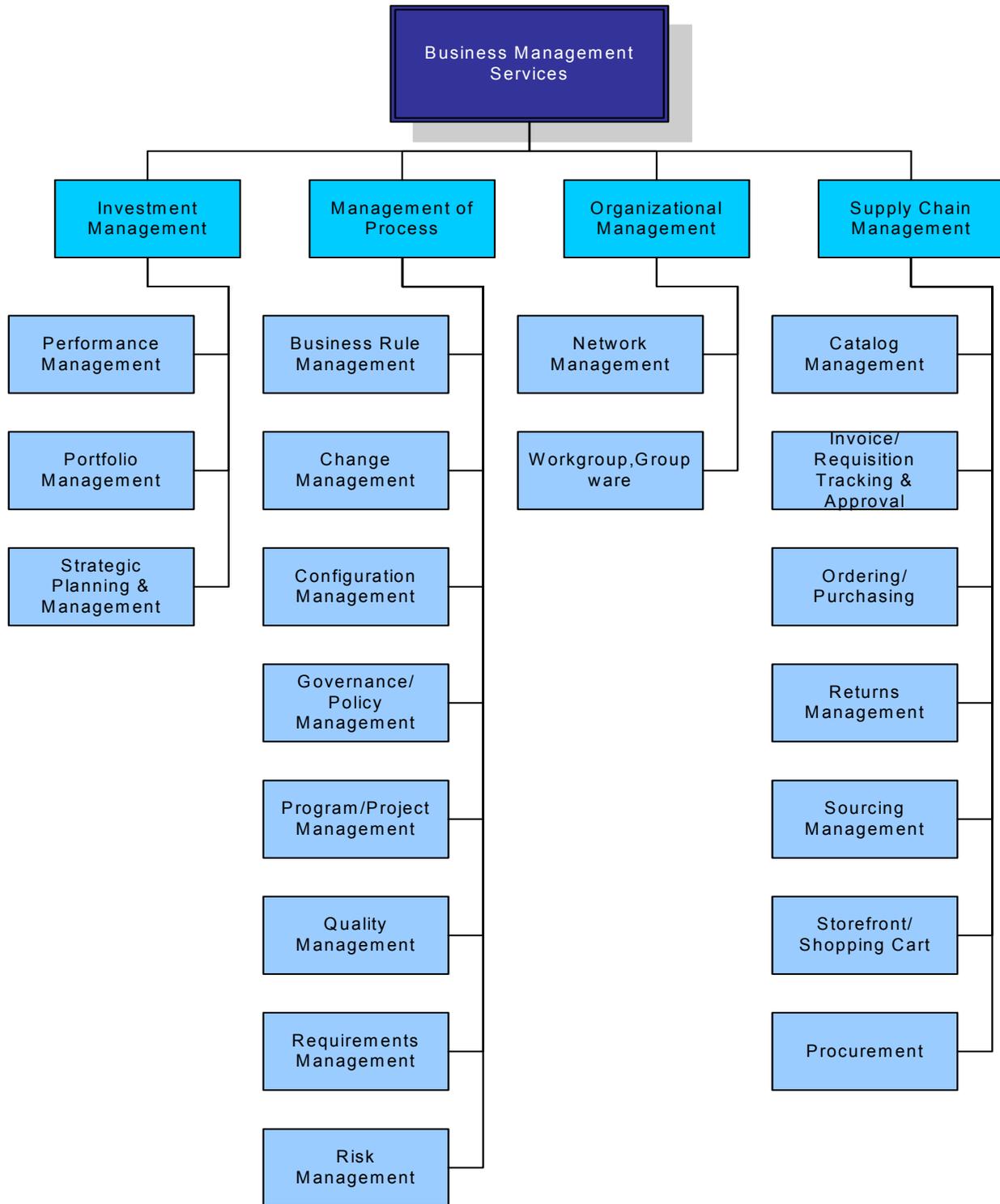


Figure 5.5. Business Management Services Domain

- **Supply Chain Management Service Type.** Defines the set of capabilities for planning, scheduling, and controlling a supply chain and the sequence of organizations and functions that mine, make, or assemble materials and products from manufacturer to wholesaler to retailer to consumer.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Business Management Services Domain and Supply Chain Management Service Type:

- Acquisition Services Program
- Asset Management Services Program

5.4 Digital Asset Services Domain

The Digital Asset Services Domain consists of the capabilities that support the generation, management, and distribution of intellectual capital and electronic media across the business and extended enterprise. Figure 5.6 illustrates the USACE Service Types and Components for the “Digital Asset Services” Domain, described as follows:

- **Content Management Services Type.** Defines the capabilities that manage the storage, maintenance, and retrieval of documents and information of a system or Web site.

None of the FY05 Business Cases address this Service Type.

- **Document Management Service Type.** Defines the set of capabilities that control the capture and maintenance of documents and files.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Digital Asset Services Domain and Document Management Service Type:

- Science, Engineering and Technology
 - Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
 - Acquisition Services Program
 - Business Management Tools Program
- **Knowledge Management Service Type.** Defines the set of capabilities that support the identification, gathering, and transformation of documents, reports and other sources into meaningful information.

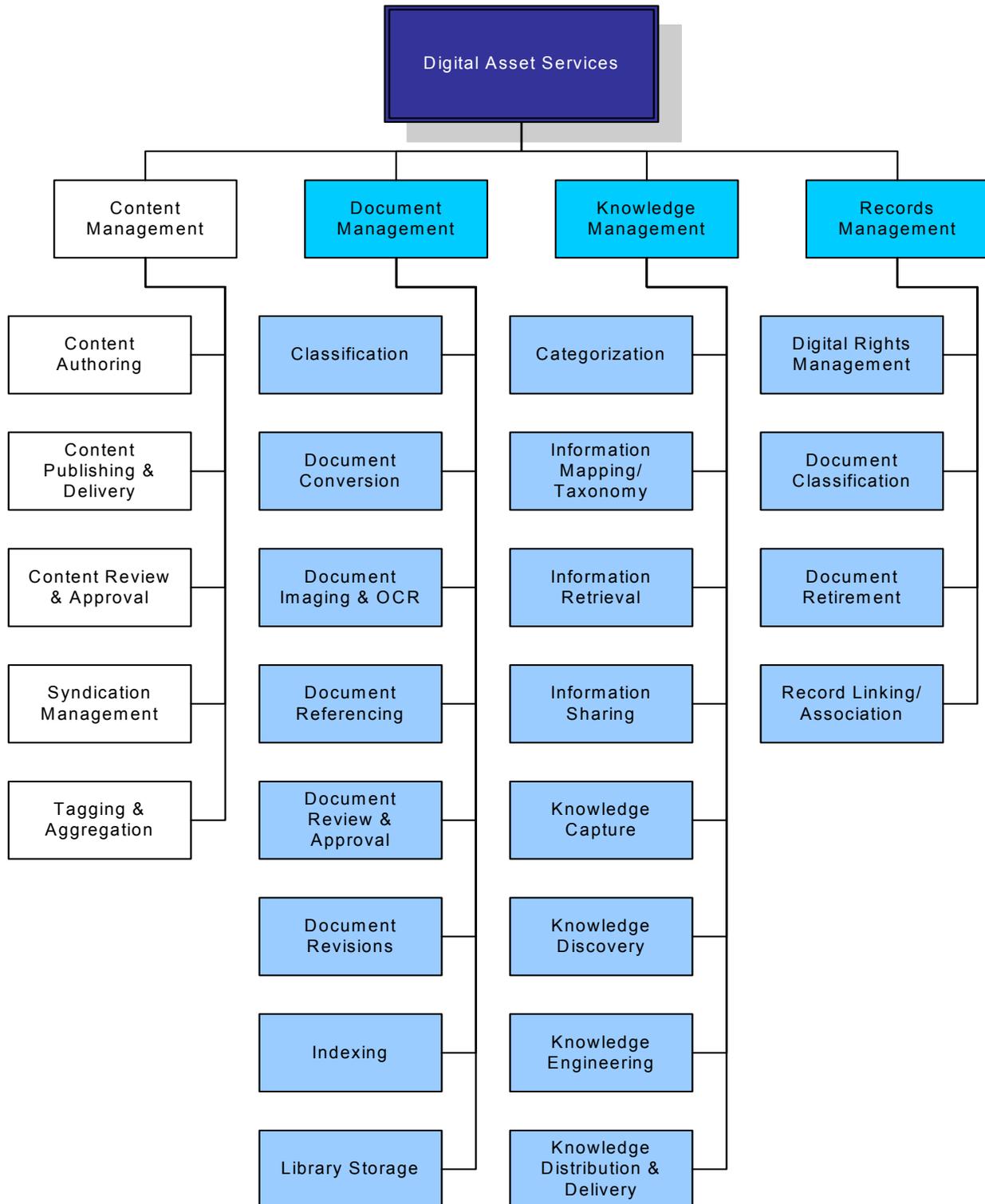


Figure 5.6. Digital Assets Services Domain

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Digital Asset Services Domain and Knowledge Management Service Type:

- Science, Engineering and Technology
 - Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
 - Real Estate Management Program
 - ENGLink
 - Asset Management Services Program
 - Business Management Tools Program
 - Corps of Engineers Financial Management Services Program
- **Records Management Service Type.** Defines the set of capabilities to support the storage, protection, archiving, classification, and retirement of documents and information.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Digital Asset Services Domain and Records Management Service Type:

- Science, Engineering and Technology
- Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
- Real Estate Management Program
- Acquisition Services Program
- Business Management Tools Program

5.5 Business Analytical Services Domain

The Business Analytical Services Area consists of the capabilities that support the extraction, aggregation, and presentation of information to facilitate decision analysis and business evaluation. Figure 5.7 illustrates the USACE Service Types and Components for the “Business Analytical Services” Domain, described as follows:

- **Analysis & Statistics Services Type.** Defines the set of capabilities that support the examination of business issues, problems, and their solutions.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Business Analytical Services Domain and Analysis and Statistics Service Type:

- Science, Engineering and Technology
- ENGLink
- Asset Management Services Program
- Business Management Tools Program

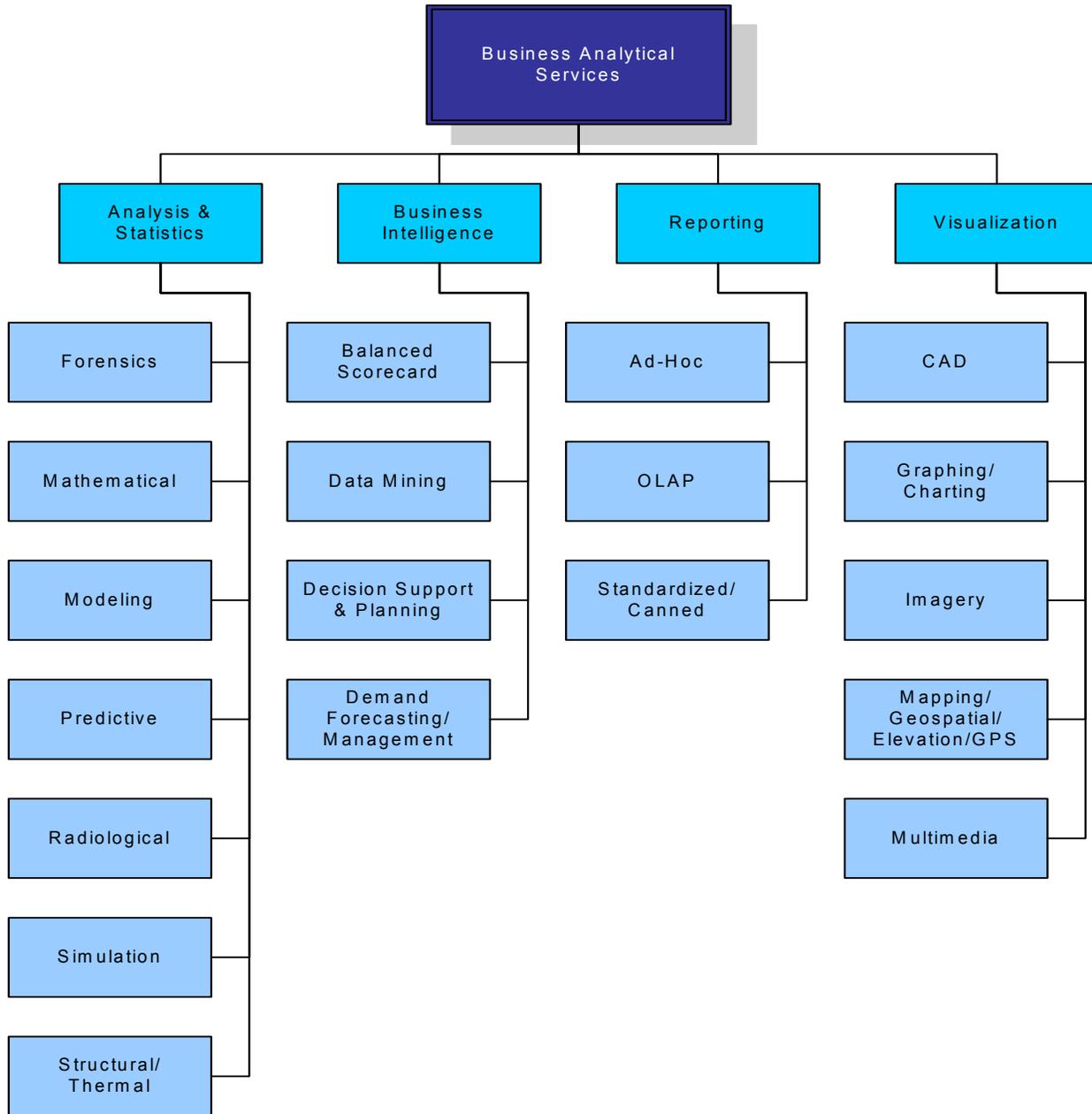


Figure 5.7. Business Analytical Services Domain

- Business Intelligence Service Type.** Defines the set of capabilities that support information that pertains to the history, current status, or future projections of an organization.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Business Analytical Services Domain and Business Intelligence Service Type:

- Science, Engineering and Technology
 - Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
 - ENGLink
 - Asset Management Services Program
 - Acquisition Services Program
 - Business Management Tools Program
 - Corps of Engineers Financial Management Services Program
- **Reporting Service Type.** Defines the set of capabilities that support the organization of data into useful information.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Business Analytical Services Domain and Reporting Service Type:

- Science, Engineering and Technology
 - Real Estate Management Program
 - Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
 - ENGLink
 - Asset Management Services Program
 - Business Management Tools Program
 - Corps of Engineers Financial Management Services Program
- **Visualization Service Type.** Defines the set of capabilities that support the conversion of data into graphical or picture form.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Business Analytical Services Domain and Visualization Service Type:

- Science, Engineering and Technology
- Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
- ENGLink

5.6 Back Office Services Domain

The Back Office Services Domain consists of the capabilities that support the management of enterprise planning transactional-based functions. Figure 5.8 illustrates the USACE Service Types and Components for the “Back Office Services” Domain, described as follows:



Figure 5.8. Back Office Services Domain

- **Assets/Materials Management Service Type.** Defines the set of capabilities that support the acquisition, oversight and tracking of an organization's assets.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Back Office Services Domain and Assets/Materials Management Service Type:

- Science, Engineering and Technology
- Real Estate Management Program
- Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
- ENGLink
- Asset Management Services Program
- Business Management Tools Program

- **Data Management Service Type.** Defines the set of capabilities that support the usage, processing, and general administration of unstructured information.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Back Office Services Domain and Data Management Service Type:

- Science, Engineering and Technology
- Real Estate Management Program
- Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
- ENGLink
- Business Management Tools Program
- Corps of Engineers Financial Management Services Program

- **Development & Integration Service Type.** Defines the set of capabilities that support the communication between hardware and software applications and the activities associated with deployment of software applications.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Back Office Services Domain and Development and Integration Service Type:

- Science, Engineering and Technology
- Consolidated Information Technology Infrastructure/Office Automation/Telecommunications

- **Financial Management Service Type.** Defines the set of capabilities that support the accounting practices and procedures that allow for the handling of revenues, funding, and expenditures.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Back Office Services Domain and Financial Management Service Type:

- Science, Engineering and Technology
 - Real Estate Management Program
 - Asset Management Services Program
 - Business Management Tools Program
 - Corps of Engineers Financial Management Services Program
- **Human Capital/Workforce Management Service Type.** Defines the set of capabilities that support the planning and supervision of an organization’s personnel.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Back Office Services Domain and Human Capital/Workforce Management Service Type:

- ENGLink
- Business Management Tools Program

- **Human Resources Service Type.** Defines the set of capabilities that support the recruitment and management of personnel.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Back Office Services Domain and Human Resources Service Type:

- Corps of Engineers Financial Management Services Program

5.7 Support Services Domain

The Support Services Area consists of the cross-functional capabilities that can be leveraged independent of Service Domain objective (and) or mission. Figure 5.9 illustrates the USACE Service Types and Components for the “Support Services” Domain, described as follows:

- **Collaboration Service Type.** Defines the set of capabilities that allow for the concurrent, simultaneous communication and sharing of content, schedules, messages, and ideas within an organization.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Support Services Domain and Collaboration Service Type:

- Business Management Tools Program

- **Communication Service Type.** Defines the set of capabilities that support the transmission of data, messages, and information in multiple formats and protocols.

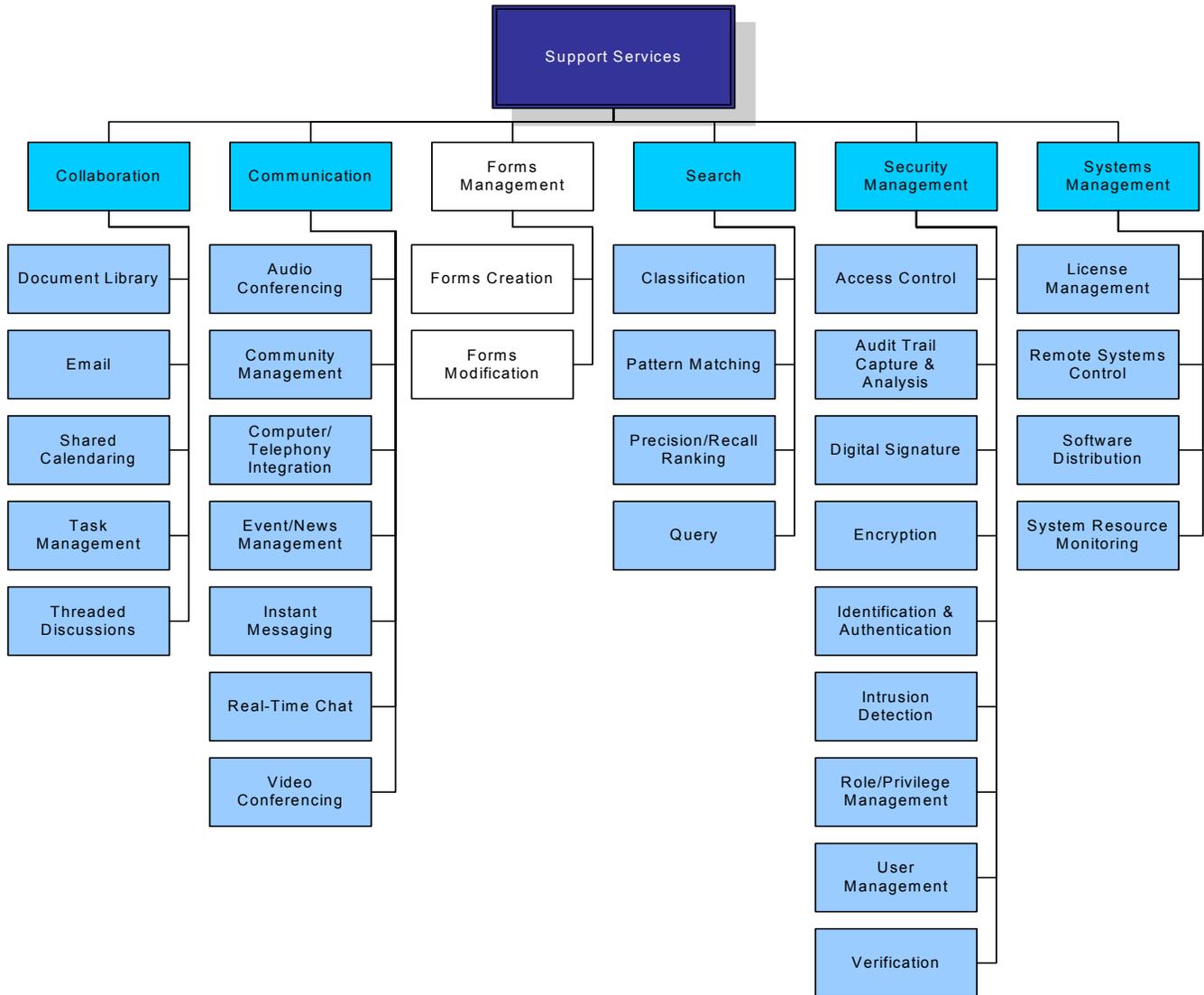


Figure 5.9. Support Services Domain

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Support Services Domain and Communication Service Type:

– Business Management Tools Program

- **Forms Management Service Type.** Defines the set of capabilities that support the creation, modification, and usage of physical or electronic documents used to capture information within the business cycle.

None of the FY05 Business Cases address this Service Type.

- **Search Service Type.** Defines the set of capabilities that support the probing and lookup of specific data from a data source.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Support Services Domain and Search Service Type:

- REMP
- Consolidated Information Technology Infrastructure/Office Automation/Telecommunications

- **Security Management Service Type.** Defines the set of capabilities that support the protection of an organization’s hardware, software, and related assets.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Support Services Domain and Security Management Service Type:

- REMP
- Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
- ENGLink

- **Systems Management Service Type.** Defines the set of capabilities that support the administration and upkeep of an organization’s technology assets, including the hardware, software, infrastructure, licenses, and components that make up those assets.

Applicable FY05 Business Cases. The following business cases submitted for FY05 funding pertain to the Support Services Domain and Systems Management Service Type:

- Consolidated Information Technology Infrastructure/Office Automation/Telecommunications
- ENGLink

The populated SRM is available in Appendix O.

Chapter 6 – Technical Reference Model (TRM)



The **CeA**–TRM provides the technical perspective of how technology is assembled to support the USACE. As such, it has two mutually supporting objectives. The first and foremost objective is to provide the foundation for a seamless flow of information and interoperability among all USACE systems that produce, use, or exchange information electronically. The second objective is to define standards and guidelines for system development and acquisition that will dramatically reduce cost, development time, and fielding time for improved systems. The **CeA** PDT put it this way:

“The TRM prescribes parameters, governance and preferred products that must be used in making informed decisions about the future work environment.”

The **CeA**–TRM is based on a subset of the comprehensive, standards-based Joint Technical Architecture–Army and the Federal Enterprise Architecture Framework, with appropriate standards modification in support of the USACE Civil Works and DoD missions. Furthermore, it provides a common technical baseline consistent with the DoD Net-Centric activities.

The TRM (Figure 6.1) is the minimal set of design principles, technologies, standards, preferred products, and configurations that govern the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. More specifically, the TRM provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are built, and products are developed. This includes a collection of the technical standards, conventions, rules, and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular system architecture views and that relate to particular operational views. See Appendix P for working draft of the TRM.

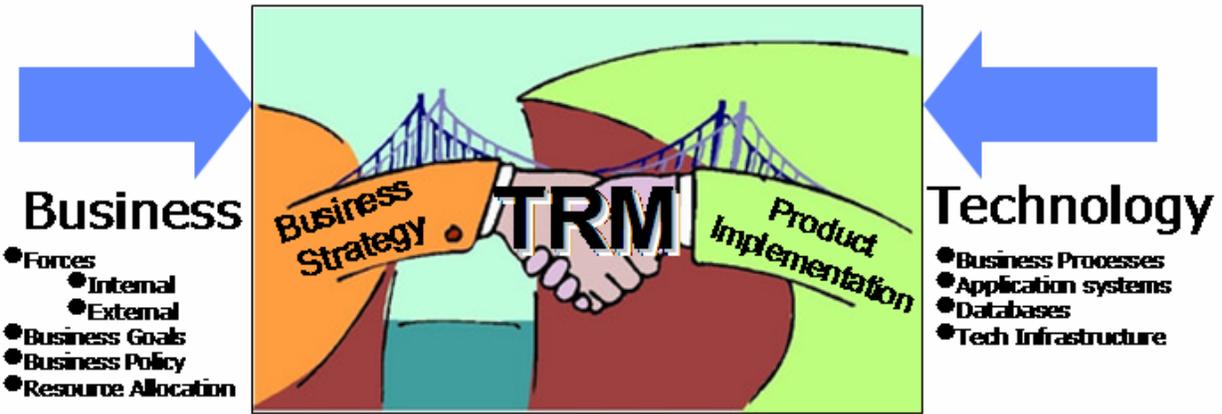
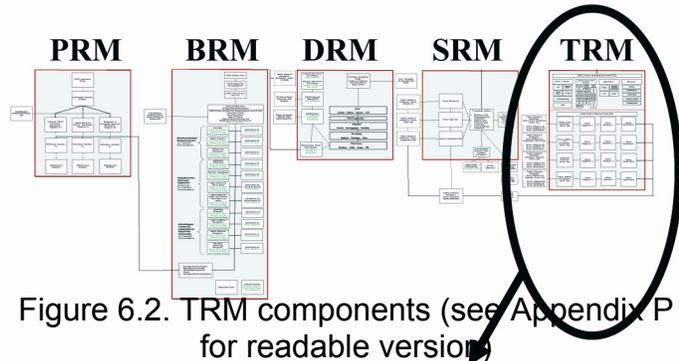


Figure 6.1. TRM

6.1 Technical Reference Model (TRM) Components

The technical direction of the TRM represents the evolving implementation of the OMB's e-Government recommendations to develop a strong, enforceable technical architecture with a heavy emphasis on commercial standards and profiles. The intent is to achieve interoperability while reducing cost by leveraging the large investment industry has made in developing and implementing standards-based technologies that are in widespread use.



Every effort has been made to avoid closed commercial or military-unique standards. Standards are based primarily on commercial "open systems" technologies (open systems approach) that are being commonly used throughout the DoD and industry. Military standards are used only where absolutely necessary. A hierarchy of standards by family was developed to guide selection of specific standards for incorporation into this version of the TRM. The general order of preference, subject to modifications due to specific operational interoperability requirements and acceptance in the commercial marketplace (market acceptance), was standards specified by neutral standard groups such as the Institute of Electrical and Electronics Engineers (IEEE) or International Organization for Standardization (ISO), followed by industry consortiums such as the World Wide Web Consortium (W3C), then vendor standards that are so widely supported as to be de facto industry standards, and finally government standards such as Federal Information Processing Standards (FIPS) and Military Standards (MIL-STDs). Several activities both inside and outside the USACE, listed in Table 6.1, contribute to the evolution of the TRM.

Table 6.1. Organizations or Activities That Impact the TRM

Organizations or Activities That Impact the TRM	Description
Federal Enterprise Architecture-TRM (FEA-TRM)	Federal Enterprise Architecture – Technical Reference Model http://www.feapmo.gov/featrm2.asp
U.S. Army Corps of Engineers ER 5-1-11	U.S. Army Corps of Engineers Business Process
Federal Information Processing Standards (FIPS)	Standards, guidelines, and technical methods developed by the National Institute of Standards (NIST). Some required standards or specifications have gone through rigid validation testing and accreditation. NIST frequently adopts standards that have been developed by national and international voluntary industry standard organizations. The use of voluntary industry standards enables the Federal government to acquire commercial-off-the-shelf (COTS) technology and to avoid the costs of developing its own standards.
International Organization for Standardization (ISO)	A non-governmental organization established in 1947 that sets international standards. It is a worldwide federation for national standards bodies from some 100 countries. Its mission is to promote the development of standardization and related activities in the world and to develop cooperation in the areas of intellectual, scientific, technological, and economic activities.
Army Knowledge Online (AKO)	A repository of Army knowledge and collaborative resources
Office of Management and Budget (OMB)	Requires the formalization of architecture practices
General Accounting Office (GAO)	Guidelines for processing of financial data within the Federal government
Army Enterprise Information Transport Reengineering Working Group (AEIT-RWG)	Effort to re-design Army-wide networking at the transport layer
Army Knowledge Management (AKM)	Strategic goals and objectives to improve the decision dominance of the Army
Network Command (Netcom)	New entity as part of AKM initiatives
Joint Technical Architecture-Army (JTA-A)	The Army's technical architecture. Version 6.5 was used in the development of the CeA -TRM.
World Wide Web Consortium (W3C)	Develops interoperable technologies (specifications, guidelines, software, and tools) for the World Wide Web (www).
Common Delivery Framework (CDF)	A managed set of corporate assets (guidance, software, catalogs, data linkages, etc.) that provide capabilities for development and delivery of information and technology. https://cdf.usace.army.mil/index.jsp

6.2 Role of the TRM

- Response to changing business needs is faster.
- Architecture has available blueprints on current IT environment.
- IT-related decision making can progress faster with lengthy fact gathering minimized.
- Integrated solutions are easier to visualize.
- Blueprints readily highlight overlooked or missed information, which translates into opportunities for IT solutions.
- Architecture framework provides USACE with a readily available pool of knowledgeable IT resources for quick and informed decision making.
- Application of key technology standards is consistent.
- Economies of scale are clear across USACE.
- Resource sharing highlights common areas.
- Market research of emerging technologies is shared enterprisewide.
- Attention is often concentrated on “bleeding edge” technology; this has resulted in wasted time and effort.
- The architecture focuses on proven market technologies.

6.3 Guiding Principles That Drive Development of the TRM

- Align technology investments with business objectives.
- Promote the use of industry leading practices.
- Eliminate duplication, incompatibility, and redundancy of systems and data.
- Provide information integrity.
- Capture and validate information once; then reuse it across the enterprise.
- Place greater significance on cooperative strategies for satisfying the common needs of multiple business lines across USACE.
- Incorporate standards that promote “open systems,” provide a seamless integration, and establish an enterprisewide perspective.
- Create consistent enterprise architecture products that are at a sufficient level of detail to be implementable.
- Accelerate sound decision making.
- Provide security and protection of sensitive information.
- Reduce the total cost of ownership.

- Reuse before buying; buy before building, utilizing industry standards.
- Standardize business rules, processes, and information across the enterprise.

6.4 Target Audience

The purpose of this document is to define a common technical model to aid in the development and purchase of technology. Over time, technology will become consistent and better aligned with the USACE business goals. Benefactors of the TRM are:

- Program Managers (PMs) – responsible for assembling commercial off-the-shelf (COTS) or government off-the-shelf (GOTS) technology to support the implementation of a project or program that may require cross-agency collaboration and the reuse of agency assets.
- System Developers – responsible for building/assembling systems and selecting technologies and standards that leverage existing assets and services across the Government and industry.

6.5 Alignment with Business Objectives and Goals

In terms of the TRM, business alignment refers to the arrangement of business objectives and goals with the technical baseline of the organization. The purpose of alignment is to focus people, money, and time on technical issues that will result in technology investments that yield value to the business aspects of USACE. Business value is generated in terms of reduction in cost of doing business and/or technology that directly benefits the ability of USACE to perform its mission.

6.5.1 TRM Relationship to the Target Business Reference Model (BRM)

The target BRM drives the target TRM. One input from the BRM team that drives the target TRM is referred to as the TWEs, listed below:

- Enterprise (Corporate-Level) Program and Asset Management.
- Regional Watershed and Installation Management.
- Protection of USACE Critical Infrastructure.
- Integrated Emergency Management.
- Enhanced Communications and Information Access Throughout USACE.
- Enhanced Management of Permits.
- Enterprise Management of Manpower Resources.
- Enterprise and Regional Acquisition Strategy.
- Enterprise Management of Knowledge That Includes Best Practices, Registry of Skills, Customer Feedback, Lessons Learned, Corporate Issues Management, etc.

- Enterprise Processes to Manage Technology and Data.
- Methods for Data Exchange with Government and Industry Partners.
- Internal and External Virtual Teaming.
- One-Stop Web Access to USACE Public Information.

6.5.2 Assess Business Alignment

Architecture alignment with the TRM is critical. This process ensures guidance presented in the TRM directly aligns with strategic plans, goals, and objectives identified in the BRM. The alignment process will use a 2x2 matrix approach to indicate where relationships exist (i.e., TRM guidance support to USACE business objectives) by indicating a point of interaction of the matrix. Rows in the matrix are based on the TWEs, while the columns are based on high level domains of the target TRM. Initially, the goal is to manage the alignment process at a relatively high level of TRM. Future efforts will drill down further into the target TRM to assess a finer level of alignment.

6.6 TRM Practices

TRM practices (Table 6.2) are defined in terms of rules, standards, guidelines, and product descriptions.

Table 6.2. TRM Practices

Practices	Description
Rules	Policies that govern system implementation and operation
Standards	Focusing on commercial and Government technology standards that are supported in the TRM
Guidelines	Communicating general guidance relating to the technical decisions
Preferred Product	COTS or GOTS product that USACE designates for use. It is either a formal or de facto standard-based product or tool that must be used for USACE projects

TRM Profiles

Practices defined within each of the subdomains (Table 6.3) are profiled in terms of their status with respect to the TRM.

Table 6.3. TRM Profiles

Profile Category	Definition
Baseline	Standard or product used in a deployed system. This category represents the highest level of criticality to the architecture. Foundation elements are the most important elements and have the largest impact across the enterprise
Tactical	Standard or product that can be used in a tactical time frame (e.g., 1 to 3 years)
Strategic	Standard or product targeted for use in a strategic time frame (e.g., 3 to 5 years). This serves as a placeholder reserved for future subdomains that are in development or are emerging but not yet populated
Emerging	Product or standard under development and should be re-examined periodically for acceptance
Retirement	Product or standard that was legacy or previously accepted, but should no longer be used

6.7 TRM Sustainment Processes

The TRM processes provide checkpoints during the life cycle of an IT project and manage technical standards that make up the target technical architecture. The TAWG is responsible for managing, governing, facilitating, and assisting in the performance of the TRM through a set of architecture processes. This is in direct support of the USACE IT goals that require oversight on all IT-related investments, whereby projects are approved and managed from an enterprise perspective, and have accountable sponsorship. More specifically, the TAWG is responsible for overseeing the following processes:

- Assess TRM compliance.
- Assess waiver/exception request.
- Conduct standards review.
- Perform new standards research and development (R&D).

In order to effectively apply the TRM, several touchpoints exist where the TAWG must facilitate an assessment, recommendations, and decision process to ensure compliance and to ensure that the TRM is properly evolving to address the needs of USACE and its customers. This process is illustrated in Figure 6.3.

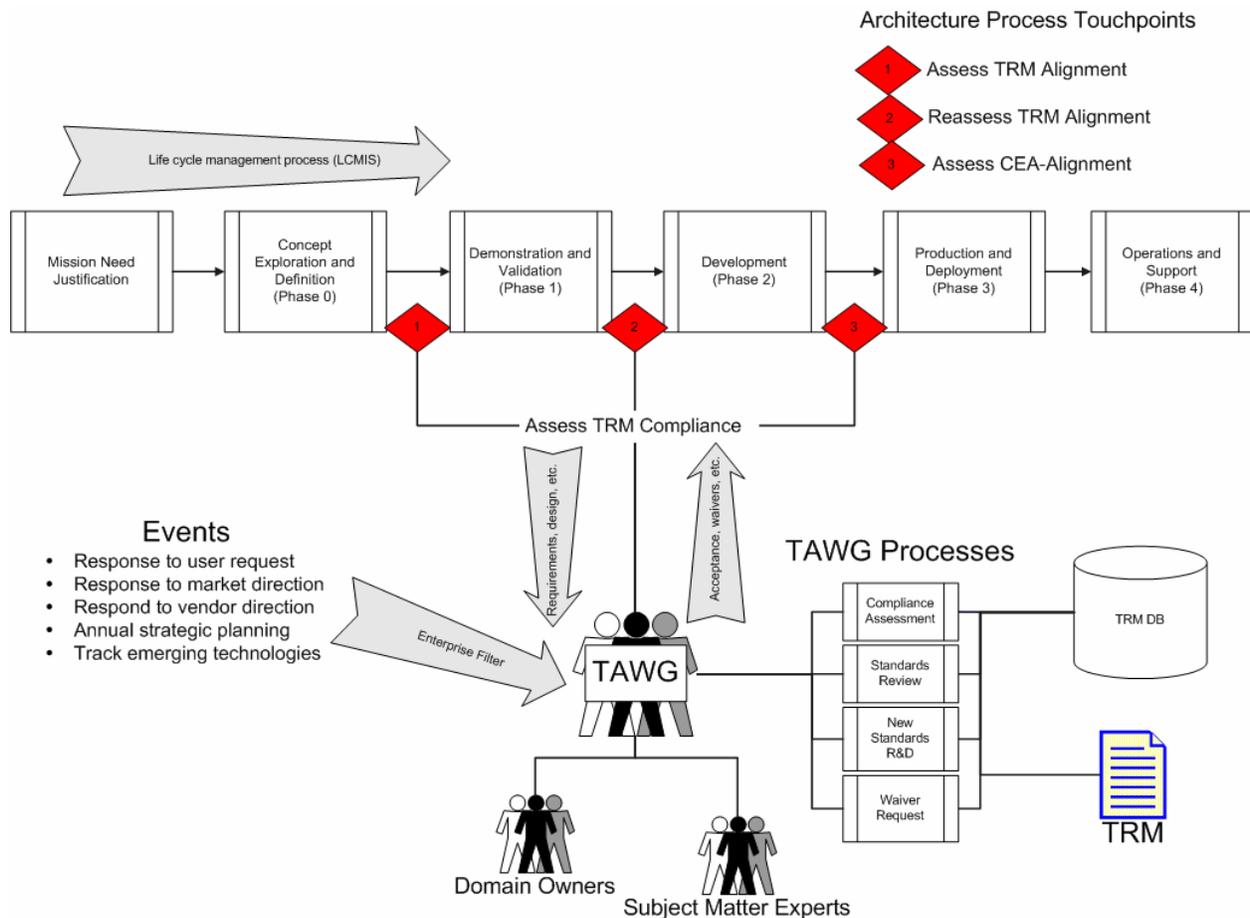


Figure 6.3. TRM alignment process

6.8 Assess TRM Compliance

The purpose of compliance activity is to ensure that the developer properly interpreted the TRM. Assessing technical compliance requires the architect to interpret how well the business, IT, and user requirements are met by the technology design (i.e., application topologies, data architectures, movement versus access strategies, system parameters – reliability, maintainability, mobility, security) and whether the technology selections have conformed to the TRM standards.

The compliance process is executed three times during the life cycle management of information systems (LCMIS) process. The output of the process is to evaluate the level of compliance of the solution being proposed with the standards as defined by the TRM. Upon completion, the TAWG will generate a TRM alignment scorecard and an overall summary to USACE AAA teams.

The standards review process (Figure 6.4), for example, is used to evaluate existing standards to determine if any modifications are necessary to accommodate repetitive exceptions or external technology trends. More specifically, the goal is to keep the TRM current to reflect technology trends and address repeated waiver request.

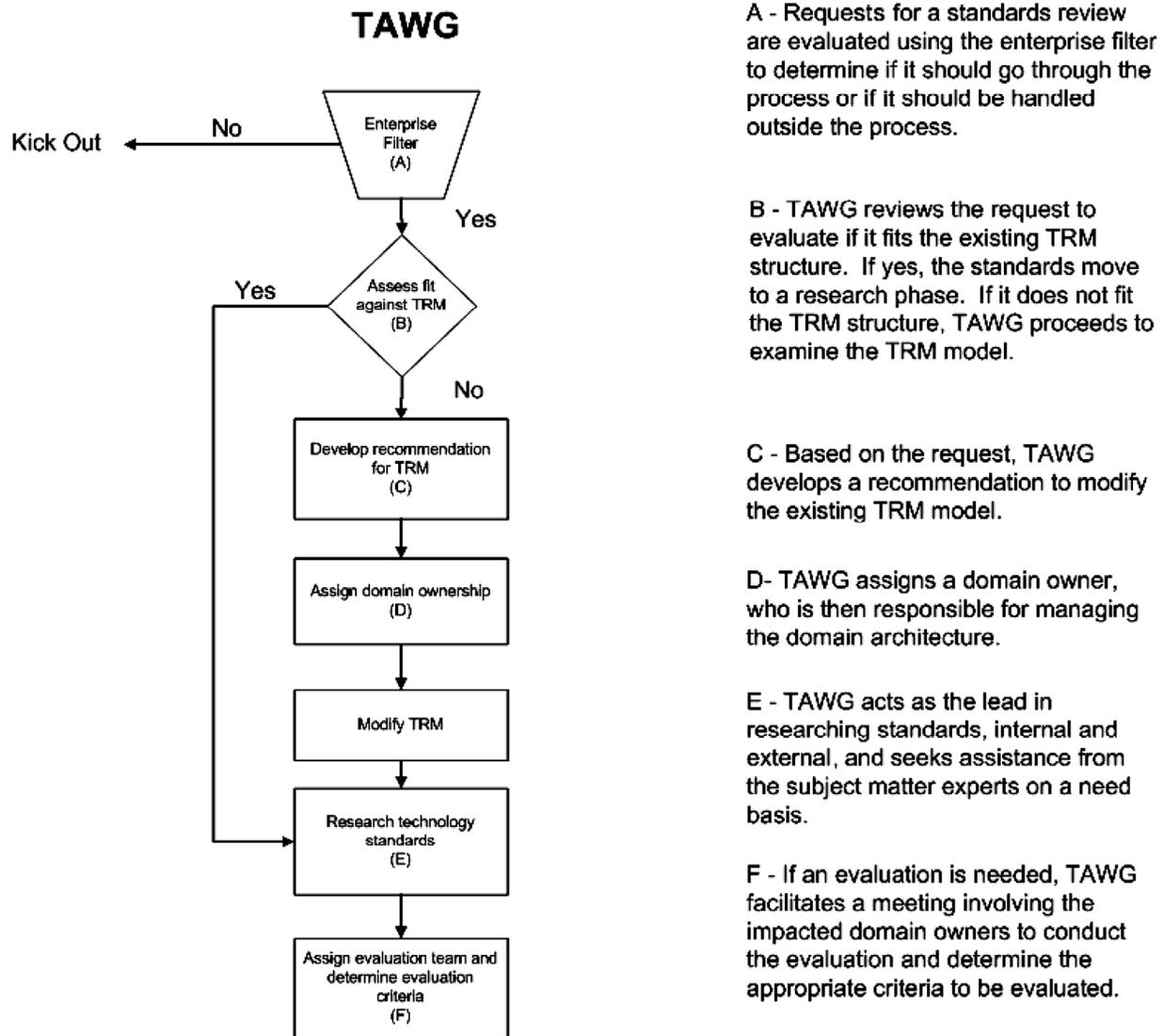


Figure 6.4. Standards review process

6.9 Technical Reference Guides (TRGs)

Technical Reference Guides are organized based on the four service areas identified in the FEA TRM. Service areas represent a technical tier supporting the secure construction, exchange, and delivery of service components. Each service area aggregates and groups standards, specifications, and technologies into lower level functional areas. The four service areas as described by the FEA TRM are:

- Service Access and Delivery – collection of standards and specifications to support external access, exchange, and delivery of service components or capabilities. This area also includes the Legislative and Regulatory requirements governing the access and usage of the service component.
- Service Platform and Infrastructure – collection of delivery and support platforms, infrastructure capabilities, and hardware requirements to support the construction, maintenance, and availability of a service component or capabilities.
- Component Framework – underlying foundation, technologies, standards, and specifications by which service components are built, exchanged, and deployed across component-based, distributed, or service-oriented architectures.
- Service Interface and Integration – collection of technologies, methodologies, standards, and specifications that govern how agencies will interface (both internally and externally) with a service component. This area also defines the methods by which components will interface and integrate with back office/legacy assets.

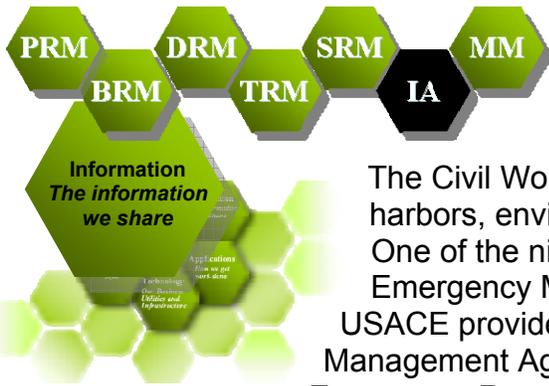
Supporting each service area is a collection of service categories. Service categories are used to classify lower levels of technologies, standards, and specifications with respect to the business or technology function they serve. Each service category is supported by one or more service standards. Service standards are used to define the standards and technologies that support the service category. The final level of the TRM is the service specification layer that provides technical direction for the service standard specification. Service standards are presented in the following six areas:

- Design Principles – general guidance relating to technical decisions.
- Technologies – recommended set of technologies.
- Standards - set of commercial and Government standards required in components associated with the service category.
- Preferred Products – a listing of COTS or GOTS packages used within the service category. Version information is also included.
- Configurations – defines how components with a Service Category are arranged to interoperate with other components inside and outside the service category.
- Status – identifies the standing of the service specification based on the following definitions.

Detailed information associated with TRM is provided in Appendix P.

Chapter 7 – Information Assurance

7.1 Missions of the U.S. Army Corps of Engineers



USACE is the Nation’s primary public engineering agency, with Civil Works, Military Programs, and Research and Development missions (Figure 7.1).

The Civil Works mission includes water control, rivers and harbors, environmental restoration, and power generation. One of the nine high-level Civil Works programs is the Emergency Management and Operations Program, where USACE provided critical support to the Federal Emergency Management Agency (FEMA) and various state and local Emergency Response Centers in dealing with earthquakes, hurricanes, floods, tornadoes, and other disasters including terrorist attacks. See Appendix R for latest Information Assurance Plan of Action and Milestones.

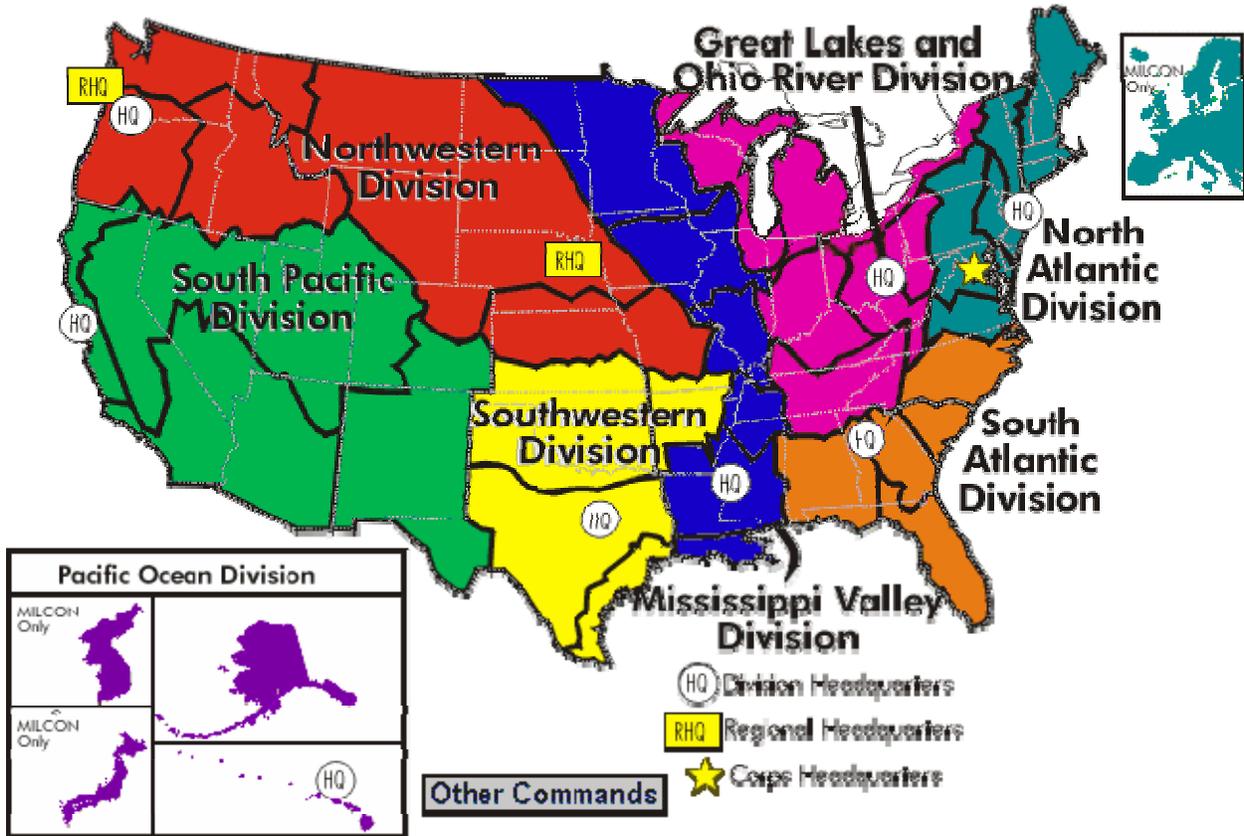


Figure 7.1. Divisions of USACE

The Military Programs mission includes support to the Army, the Air Force, and other Federal agencies for general construction, operations and maintenance, environmental management, and direct military mission support.

The Research and Development mission includes direction of USACE R&D effort for military and Civil Works programs and support-for-others by providing execution direction and oversight in the development, integration, execution, and implementation of R&D conducted by USACE.

The information flow necessary to carry on these activities is supported through the Corps of Engineers Enterprise Information System (CEEIS) network, which provides backbone communications and data services, information processing for corporate information systems, and, through a corporate enterprise information architecture, data and information at the desktop to Corps personnel and managers at all levels.

7.2 The U.S. Army Corps of Engineers Computer Network

CEEIS is composed of two Internet gateways, two information processing centers at Vicksburg, MS, and Portland, OR, and T-1 connections into the FTS2001 network with 45-Mbps connections at the processing centers. This network provides for the passing of data and message traffic between USACE sites in support of engineering, financial, e-mail, water control, and other USACE Business functions as well as providing connectivity to a high number of external customers and partners, both military and nonmilitary. These customers access USACE systems and data via Internet gateways at selected sites. CEEIS uses Cisco routers and Frame Relay to maximize the effective use of available bandwidth. CEEIS also provides connectivity to the DoD Secure Internet Protocol Router Network (SIPRNET) to support military missions and provide command and control capability for the Chief of Engineers. Riding the CEEIS network/processing center infrastructure in turn, and supporting the business processes that make up our Civil Works, Military Programs, and Emergency Operations mission areas, is the Corps logical information architecture including all mission-essential AIS.

7.2.1 Information Assurance Team

The Information Assurance (IA) team is responsible for implementing procedural and materiel protective measures, developing plans and policies, and validating requirements to protect the Corps communications, computers and data. It performs the following:

- Is the focal point for the Corps IA Program.
- Establishes Corps IA policy.
- Supports the development of an infrastructure that integrates the network management capabilities.
- Administers the IA management plan in support of the Corps' Technical Architecture and the Corps' Information Systems Security Resource Program.

- Supports Corps funding efforts to implement IA.

7.2.2 Information Infrastructure Protection Plan

The Information Infrastructure Protection Plan of the Directorate of Corporate Information is a set of ongoing activities focused on enabling and sustaining the Information Infrastructure Protection Program over the long run. These ongoing sustainment activities focus on technological awareness/capability enhancement, developing and protecting the workforce, and developing and/or implementing policies and procedures to accomplish the first two.

Under Department of Army Regulation AR 25-2, Information Assurance, which may be accessed through the Policy and Guidance Web page of the Defense Information Systems Agency, <http://iase.disa.mil/policy.html>, paragraph 2-7:

2-7. Commanders of MACOMs; Chief, Army Reserve (CAR); Chief, National Guard Bureau (NGB); program executive officers (PEOs); direct reporting program managers; NETCOM RCIOs; direct reporting units (DRUs); Installation Management Agency (IMA); and the Administrative Assistant to the Secretary of the Army

Commanders of MACOMs; Chief, Army Reserve; Chief, National Guard Bureau; Program Executive Officers; direct reporting program managers (PMs not under the PEO structure); NETCOM RCIOs; direct reporting units; Installation Management Agency; and the Administrative Assistant to the Secretary of the Army (acting as the senior official for all HQDA administrative and management services), in addition to the responsibilities defined in paragraph 2-2 [of this regulation], will —

- a. Develop and implement an IA program with the hardware, software, tools, personnel, and infrastructure necessary to fill the IA positions and execute the duties and responsibilities outlined in this regulation.
- b. Oversee the maintenance, documentation, and updating of the certification and accreditation (C&A) requirements required for the operation of all ISs as directed in this regulation.
- c. Implement and manage IT system configurations, including performing IAVM processes as directed by this regulation.
- d. Appoint IA and other personnel (for example, alternates) to perform the duties in chapter 3 of this regulation and provide IAPM POC information to the NETCOM RCIO, supporting Regional Computer Emergency Response Teams (RCERTs)/Theater Network Operations and Security Centers (TNOSCs), and the Army Computer Emergency Response Team (ACERT). MACOM IAPMs will report to the RCIO of the region in which the headquarters is physically located.
- e. Appoint or approve DAAs as required.
- f. Establish an oversight mechanism to validate the consistent implementation of IA security policy across their areas of responsibility.

- g.* Oversee annual security education, training, and awareness programs to all users that address, at a minimum, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.
- h.* Oversee the implementation of IA capabilities.
- i.* Incorporate IA and security as an element of the system life-cycle process.
- j.* Develop and implement an AUP for all users for privately owned equipment (for example, cell phones, personal digital assistants (PDAs), wireless devices) and ISs prohibited during training exercises, deployments, and tactical operations. Incorporate, as a minimum, the prohibition of utilizing such devices or the limitations of acceptable use, as well as the threat of operational exposure represented by these devices in garrison, pre-deployment staging, tactical, and operational areas.
- k.* Develop procedures for immediate notification and recall of IA personnel as assigned.
- l.* Report security violations and incidents to the servicing RCERT in accordance with Section VIII , Incident and Intrusion Reporting.
- m.* Adhere to and implement the procedures of the networkiness certification process.
- n.* Program, execute, and report management decision packages (MDEPs) MS4X and MX5T resource requirements

Within USACE, the Chief of Engineers, as Major Command (MACOM) Commander, has delegated program management responsibilities for enterprise IA to the CIO, who heads the Directorate of Information Management (DIM), within the HQUSACE. Within the DIM, IA responsibilities, including the position of Information Assurance Program Manager (IAPM), are resident with the Information Assurance Division (CECI-A), which was instituted as a separate divisional element in 2002, subsequent to the 2001 Financial Information System Controls Audit Manual (FISCAM) audit. The Division mission is to "provide planning and management of the USACE Information Assurance (IA) Program to ensure the confidentiality, integrity, and availability of information processed by the USACE information-based systems." This includes providing a measure of confidence that the security features, practices, procedures, and architecture of an information system accurately implements and enforces security policies.

The post-9/11 USACE, like other Federal agencies, finds itself coping with a world greatly changed. Where previously the Command was concerned primarily with denial of service or fiscal/property impacts, today we must contend with threats of physical harm to American citizens caused by cyber intrusion directed against USACE operational assets. The change is neither trivial nor simple to implement. USACE is closely watching the Department of the Army's evolution of DA PAM 25-IA, Information Management Information Assurance Implementation Guide (DRAFT). It is clear that

USACE will have to issue similar implementation guidance via an Engineer Regulation (ER).

7.2.3 Technology Security

USACE missions are continually evolving, as is the technology available to support them. The introduction of new technologies or the implementation of existing technologies in new ways to support existing missions may result in the recognition or emergence of new threats to the operating environment. Among recent technological evolutions offering security risks or potential security enhancements are:

- “Wireless” technologies
- Portable Electronic Devices (PEDs)
- Software auditing tools

Various wireless technologies offer tempting capabilities to the managerial problem solver while posing considerable risks to the enterprise. Wireless technologies are generally based on some variation of the IEEE 802.11 standard, which lacks secure cryptographic capability. While extremely flexible in their general mobility and utility, personal electronic devices such as Personal Digital Assistants (PDA’s) lack any meaningful secure capability, and can, if improperly implemented, offer a window of vulnerability into the enterprise.

Software auditing tools offer the enterprise the opportunity to test rapidly for multiple vulnerabilities in a thorough and cost-effective manner. Tools such as **Internet Scanner** and SafeSuite **Database Scanner** by Internet Security Systems, which have recently been ordered, will significantly improve the enterprise’s ability to ascertain its security vulnerability status by performing automated probes of communication services and devices, operating systems, and applications including database systems implementations in support of corporate AIS.

7.2.4 People Security

People are the heart of any of any security program – they are the greatest enabler and the greatest vulnerability. In accordance with AR 25-2, *Information Assurance*, security awareness begins when the employee is brought onboard. The Security Monitor for the Division briefs new employees, and anyone new to the DoD and/or the Department of the Army is acquainted with AR 25-2, which is the generally governing regulation.

After the initial personnel level, the security hierarchy within the enterprise follows the structures laid out in AR 25-2. At the fundamental level is the Systems Administrator (SA) – responsible for the security of a single AIS, in all its self-determined aspects. At the next level up is the Information Assurance Security Officer (IASO); the IASO is typically responsible for security at the workgroup or local area network (LAN) level. Above the IASO is the Information Assurance Manager (IAM), who is responsible for security at the Division or District level. At the head of the security “pyramid” is the IAPM, who is responsible for the security of the enterprise.

Security awareness must encompass not only vulnerabilities of/to computer systems, but also vulnerabilities of the individual for the enterprise involving various types of “social engineering” hacker exploits. Yearly Subversion and Espionage Directed Against the Army (SAEDA) briefings assist in maintaining awareness of these types of vulnerabilities and preventing corporate compromise. While most social engineering penetration efforts are not directly destructive, they can create hidden vulnerabilities, which can be difficult and costly to rectify. All personnel also receive Yearly Information Security briefings to keep them current with emergent and emerging information security threats.

7.2.5 Information Assurance Procedures

Security procedures in USACE are directed under a number of Army Regulations and DoD Directives and Instructions, including:

- AR 25-2 Information Assurance
- AR 380-53 Information Systems Security Monitoring
- AR 380-67 Personnel Security Program
- AR 530-01 Operations Security
- AR 25-1 Army Information Management, and
- DoD Directive 8000.1 Defense Information Management Program

The Information Assurance Division (CECI-A) has summarized much of this directive information in operational form and placed it on the corporate intranet, available Corps-wide at <https://corpsinfo.usace.army.mil/ci/ia>.



Information Assurance Division

The Information Assurance Intranet

US Army Corps of Engineers
Corporate Information

Sitemap
Security Organizations
Contacts - What to do and Who to Contact
SIPR Net
Organization
Publications

[IA Home](#) | [DITSCAP](#) | [IAVA](#) | [PKI-CAC](#) | [SecuringYour System](#) | [Training](#)

The IA Team is responsible for implementing procedural and materiel protective measures, developing plans and policies, and validating requirements to protect the Corps communications, computers and data.

- Focal point for the Corps IA Program.
- Establish Corps IA policy.
- Support the development of an infrastructure that integrates the network management capabilities.
- IA management plan in support of the Corps' Technical Architecture and the Corps' Information Systems Security Resource Program.
- Support Corps funding efforts to implement IA via the ISSR program (MS4X and MX5T).

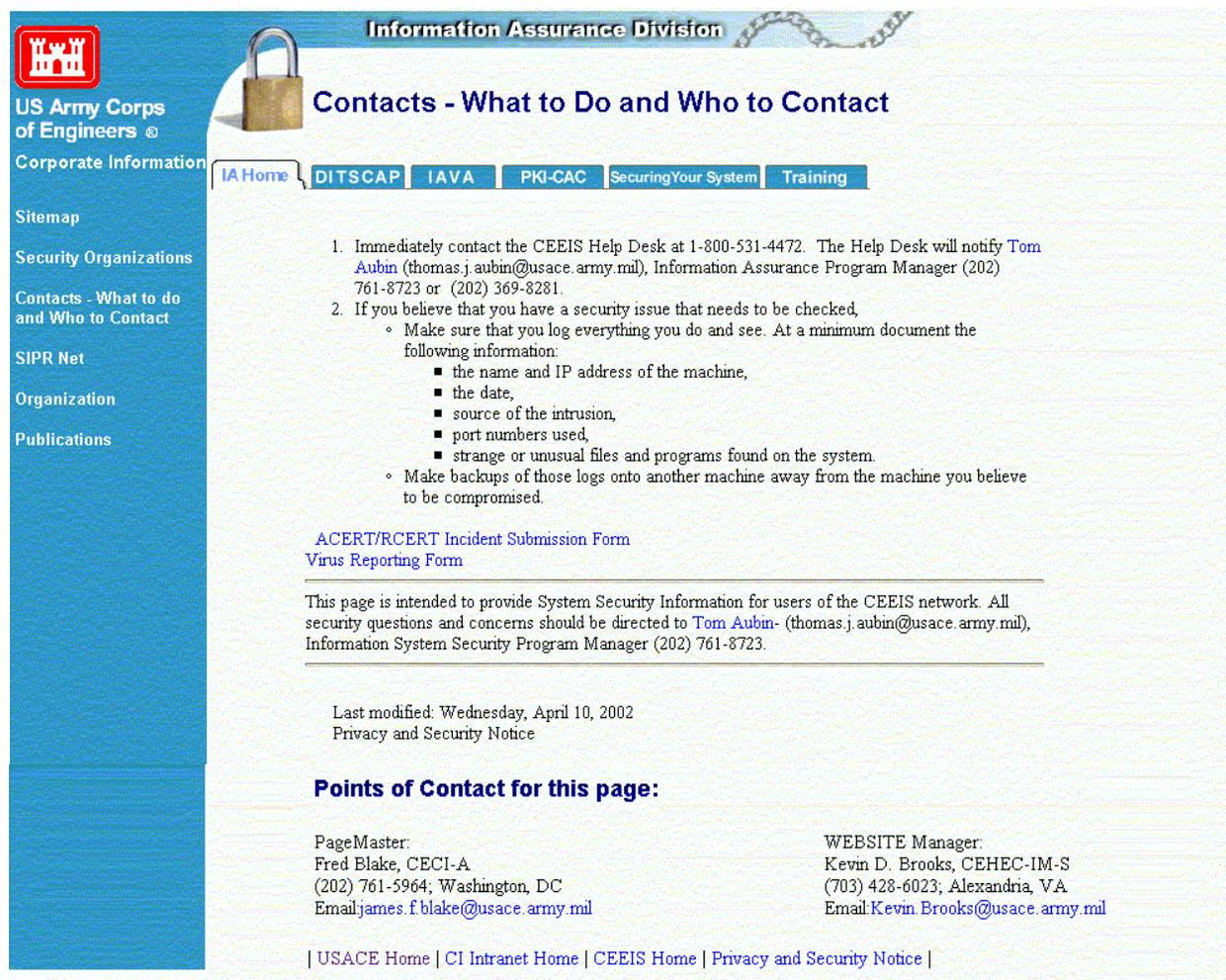
**If you need technical assistance, call the CEEIS Help Desk
1-800-531-4472**

This site is intended to provide information for users for Information Assurance. Questions and comments should be directed to [Tom Aubin](mailto:thomas.j.aubin@usace.army.mil) - (thomas.j.aubin@usace.army.mil, CECI-A-IAPM@usace.army.mil), Information Assurance Program Manager (202) 761-8723.

Privacy and Security Notice

Points of Contact for this page:

From the front page one can quickly go to information on any critical security function, such as incident reporting:



Information Assurance Division

US Army Corps of Engineers

Contacts - What to Do and Who to Contact

IA Home | DITSCAP | IAVA | PKI-CAC | SecuringYour System | Training

1. Immediately contact the CEEIS Help Desk at 1-800-531-4472. The Help Desk will notify [Tom Aubin](#) (thomas.j.aubin@usace.army.mil), Information Assurance Program Manager (202) 761-8723 or (202) 369-8281.
2. If you believe that you have a security issue that needs to be checked,
 - Make sure that you log everything you do and see. At a minimum document the following information:
 - the name and IP address of the machine,
 - the date,
 - source of the intrusion,
 - port numbers used,
 - strange or unusual files and programs found on the system.
 - Make backups of those logs onto another machine away from the machine you believe to be compromised.

[ACERT/RCERT Incident Submission Form](#)
[Virus Reporting Form](#)

This page is intended to provide System Security Information for users of the CEEIS network. All security questions and concerns should be directed to [Tom Aubin](#) - (thomas.j.aubin@usace.army.mil), Information System Security Program Manager (202) 761-8723.

Last modified: Wednesday, April 10, 2002
Privacy and Security Notice

Points of Contact for this page:

<p>PageMaster: Fred Blake, CECEI-A (202) 761-5964; Washington, DC Email: james.f.blake@usace.army.mil</p>	<p>WEBSITE Manager: Kevin D. Brooks, CEHEC-IM-S (703) 428-6023; Alexandria, VA Email: Kevin.Brooks@usace.army.mil</p>
---	--

| [USACE Home](#) | [CI Intranet Home](#) | [CEEIS Home](#) | [Privacy and Security Notice](#) |

The ultimate security and survival guarantor is a robust Continuity of Operations (COOP) plan as required by AR 25-2. Each of USACE CEEIS processing centers acts as a COOP site for the other.

7.2.6 Physical Information Infrastructure

USACE uses a “defense in depth” (Figure 7.2) strategy for its information infrastructure, beginning with firewalls at every network entrance point.

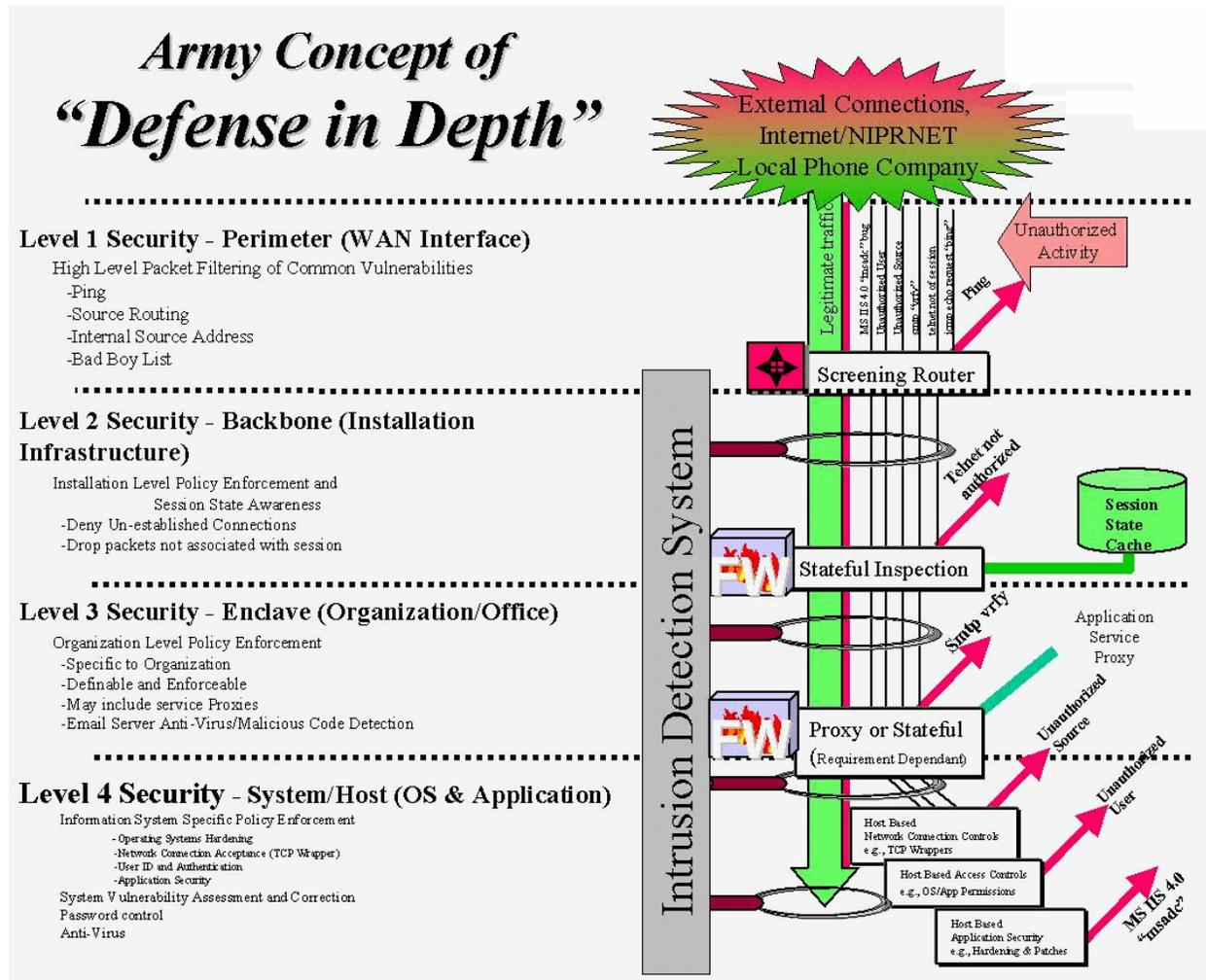


Figure 7.2. Defense in depth concept

Information/data traffic entering USACE first encounters an Army-supplied router (ASR) (Figure 7.3), and then a **Real Secure** intrusion detection system (IDS) managed by the Army’s Technical Network Operating Security Center (TNOSC) at Fort Huachuca. Subsequently the traffic encounters a USACE-operated gateway firewall. USACE uses **Nokia Checkpoint** firewalls supplied by NAI Corporation, and approved by the Department of the Army (DA). The Network Operations Center (NOSC) in Portland, OR, and Vicksburg, MS, centrally manages USACE firewalls. The two sites provide continuous operational support (24/7/365). The CEEIS NOSC is responsible for keeping the firewalls under constant observation and updating the “rules base” by which each firewall filters incoming traffic, based on Security Advisories from the Army Computer Emergency Response Team (ACERT).

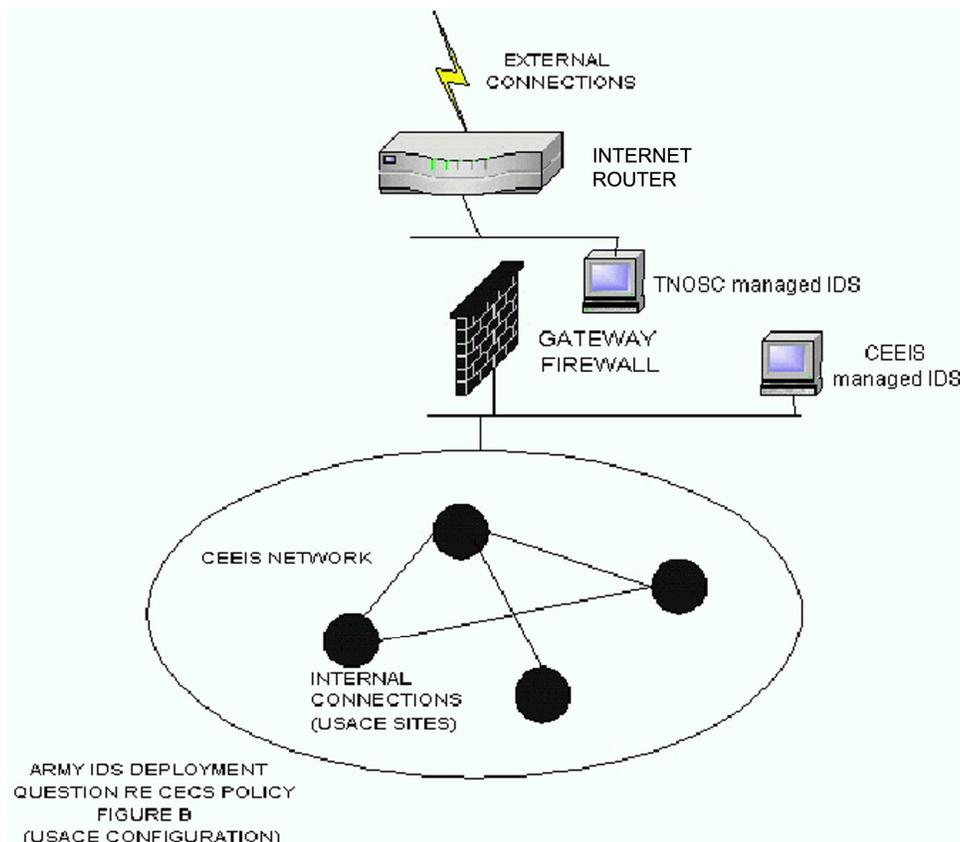


Figure 7.3. USACE IDS

After passing the gateway firewall, traffic encounters an additional CEEIS-managed **Real Secure** IDS. Incoming e-mail is initially filtered for hostile traffic at the mail servers in Portland and Vicksburg using **Antigen** anti-virus/anti-spam software; it is further filtered at the servers in the Field Operating Activities (FOA) using **Norton** anti-virus, and finally filtered at the desktop by either the **McAfee** or **Norton** anti-virus, which are also provided to those who access the system remotely. Remote system access, in accordance with DA policy, is permitted only to modem pools employing the remote authentication dial-in user system (RADIUS) standard. Security at the desktop is further enhanced by the use of password-protected screen saver “timeouts.”

Operationally, the applications, network and the enterprise components to the FOA level, have been, or are being, subject to ongoing security accreditation and review under the Defense Information Technology Security Certification and Accreditation Process (DITSCAP). DITSCAP is an intensive standardized four-phase security certification process consisting of Definition, Verification, Validation, and Post Accreditation phases. The DITSCAP process provides vulnerability assessments for the system or subsystem under review, as well as detailed procedural documentation for determining, securing, and maintaining the security of a given program, FOA, or AIS. Security of the network is critical, because information that travels the network, including

Water Control data, inland waterways traffic usage data, and emergency operations support (ENGLink) data, is not only mission critical but also life critical.

In addition to responding to Information Assurance Vulnerability Alerts (IAVAs) as required by the DoD and the Department of the Army, USACE regularly performs internal assessment testing to identify vulnerabilities. Assessment testing involves not only penetration testing for known vulnerabilities in network control systems and processing center operating systems, but also “war dialing” to identify violations of general security access and control policy via unauthorized modems.

Ideally, all USACE servers and sites would be scanned for vulnerabilities every 6 months and the results reported to the IAPM and the CIO. Current manpower restrictions inhibit this, but the acquisition of the **INTERNET SCANNER** software, currently underway, should significantly improve USACE capabilities in this regard. Although we currently capture assessment results in a database, there is, at present, no feedback capability from the assessment subject, nor any automated upward reporting capability; this was proposed as an automation initiative for 2003.

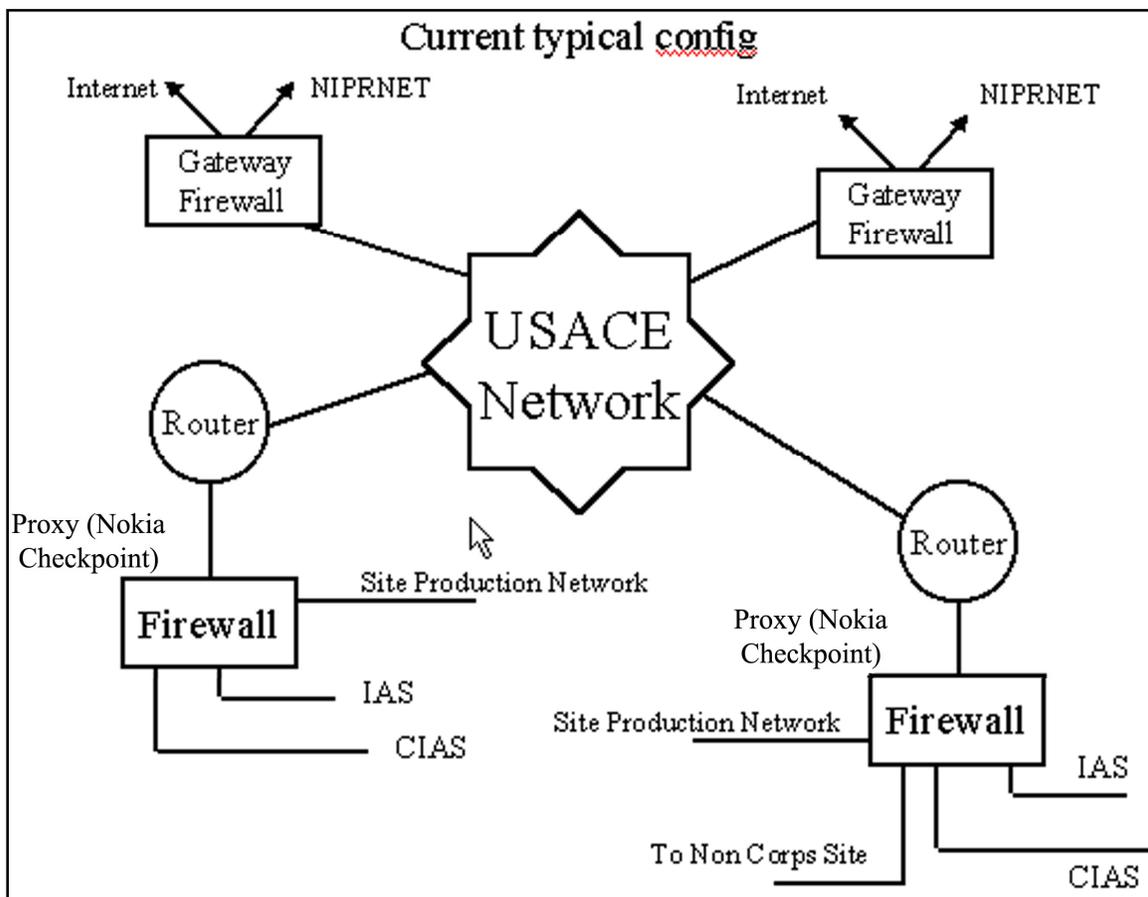


Figure 7.4. Current typical configuration of USACE network

Incident response procedures follow the Computer Emergency Response Team (CERT) guidelines for detection checklists and report formats, and flow through the chain of command in parallel, to the Information Assurance Manager/Officer (IAM/IAO), the IAPM and the CEEIS Security Operations Center (SOC). Incidents are promptly reported and worked with the appropriate levels within Army (ACERT/CID) and other agencies (FBI/CID).

To further enhance USACE security posture, enterprise data has been partitioned into “publicly accessible” data sets, and private or enterprise data sets. “Publicly accessible” data sets comprise data generally available for the public good, such as the data on the availability of space in recreation areas; data available for public safety, such as water control data; and data available for public planning, such as data on the progress of the South Everglades Restoration Project. Publicly accessible data sets are “quarantined” away from “production” enterprise data sets supporting daily mission operations using “controlled Internet accessible segments (CIAS)” versus the Internet accessible segments allowed internal enterprise users.

- a. Future enhancements to USACE information security posture, either underway or in planning, include: adoption of the DoD Common Access Card (CAC) as the single network access token, with eventual migration to its use as the single point of entry, for both physical network access and logical data access, which in turn involves Public Key Enabling of the network and selected information systems resident thereon.

7.2.7 Logical Information Infrastructure

The USACE logical information infrastructure consists of multiple information systems that support major Corps mission areas, or business processes, which in turn support those business areas. These AIS either have been, or are in the process of being, accredited with a DITSCAP review. In 2001, USACE invested \$1.6M in 100 copies of the XACTA tool by TELOS Corp, which automates and simplifies the DITSCAP process. Additionally, training and support for 3 years was also acquired under the same acquisition. All AIS on the CEEIS network are password access controlled, both at the network access and again at the information system access level. The corporate information systems database management system standard is ORACLE, which has a robust security architecture. USACE AIS are implemented in ORACLE and take advantage of these security features, including the use of:

- **UserID's/Passwords** – independent passwords are issued for ORACLE access to selected databases
- **Product_user_profile table** – users are restricted to the specific tools within the ORACLE tool suite necessary to accomplish their specific tasks within the AIS framework
- **Roles** – roles are predefined object and system privileges which grant different classes of users the necessary capabilities to accomplish their tasks within the AIS framework

- **Views** - views are used to segregate data access, permitting users to access only the data necessary to accomplish their tasks
- **Auditing** – some applications make extensive use of how and when given SQL capabilities are executed, as well as how data definitions and data manipulation are executed

USACE was a pioneer within DoD in reducing paperwork and adopting electronic signatures (e-sigs). The Corps of Engineers Financial Management System (CEFMS) has incorporated e-sigs as a keystone of secure financial operations since 1994. USACE is presently migrating this current secure e-sig standard from the FIPS 140-1 to a more robust PKI enabled FIPS 140-2 e-sig, in a cooperative effort between USACE, the National Institute of Standards and Technology (NIST), and the Government Accountability Office (GAO) who pioneered this process with us. At the same time, we will be cooperatively defining the requirements for a “secure Web enabled” application. This effort is being funded using Department of the Army RDT&E monies made available for this purpose as a result of CEFMS being a “legacy” electronic signatures (e-sig) system.

USACE AIS are managed under an ongoing LCMIS process, with security reviews included as a normal part of the systems architecture, design, and acceptance process. Under Army guidance, additional AIS will be considered for migration to PKI enablement.

7.2.8 Ongoing Internal and External Reviews and Related Reports

7.2.9 Health of the Network Study:

As part of our efforts to maintain efficiency and enhance security, the Directorate of Information Management commissioned a DA, to test these products’ ability to enhance management’s “span of control,” improve scarce personnel utilization, and offer improved security opportunities.

7.3 Financial Information System Controls Audit Manual (FISCAM)

In the past 2 years the GAO in combination with USACE Inspector General (IG) and the Army Audit Agency (AAA) have participated in extensive Financial Management (FISCAM) reviews. Through the use of a private contractor (Price-Waterhouse Coopers) these audits have identified weaknesses in the areas of:

- Access controls
- Software
- Segregation of duties

In response to this, access controls in the form of firewalls and intrusion detection systems are now monitored 24/7/365. New and stricter authentication procedures have been established at the INTERNET gateways and at each individual server. We have also implemented both random and “by request” inspection procedures to look for

system vulnerabilities, and unauthorized access through modem dial-up (using war-dialing techniques, as referenced previously). We continue to limit physical access to devices or computer rooms via keypad access control locks, and we limit the number of persons having access as much as possible. In areas where changes were not technically or fiscally possible, we have put in place other procedures to mitigate the security risks. As a result, while the GAO report for the fiscal year 2000 has not yet been finalized, we are confident the report will document significant improvement in our security posture. Communications Architecture Assessment, which was completed in October of 2000, addressed network performance, documented our bandwidth deficiencies and some of the causes thereof, and projected the expected trends that we would have to deal with in the coming years. As a result of this study, the Corps acquired and installed **Sitara** network traffic prioritizers, and installed caching servers at selected sites to improve throughput. In addition, the Corps initiated an Enterprise Management Systems (EMS) Pilot in partnership with our South Atlantic Division, deploying the **CA Unicenter** EMS products recommended by



Chapter 8 – CeA Management and Maintenance



The architectural methodology chosen for the **CeA** is based on a set of prescribed reference models (sometimes referred to as views) that allow detailed analysis to be performed on the complex relationships between business performance and IT support requirements. The **CeA** PDT developed a skeletal framework to help categorize complex components. See Appendix S for Federal Government Model used as a guide. The five **CeA** reference models that serve as vantage points to conduct this relational analysis are:

- The **Performance Reference Model (PRM)**: Identifies a common set of general performance outcomes and metrics used to achieve program goals and objectives. Think of this as a view of USACE **Business and IT Performance – Knowing the value of IT.**
- The **Business Reference Model (BRM)**: Describes USACE business functions and subfunctions. Think of this as a view of USACE **Business – Who we are and what we do.**
- The **Data and Information Reference Model (DRM)**: Describes the data and information that support program, support and internal lines operations. Think of this as a view of USACE **Information – The Information we share.**
- The **Service Component Reference Model (SRM)**: Identifies and classifies horizontal and vertical IT capabilities that support business functions and subfunctions. Think of this as a view of USACE **Applications – How we get work done.**
- The **Technical Reference Model (TRM)**: Provides a hierarchical foundation to describe how technology is supporting the delivery of the application capability. Think of this as a view of USACE **Information Technology – Our business utilities and infrastructure.**

Two additional management constructs are prescribed to ensure safeguard of people/information and effective management of **CeA** resources:

- **Information Assurance**: Ensures special emphasis on safeguarding people and information in all aspects of the **CeA**. Think of this as a view of USACE **Security – keeping people and work safe.**
- **Management and Maintenance**: Provides guidance and tools provided to assist users in locating and analyzing information and technical specifications. Think of this as a view of USACE **CeA Management – Our focus and style.**

8.1 CeA Policy

CeA policy establishes rules and guidelines for applying the information contained in the reference models for making informed management decisions and solving technical problems. Mandatory requirements are incorporated in the USACE IT CPIC Regulation No. 25-1-106, released in 2003, as a critical element in method for *selecting, controlling, and evaluating* IT investments.

CeA policy as presented in the CPIC policy states IT investments and the IT investment decisions will be:

- Tied to strategic goals and missions/programs/projects.
- Tied to the business process(es) they enable.
- Linked to strategies that foster and enable e-government for the effective and efficient delivery of products and services to citizens, partners, stakeholders and customers.
- Acquired or developed in accordance with prescribed technical standards.
- Acquired or developed to share data/information and create opportunities to unify and/or simplify systems and processes across the enterprise.
- Acquired, developed, operated and maintained using cost, schedule, and other performance measurements that are monitored and reported to the IT investment sponsor and IT investment decision authority to assure systems are working together synergistically and are meeting performance goals.
- Aligned with the Corps Enterprise Architecture (**CeA**).

The USACE CIO serves as the Commanding General's principal agent to facilitate the CPIC business process, and is responsible for establishing and maintaining **CeA** guidelines and configuration management practices.

CeA Policy requires USACE Staff Principals and USACE Commanders/Directors to:

- Streamline and reengineer business processes before making IT investments or modernization decisions to support the business processes.
- Ensure that performance measurements are in place to assess the effectiveness and efficiency of their IT investments.
- Conduct annual **CeA** Alignment and Assessment of each IT investment.

As stated in the CPIC policy, the following example tasks will be required to achieve benefits:

- Enhance communication among and between LOBs and program areas across the enterprise.

- Identify opportunities to unify and/or simplify processes and information systems across the enterprise and the Federal Government.
- Promote alignment, integration, change, time-to-delivery, and convergence opportunities to improve mission, program, and project performance.
- Identify redundant, obsolete, or duplicative systems or processes and consolidate or eliminate where appropriate.
- Achieve economies of scale by optimizing the sharing of IT assets, information systems, and services on a regional and enterprise basis.
- Expedite the integration of legacy, migration, and new information systems.
- Implement and provide leadership for the **CeA**.

CeA Policy References

The following references contain policy and guidance directly related to the functions, roles, and responsibilities inherent with the IT CPIC business process:

- National Defense Authorization Act for FY2001, Title X, Subtitle G, 44 U.S.C. 3531
- Clinger-Cohen Act, Division D, 40 U.S.C. 251
- Clinger-Cohen Act, Division E, 40 U.S.C. 1401
- E-Government Act, 2002 PL 107-347
- National Information Infrastructure Protection Act, 18 U.S.C. 1030
- Paperwork Reduction Act, 44 U.S.C. 101
- Government Performance and Results Act, U.S.C. 1101
- Government Paperwork Elimination Act, 44 U.S.C. 3504
- Privacy Act, 5 U.S.C. 552a, as amended
- Freedom of Information Act, 5 U.S.C. 552, as amended
- Executive Order 13011, 16 Jul 96, "Federal Information Technology"
- OMB Circular A-11, Preparation and Submission of Budget Estimates
- OMB Circular A-123, Management Accountability and Control
- OMB Circular A-127, Financial Management Systems
- OMB Circular A-130, Management of Federal Information Resources
- OMB memorandum M-97-02, Funding Information Systems Investments
- OMB memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments

- DoD Instruction 5000.2, Operation of the Defense Acquisition System, April 5, 2003
- DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP)
- DoD Directive 5400.11, DoD Privacy Program
- DoD C4ISR Architecture Framework, Version 2.0
- AR 11-18, Cost and Economic Analysis Program
- AR 25-1, Army Information Management
- AR 70-1, Army Acquisition Policy
- AR 71-9, Materiel Requirements
- AR 340-21, The Army Privacy Program
- AR 25-2, Information Assurance
- Joint Technical Architecture – Army (JTA-A), V6.5
- Department of the Army, Economic Analysis Manual, U.S. Army Cost and Economic Analysis Center
- Department of the Army, Cost Analysis Manual
- ER 5-1-11, USACE Business Process
- ER 25-1-2, Life Cycle Management of Information Systems (LCMIS)
- Federal CIO Council, Architecture Alignment & Assessment Guide
- Federal CIO Council, Federal Enterprise Architecture Framework (FEAF), Version 1.1
- Federal CIO Council, A Practical Guide to Federal Enterprise Architecture

8.2 CeA Work Products

Each **CeA** work product provides a starting point for probing specific areas in greater detail where more interrelationships will be seen. The type of interested reader or researcher will likely shift more to system builders from the business owner level. Please note that the **CeA** is in the development stage and it will take time to create additional work products that are missing at this time. The following brief descriptions offer explanations for the use and value of the various, known work products used in the **CeA** (as of May 2005).

8.2.1 Business Reference Model Work Products

Value Chain - Provides an overview of the missions and services the Corps provides. Serves to define the scope of the enterprise covered by the architecture. Used by all team members and for external communication.

Graphic and Narrative for the Baseline and Target Work Environments - Provides a quick look at the current stovepiped nature of the Corps. Shows that the future will not be constrained by organization or by location. Used by all team members and for external communication.

Business Functions and Subfunctions - Provides details on what the Corps does. Used by each of the teams for mapping between views. Also used for external communication. It helps everyone in the Corps understand how they fit into the enterprise. Used by the IT Capital Planning Process to show the relationship of investments to the business.

Subfunction Mapped to Federal Business Reference Model - Used by OMB to see across the whole Federal Government. Used to demonstrate the complexity of the Corps.

Business ICOM Diagrams - Provide a basis for understanding relationships among processes, and provide a structure to be decomposed into more detailed diagrams. Used by business owners to confirm their accuracy, and by system designers to understand what needs to be in a system.

Calendars of CeA Related Events - Used by the **CeA** team to understand business events that **CeA** products will be used to support.

8.2.2 Data and Information Reference Model Work Products

Baseline Data Classes and Definitions - Used by all users of data to ensure consistency.

Baseline Data Objects - Used by database designers to allow reuse.

Baseline Entity Relationship Diagram - Used by database designers to understand what types of things are represented by the data, and by business owners to validate any missing items.

Baseline Create Reference Update Delete (CRUD) Matrix - Used by application designers to understand system constraints. Also used to show possible problems if more than one process has the ability to delete data.

8.2.3 Information Assurance Work Products

Products make up a description of the environment. Used in concert with the business owners to understand what information needs to be protected.

8.2.4 Management and Maintenance Work Products

Principles - Used to ground the work. Helps decision makers make choices between alternatives based on the priorities expressed by the principles. Used by all team members and for external communication.

Relationship Diagram - Provides an overview of the views of the architecture and their relationship to one another and to other external processes. Used by all team members and for external communication.

Web Site - The **CeA** Web site is the **CeA**. This Web site is to provide an information exchange between business owners and IT professionals. Used by all team members and for external communication.

Glossary - Tells what the terms and acronyms used by the products mean. Ensures consistency within and between the products. Used by all team members and for external communication.

8.3 CeA Architectural Alignment and Assessment

The management objective of the architectural alignment and assessment process is to establish a line of sight between business needs and IT performance that identify opportunities for adjustments. Figure 8.1 illustrates how proper alignment of IT initiatives to business subfunction requirements can enhance mission performance.

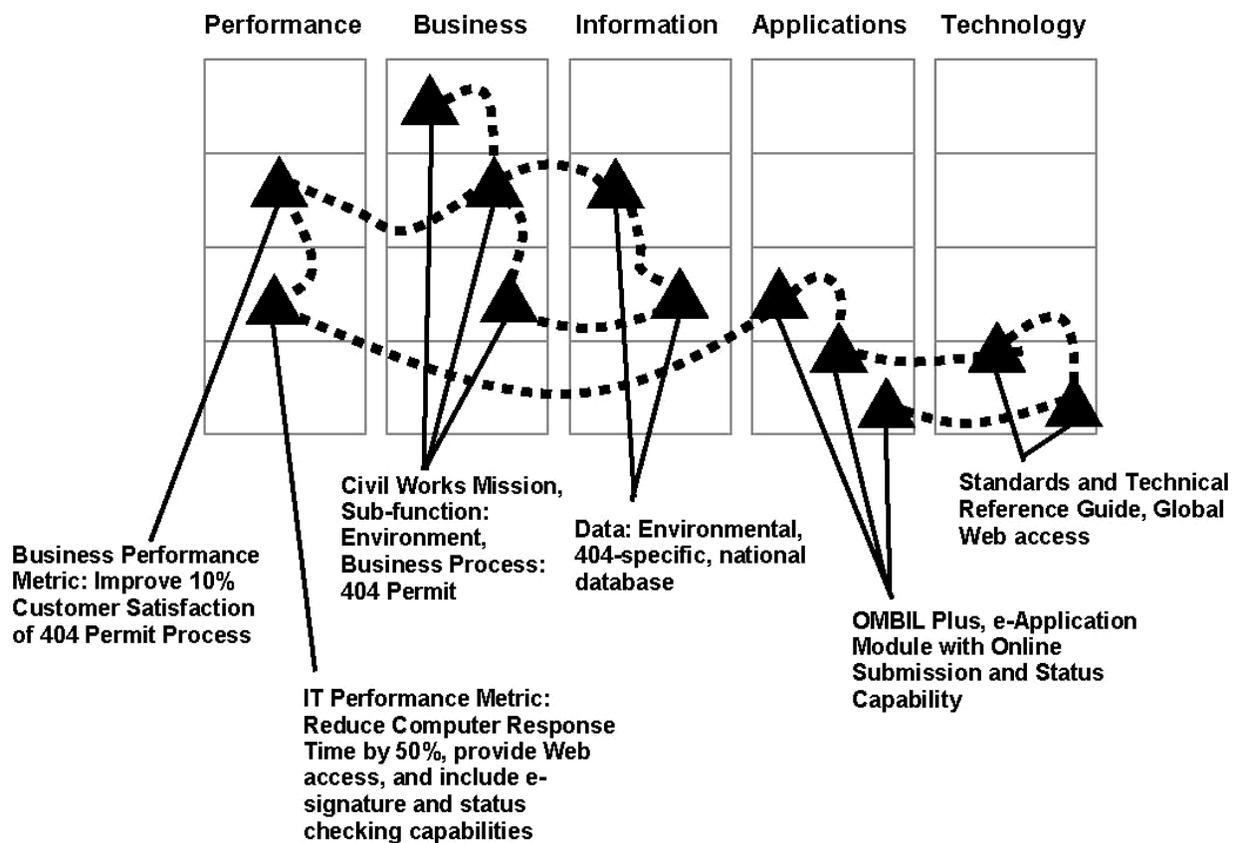


Figure 8.1. Architectural alignment and assessment process

It should be noted that the **CeA** is a multifaceted program that will evolve over several years (Figure 8.2). Detailed, *Component* level exchanges of information can be achieved only after a solid foundation and an architectural framework are established.

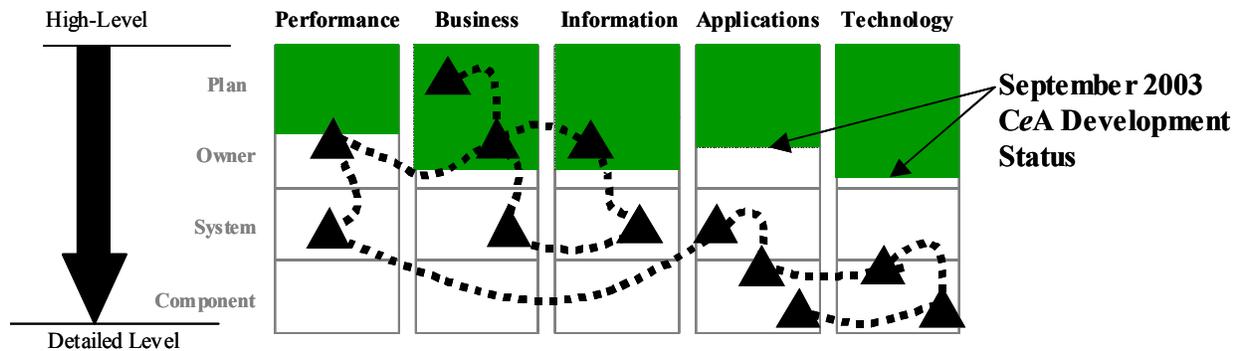


Figure 8.2. **CeA** development status (September 2003)

CPIC and **CeA** policy requires business owners, as proponents of IT investments, to conduct an annual **CeA** Alignment and Assessment. In the first year or so of **CeA** development, however, there will simply not be enough data and information to conduct a thorough alignment and assessment. The interim decision matrix in Table 8.1 is recommended, therefore, to help business owners determine how well IT initiatives are supporting business needs.

Table 8.1. IT Investment Decision Matrix

IT Investment:			
Analysis	Performance Criteria	Assessment Rating (Red, Amber or Green)	Notes
1. Explain how the IT investment supports USACE missions and functions.	Red = IT investment does not support mission and functions Amber = Somewhat supports mission and functions Green = Directly contributes to mission and function performance		
2. Explain how IT will improve the business process.	Red = Cannot articulate how the IT investment improves process Amber = IT investment contributes to process Green = IT investment clearly contributes to performance		

IT Investment:			
Analysis	Performance Criteria	Assessment Rating (Red, Amber or Green)	Notes
3. Identify data elements used to support this requirement and if data is shared with other USACE systems.	Red = Cannot articulate list of data elements and data sharing aspects of data generated Amber = List of data elements available but data is not shared Green = Enterprise data standards are used and data is shared extensively.		
4. Explain standard and unique system requirements.	Red = Cannot articulate whether the IT investment is a justifiably unique solution or part of an enterprisewide solution Amber = Some analysis has been done to consider relation of system components to similar technical solutions. Green = Can articulate why system is unique or part of a standard solution		
5. Explain the project management approach and list major milestones.	Red = No Project Management Plan (PMP), no Project Manager (PM) credentials, no PDT, etc. Amber = Can articulate milestone and progress toward goals Green = Highly capable PM assigned to lead a multi-functional PDT, project on target and within PM limitations.		
6. Explain progress made toward capability to conduct future (objective) more complete CeA Alignment and Assessment.	Red = Cannot articulate progress Amber = Some progress made Green = Good to significant progress made toward ability to conduct more detailed alignment and assessment		
Overall Assessment Rating (Red, Amber or Green):			

As the **CeA** matures, business owners will be able to conduct a more thorough architectural alignment and assessment. This will be a six-step process that walks the business owner through 15 important architectural questions as shown in the illustration (with today's business/IT examples) in Table 8.2.

Table 8.2. Sample Architectural Alignment and Assessment

Step 1	Step 2
<p>Identify Primary Business Function, Subfunction and Sub-subfunctions. Example: Civil Works Primary Business Function, Environment Subfunction, and 404 Permit as the Sub-subfunction.</p>	<p>Identify Business Performance Metrics. Example: Improve 10% Customer Satisfaction of 404 Permit Process.</p>
<p>The following question must be answered: 1. Which Primary Function Area and Subfunctions (and references) are being supported by this IT investment? Example: The two Enterprise-wide emphasis statements below depict the importance of seeking improvements to the 404 Permit process associated with providing direct service for citizens: "...applicants for wetland development permits - are also counted as customers."* "Regulatory Issues. Attendees called for streamlining the regulatory process by: shortening the permitting time (especially for Clean Water Act, Section 404 permits), simplifying the process, providing easy tracking of permits after they have been submitted, obtaining more consistency along with the ability to particularize regulations to meet regional challenges, closing loopholes, and achieving better balance between commercial/industrial beneficiaries and community and environmental beneficiaries. People want to see Federal-state communication improve. Many called for better enforcement of regulations. Some highlighted staffing shortages as contributing to processing delays."* * Reference CW Program Strategic Plan (Draft) FY03-FY08</p>	<p>The following question must be answered: 2. What are the business performance metrics (and references) associated with this IT investment? Example: The two metrics below would be evaluated against a customer satisfaction survey to determine improvements: - Customer Satisfaction* - % All permits in 60 days (85%)* * Reference FY05 CW Performance Plan</p>

Step 3	Step 4
<p>Identify IT Performance Metrics. Example: Reduce Computer Response Time by 50%, provide Web access and e-signature capability.</p>	<p>Assess Data Requirements and Source. Example: Requirement to collect 404 Permit Transaction Data. Data Standard is <i>Environment</i>.</p>
<p>The following question must be answered: 3. What are the IT-specific performance metrics (and references) associated with supporting the business performance metrics identified earlier? Example: Performance metrics would be established to measure response time improvements per the IT objective below: “Objective 2.1. Implement Web-based technologies to enable flexible and timely information sharing and exchange in warfighting, mission critical and sustaining base processes and/or applications. Initiatives under this objective include identifying applications to Web-enable; acquiring, on an enterprise-wide basis, Web-based technologies; converting applications to be Web-based; building data marts and warehouses to leverage corporate information; using on-line analytical and graphical information tools to improve information collection and dissemination to a wide range of various information consumers; and creating an enterprise-wide horizontal and vertical framework (i.e., taxonomy) to build a shared, knowledge-rich environment that achieves information superiority and creates a learning organization.” * Reference IRM FY03-FY08 Strategic Plan (Draft)</p>	<p>The following questions must be answered: 4. Is the data needed to assess performance already being collected by USACE or another government agency? 5. Is data being collected or proposed to be collected using standard naming conventions and definitions within parameters set by USACE Enterprise Data Classes and USACE Standard Data Classes? 6. Has a data management plan been prepared to identify specific data requirements (accuracy, timeliness, etc.)? 7. Will data being generated be shared with other systems/agencies? Examples: Data being collected is not available in electronic form by any government agency. Data elements use USACE Data class naming conventions. A data management plan is used and updated XX/X/XXXX. Data generated will be shared with EPA, as well as State and local governments.</p>

Steps 3 and 4 focus on the integral contributions IT initiatives make to business objective and overall performance. It is not simply increasing computer speeds but adding value by reducing steps in the business process via automated mechanisms like the Web or workflow and authoring tools.

Step 5	Step 6
<p>Consider Availability of Alternative IT Solutions and Standards. Example: Use Technical Reference Model to Apply Standards and Technical Reference Guide Suggestions.</p>	<p>Demonstrate Good Project Management Practices. Example: Time, Cost, Scope, and Risk Management demonstrated. Existing resources and technology applies to IT technical solutions.</p>
<p>The following questions must be answered: 8. Is there a comparable technical solution available else where in government or private industry? 9. Are any modules being used as part of the technical solution duplicates or similar to modules in other USACE automated systems? 10. Is the IT technical solution proposed within the parameters set by government, private industry and the CeA Technical Reference Guide? Examples: Comparable IT technical solutions were considered in the original analysis of alternatives in XX/XX/XXXX. Two existing modules with the OMBIL-Plus application will be used to additionally support this data requirement. Technical solution proposed incorporates latest TRG e-signature standards and Web-enabling software recommendations.</p>	<p>The following questions must be answered: 11. Has the PMP been updated within the last 12 months to include time, costs, scope, and risks? 12. Has an analysis of alternatives been conducted within the past 36 months? 13. Are all Milestone Decision Authority documents complete and on file with the CIO Office? 14. Has the ITIPS Record been updated within the past 12 months? 15. Has an Architectural Alignment and Assessment been conducted within the past 24 months? Examples: PMP updated on XX/XX/XXXX. AA last conducted on XX/XX/XXXX. MDA approved for MS III, Deployment on XX/XX/XXXX. ITIPS last updated on XX/XX/XXXX. This investment was last reviewed by the EFAT in May 2003.</p>

Steps 5 and 6 force attention to situational awareness of other options that might be available to solve business and technical solutions, and good project management of IT resources.

8.4 CeA Management Team and Tools

Creating a **CeA** environment that encourages and nurtures meaningful exchange of information between business owners and IT professionals will require dedicated stewardship of the five reference model frameworks and constant reassessment of management tools and techniques. The **CeA** PDT must include multifunctional representation from the many business areas and from various tiers in the organization chain. Team membership will include representatives from business areas and stakeholders.

Project Delivery Team (PDT)

- Business Owners from Headquarters
- Stakeholders from Districts
- System Developers
- Strategic Planners

- Contract Consultants
- CeA Chief Architect and Operations Staff

PDT Administration

- The PDT will meet weekly for the first year and monthly after the first year.
- Management decisions will be made by reaching team consensus.
- Disputes will be resolved by majority vote if necessary.
- A **CeA** Glossary of Terms (Available in Appendix U) will be used to establish common understanding of technical terms.

Automated Architectural Tool

- The automated management tool chosen to support the **CeA** is the Metis® tool (reference: http://www.enterprise-architecture.info/Architecture_Tools.htm). Metis® does a particularly good job of capturing and linking information in multiple areas and illustrates effects of changes that may result from making informed business decisions. Architecture models will be built and shared via the Internet or intranet using the Metis® Model Browser.

8.5 Technical Reference Manual (TRM) Governance

The TAWG is responsible for the creation of the architecture and the set of architecture processes directed toward the management, assessment, and governance of the TRM. The TAWG works under the direction of the USACE AAA team and the USACE CIO.

The TAWG is the primary decision-making body for the introduction of new or revised standards into the TRM. Domain/Service Area owners and subject matter experts are assigned by the TAWG members to provide evaluations and technical expertise relating to their areas of competency. Details concerning the members of the TAWG and their processes are further discussed in the Technical Reference Guide (TRG).

8.6 CeA Components and Mapping to the Federal Enterprise Architecture

The relational diagram in Figure 8.3 provides a snapshot (September 2003) of **CeA** components with relation to themselves and where they provide input to the FEA. Enlarged graphics of each of the five reference models will be discussed on the next few pages. A more readable copy of the relational diagram is available in Appendix E.

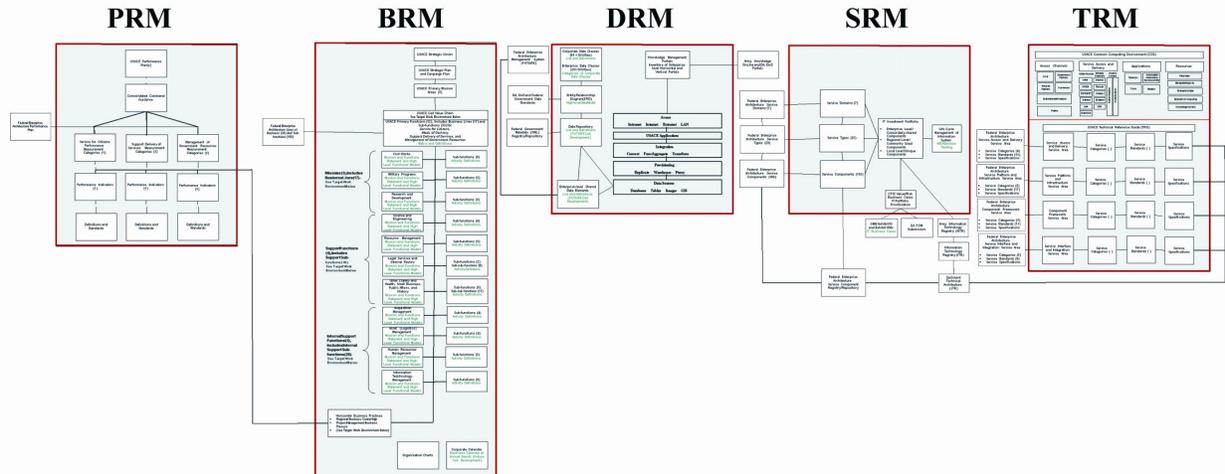


Figure 8.3. Relational diagram of **CeA** components (September 2003 snapshot)

The **CeA** BRM framework shown in Figure 8.4 (September 2003 snapshot) will identify USACE business functions and subfunctions across the enterprise. Although the terminology for categories of mission, function and lines of business are changing at this point in time, the relative hierarchy can be assumed to remain the same. The BRM relationship to the PRM is one where the performance requirements dictate business function structure. This structure will go through major changes in the next few years based on USACE stakeholder and customer demands. The business functions in the BRM dictate data and information needs found in the DRM, and application functionality found in the SRM. The relationship of the BRM to the TRM is one of give and take. The BRM drives applications in the SRM, which in turn drive the specific technology used, while new technology capabilities can create opportunities to improve processes.

The **CeA** business functions and subfunctions have a direct correlation to functions and subfunctions in the FEA (see Appendix E).

The **CeA** PRM framework shown in Figure 8.5 (September 2003 snapshot) will identify USACE business performance metrics and supporting USACE Information Technology performance metrics and the subfunction and sub-subfunction levels across the enterprise. The PRM relationship to the Business Reference Model (BRM) is one where the performance requirements dictate business function structure. These metrics will be rapidly developed and/or refined over the next several months based on USACE stakeholder and customer demands. The PRM also dictates data and information needs found in the Data and Information Reference Model (DRM), and application functionality found in the Service Component Reference Model (SRM).

The USACE Performance Plan(s) have a direct correlation to the Federal Performance Plan identified in the Federal Enterprise Architecture (FEA).

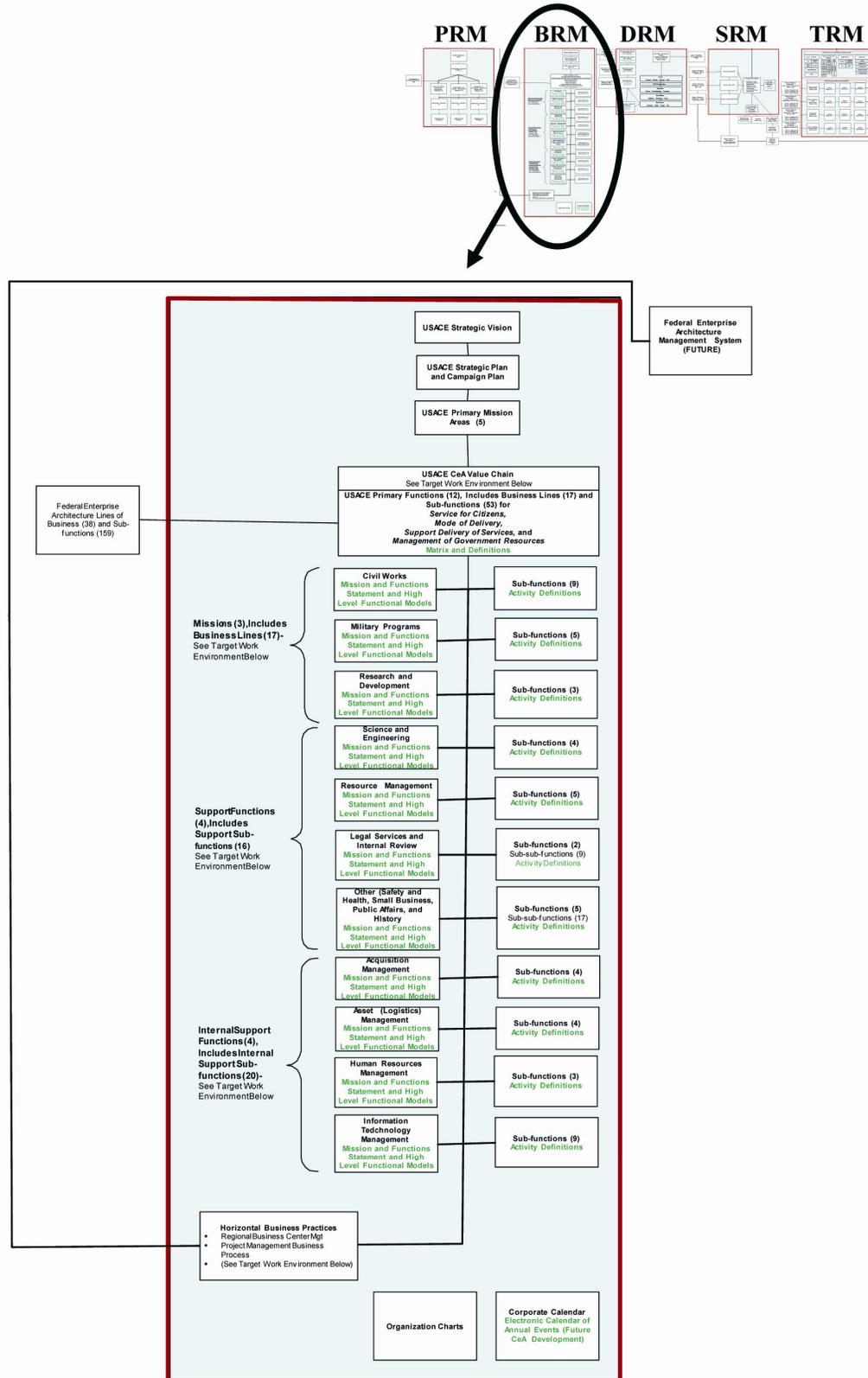


Figure 8.4. BRM framework (September 2003 snapshot)

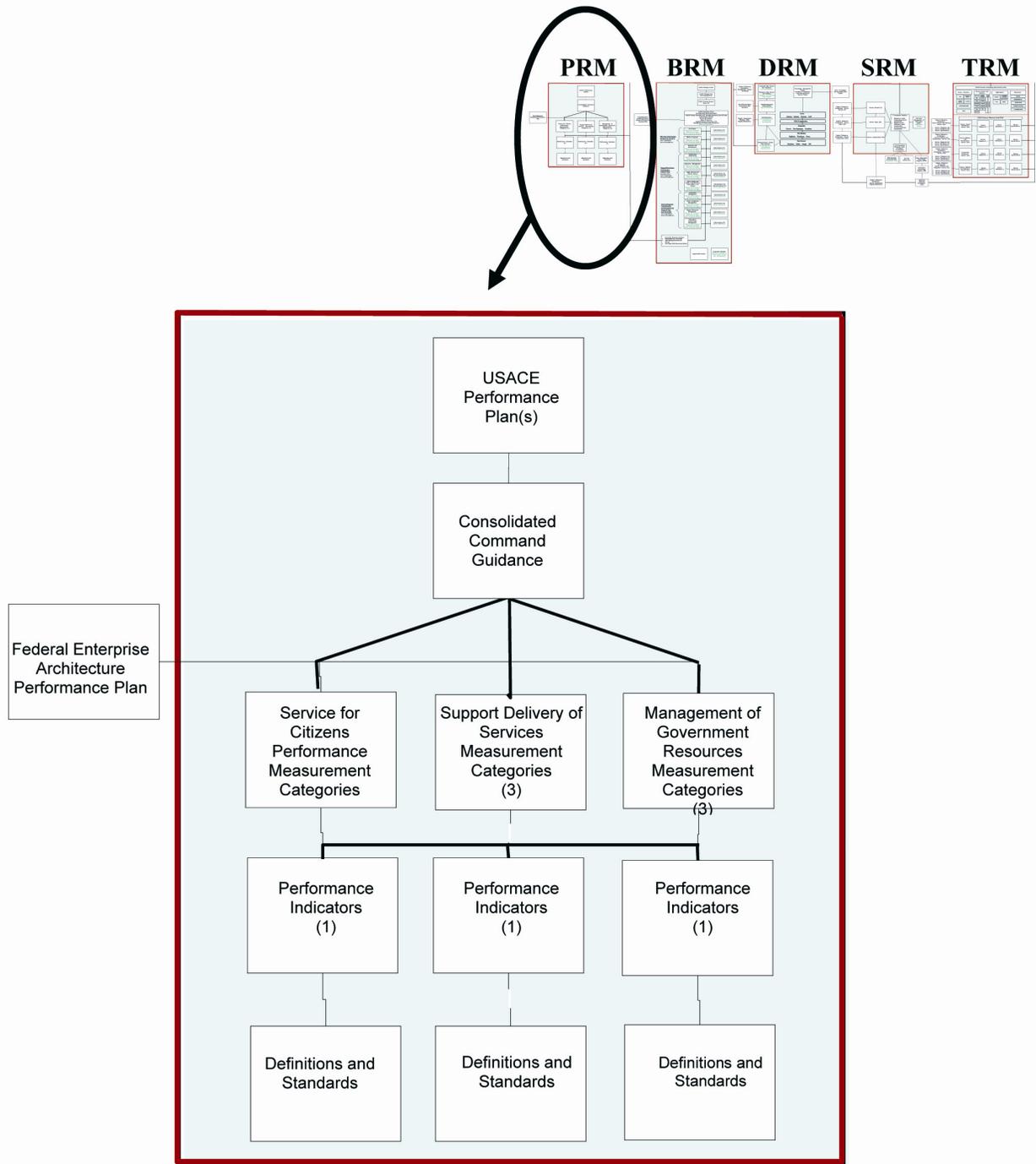


Figure 8.5. PRM framework (September 2003 snapshot)

The **CeA** DRM framework shown in Figure 8.6 (September 2003 snapshot) will identify USACE requirements and capabilities for sharing data and information across the enterprise. The DRM relationship to the BRM is one where the business owner, stakeholder, customer and public requirements for data and information dictate the timeliness, accuracy, placement and shareability of data and information. The DRM provides a view of how effectively data is meeting the needs for measuring performance, as required in the PRM. The housing and maintenance of data created by USACE applications will be mapped at the component level, from applications found in the SRM to standard data classes and data elements prescribed in the DRM.

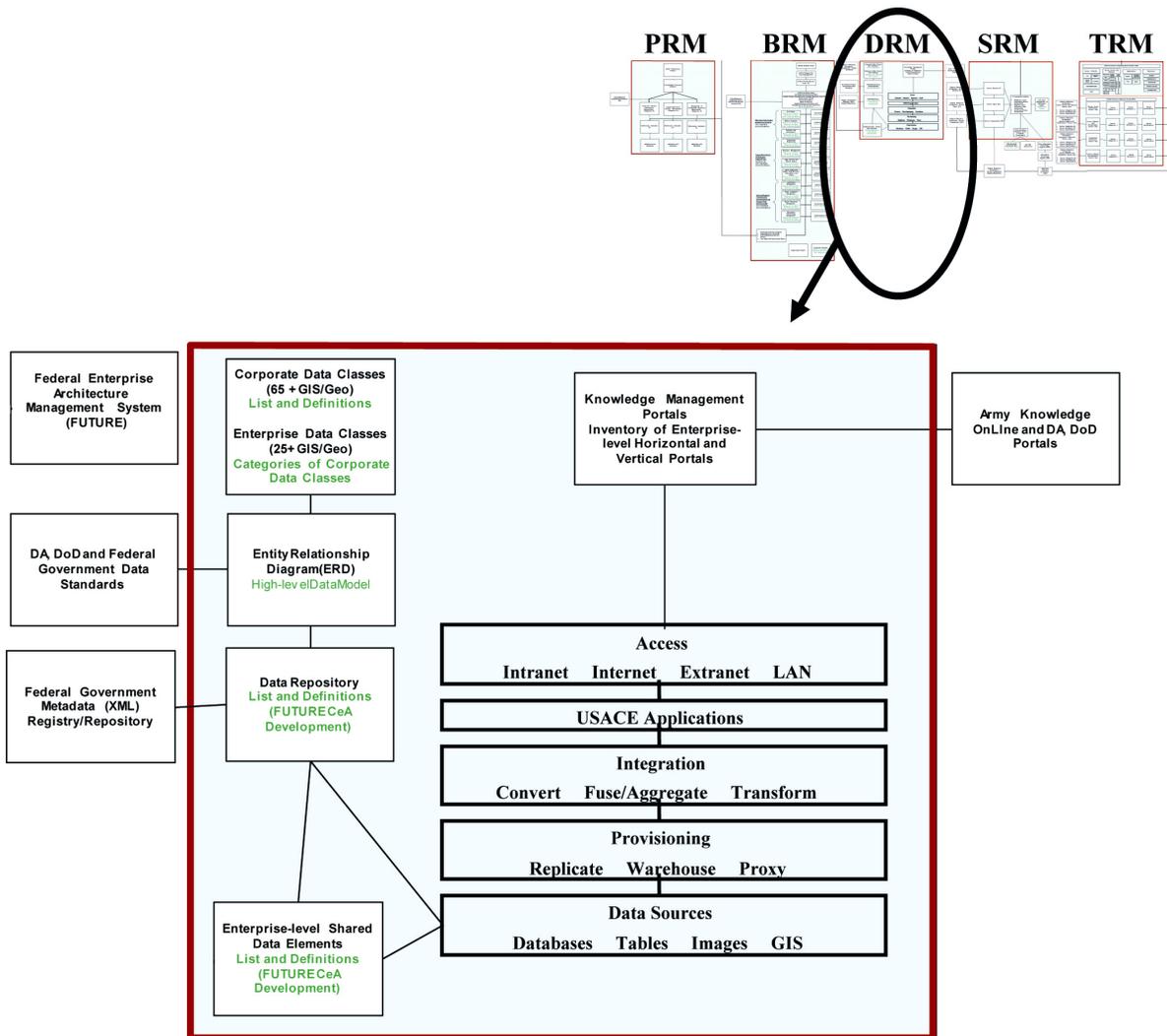


Figure 8.6. DRM framework (September 2003 snapshot)

CeA DRM data classes and data elements will map to DA, DoD, and Federal standards and repositories like the Federal Enterprise Architecture Management System (FEAMS). FEAMS was recently completed and released in mid FY04.

The **CeA** SRM framework shown in Figure 8.7 (September 2003 snapshot) will identify USACE automated applications and IT tools used by business owners, stakeholders, customers and the public to improve processes and obtain information across the enterprise. The SRM relationship to the BRM is one where the business owner, stakeholder, customer and public requirements for process improvement are catalogued and improved over time. USACE applications will be mapped at the component level, from applications found in the SRM, to standard data classes and data elements prescribed in the DRM. The relationship of the SRM to the TRM is one of give and take. SRM application technical requirements drive technical specification, while new technology capabilities can create opportunities to improve processes.

CeA SRM components will directly map to the FEA SRM framework, as well as other Federal, DoD, and DA application repositories. The SRM will be particularly useful in providing input to the USACE Capital Planning Investment Control process and input to the annual DA and/or OMB budget submission.

The **CeA** TRM framework in Figure 8.8 (September 2003 snapshot) will identify USACE-applied technology used to support performance found in the PRM, business functions found in the BRM, data collection and management found in the DRM, and automation requirements found in the SRM. Technology identified in the TRM will be used to assess opportunities for improvement in each of the other reference models as well.

CeA TRM components will directly map to the FEA TRM framework, as well as other Federal, DoD, and DA application repositories.

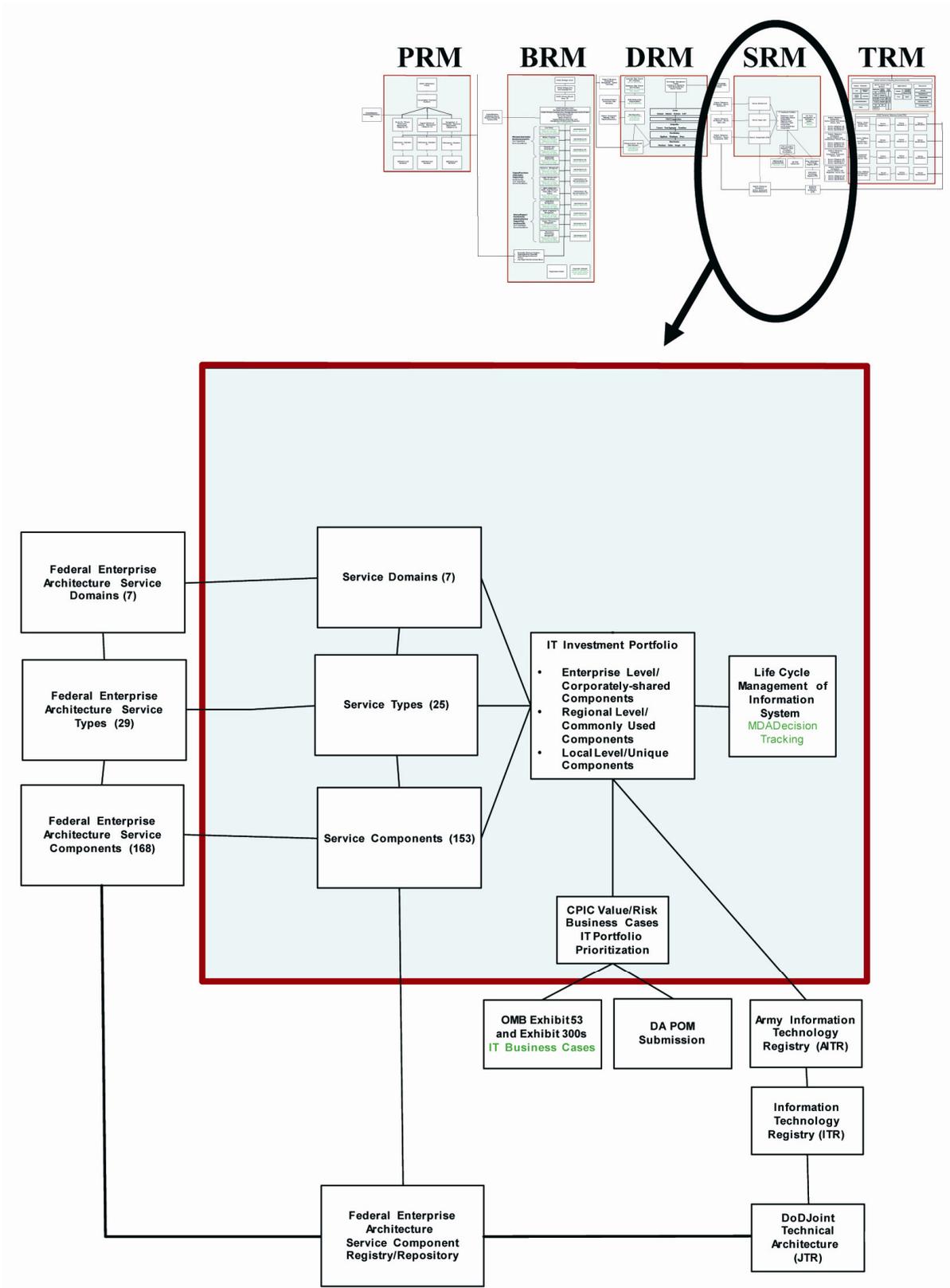


Figure 8.7. SRM framework (September 2003 snapshot)

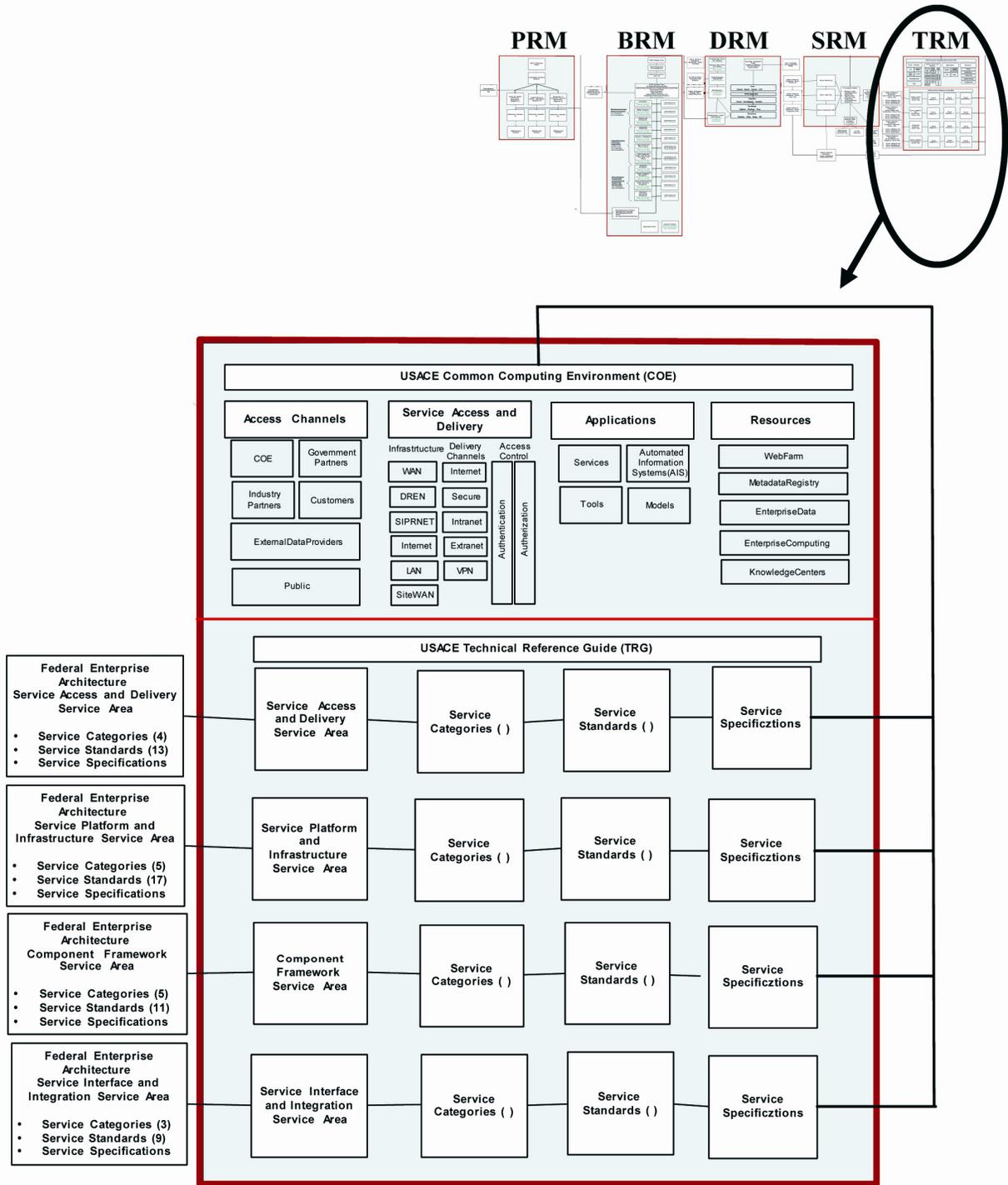


Figure 8.8. TRM framework (September 2003 snapshot)

Appendix A – Principles



Decisions made about USACE IT assets have important consequences to the ability to deliver quality service to customers. These decisions are based on sound professional guidance. **CeA** principles were established to provide universal constraints that narrow the parameters of success in applying **CeA** concepts for aligning IT assets with business requirements. The Principles below serve as common thread throughout the development and use of the **CeA**.

Value Added Principles:

- IT policies and practices improve customer satisfaction by improving delivery of products and services.
- The **CeA** supports the USACE Strategic Vision, Campaign Plan, missions and operations.
- The **CeA** is business driven, delineating business functions and subfunctions.
- IT activities are communicated and disseminated throughout the enterprise.
- Sound business decisions are enhanced by aligning the **CeA** framework with business needs.
- The **CeA** is used by systems developers to promote efficiency and effectiveness of individual IT products and services as they evolve.

Performance Principle:

- Performance metrics are established, approved, and measured.

Change Management Principle:

- Changes to the **CeA** will include input from stakeholders to ensure improvement in workforce productivity.

Availability Principles:

- Systems, applications and data are available 24x7
- Applications and data are redundant, recoverable & continuous as necessary to ensure continuity of operations

Standards-Based Principles:

- **CeA** policies, procedures, and practices conform to standards.
- Established standards (Federal, DoD, Army, Industry, Best Practices) are complemented to reinforce a common operating environment.
- New Standards are approved, controlled, planned, tested, add value to business function, financially justified, and documented iteratively.
- Standards are chosen to maximize interoperability.

Information Principles:

- Structured and unstructured data is treated as a corporate resource in support of business operations.
- Information is accurate (Confidential, Integrity, and Available).
- Information is timely/synchronized.
- Information is protected.
- Information is appropriately shared/distributed.
- Information is warehoused and mined in support of knowledge-centric activities.
- Information is consistent and indexed and taxonomy will be used to search for information.

Appendix B – Communication Plan



Purpose: The purpose of the **CeA** Web site is to provide an information exchange between business owners and IT professionals.

Communication Vehicle: The **CeA** Web Site (<https://cea.usace.army.mil/>) will serve as the primary source for **CeA** information.

Primary Audiences: The following communities are target audiences of the Web site:

- Business Owners
- Strategic Planners
- System Developers
- CIO Staff
- CeA Team Members

Business Owners and Strategic Planners: come to find information about other business functions and their relationships to IT. They provide information about their business areas. They see opportunities to create synergy.

System Developers: come to find out about the building codes (standards) that are to be used for Corps projects. They also find out about existing tools used in the Corps. They provide information about solutions to problems that they have found.

CIO Staff: come to support their stewardship responsibilities for the Capital Planning and Investment Control process. They provide information about policies, especially from DA and DoD. Members of the Investment Control committees (CFAT, EFAT) use it to support their decision-making work.

CeA Team Members: come to review documents and to provide information and solutions to problems posed.

Each audience uses the tool to ask questions via the forums, and provide answers within their areas of knowledge. All team members may post documents. The tool supports the Corps as a learning organization.

Because there are other Web sites that contain information of interest to the business and information technology communities, the following rules are provided to make the relationships clearer:

- To reduce the maintenance burden, and prevent duplication, point to original sources of information rather than duplicating it here.
- Consider information found at the site to be references.
- All information on the site is unclassified, and can be viewed by anyone with access to the usace.army.mil domain.
- Site registration (profile) gives the user the ability to upload documents and to contribute to the forums.

Appendix C – Team Members



Ce A Team List - 2 September 2003, POC: Tony Brunner

Team Member	Office	PRM	BRM	KM	DRM	SRM	TRM	IA	M&M	Strat Comm	Resource Team
1 Aiken, Chris	QuTech	C	C		C				C		
2 Bank, Robert	CECW-EE		X						X		
3 Bentz, Eugene	CESAM-OP-R						A				
4 Berrios, Wil	CECI-ZA	CIO	CIO		CIO	CIO	CIO	CIO	CIO	CIO	
12 Bradley, Sam	CEDC-ITL						X				
5 Brunner, Tony	CECI-H	PM	PM		PM	PM	PM	PM	P	PM	
6 Butler, Cary D	ERDC-ITL-MS				X		P				
7 Cadieu, Vesta S	CECI-H									P	
8 Charlton, Sondra	CECI-A							P			
9 Clark, Terence B	CECI-H						X				X
10 Demby, Constance E	CECI-TA				X				X		
11 DuPuis, Barry	QuTech	C	C		C						
13 Ercums, Namejs	CERE-R-PD					X			A		
14 Faget, Nancy G	CEHEC-IM-L				X						
15 Fagot, Liz	CERE-ZB		X								
16 Frank, Richard	CECC-G										
17 Gmitro, Mark	CECS-PMBP		A								
18 Gooden, Brenda A	CECI-T								X		
19 Hart, Thomas	CEERD-Z		P								
20 Hamilton, Jeffrey	QuTech	C	C		C				C		
21 Henderson, Michael	CECI-TA						X				
22 Howard, Esther	CECI-ZO										X
24 Jones, Chuck	QuTech	C	C		C				C		
25 Lanzarone, John R	CECW-EE				X						
26 Lichy, David E	CEIWR-NDC-N	X	X		PM	X	X	X	X	PM	
27 Lynn, Raymond L	CEDW-EI	X			X	X					
28 Mahoney, Sally E	CECI-TR									P	
29 Matyas, Gary	QuTech	C	C		C				C		
30 McDermott, Kathleen	CECI-H										
31 Miles, Moody K	CECW-EE		X			P					
32 Mordecai, William H	CEFC-S	X			X						
33 Pixa, Rand	CECC-L				X						
34 Rice, Judith V	CECW-ON				X						
35 Romano, Cathy	CECI-A							X			
36 Rowson, David M	CECI-ZB	A									
37 Seguin, Paul B	CECS	P									
38 Sevila, William W	CECI-TR					A					
39 Sheridan, Catherine A	CECI-TA		X								
40 Spewak, Steve	Dig Consult Inc	C	C		C				C		
41 Stolley, Joan I	CECI-H				P						
42 Stoutenburgh, Linda E	CEFC-ZI	X			X	X					
43 Titus, Martin	CECI-T						X				
44 Toole, Jeff	QuTech	C	C		C				C		
45 Urena, Raymond F	CELD-MS		X		X	X					
46 Walker, Chester B	CECI-TA	X									
47 Walters, Meredith C	CECI-A							P			
48 Pinol, Phil	CEMP-MP	X	X		A	X	X	X	X		
23 Gunn, Daryll	Thomas and Herbert					C					

Technical Architecture Working Group

Cary D. Butler	TAWG
Eugene Bentz	TAWG
Roger Souser	TAWG
Michael Henderson	TAWG
Paul May	TAWG
John Samuelson	TAWG
James Ligh	TAWG
TBD	TAWG
Greg Bigelow	TAWG
York Yarbrow	SME - CEEIS
Denise Martin	SME - CDF
Peggy Wright	TAWG
Tony Brunner	CEA Lead
Sam Bradley	SME - CEEIS
David Richards	SME - Scientific Computing
Toby Wilson	SME - CADD and GIS
TBD	

Notes:

- PRM** - Performance Reference Model
- BRM** - Business Reference Model
- DRM** - Data and Information Reference Model
- SRM** - Service Component Reference Model
- TRM** - Technical Reference Model
- IA** - Information Assurance Architecture
- M&M** - Management and Maintenance
- Strat Comm** - Strategic Communications Team
- Resource Team**
- CIO** - Chief Information Officer
- PM** - Project Manager
- P** - Primary Team Leader
- A** - Alternate Team Leader
- X** - Team Member
- C** - Contractor

Appendix D – Business Functions and Subfunctions



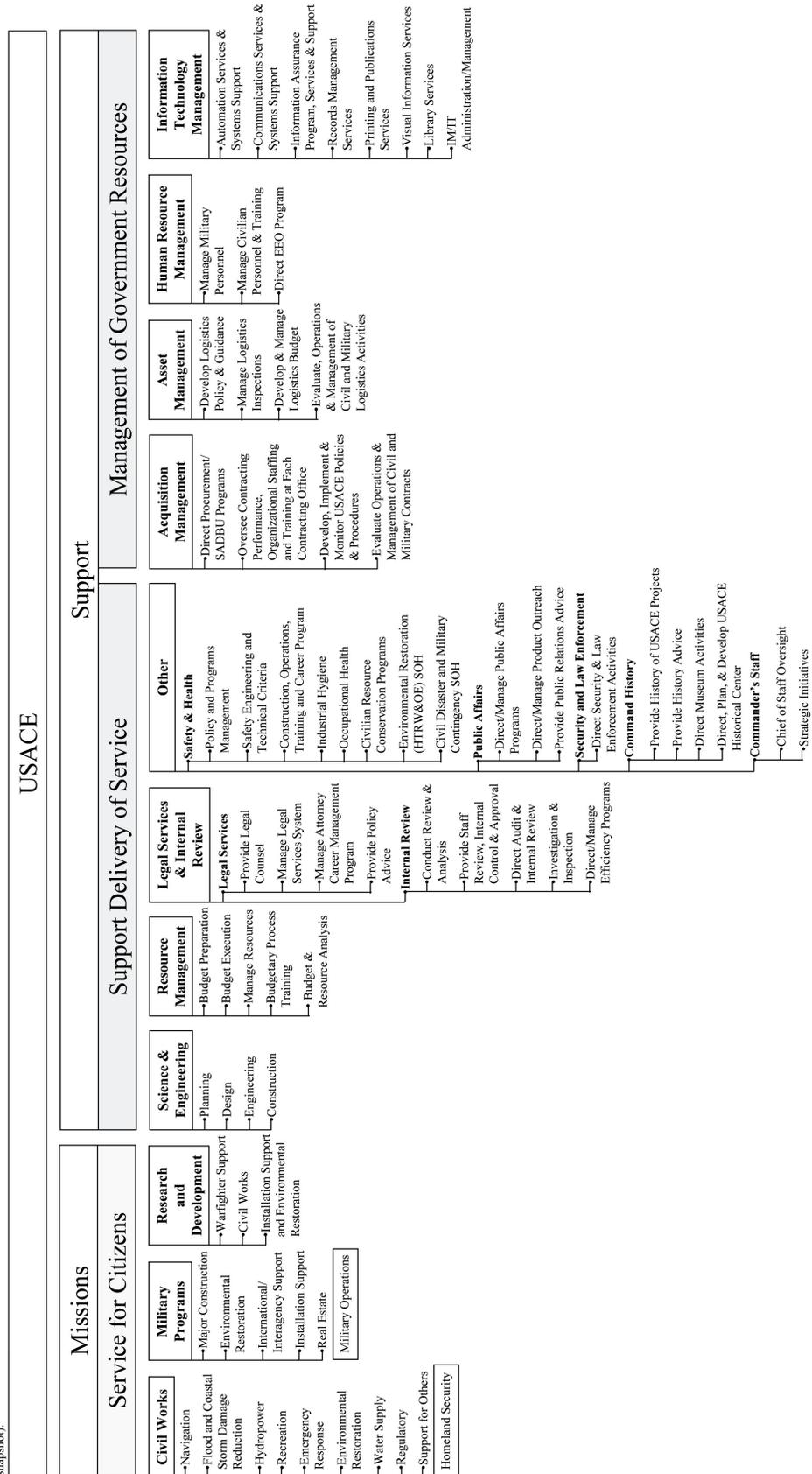


USACE Business Functions

Last Update: 2 June 2004

POC: Tony Brunner, CeA Chief Architect

The Hierarchy diagram below depicts the functional decomposition of the primary business areas (2004 snapshot).



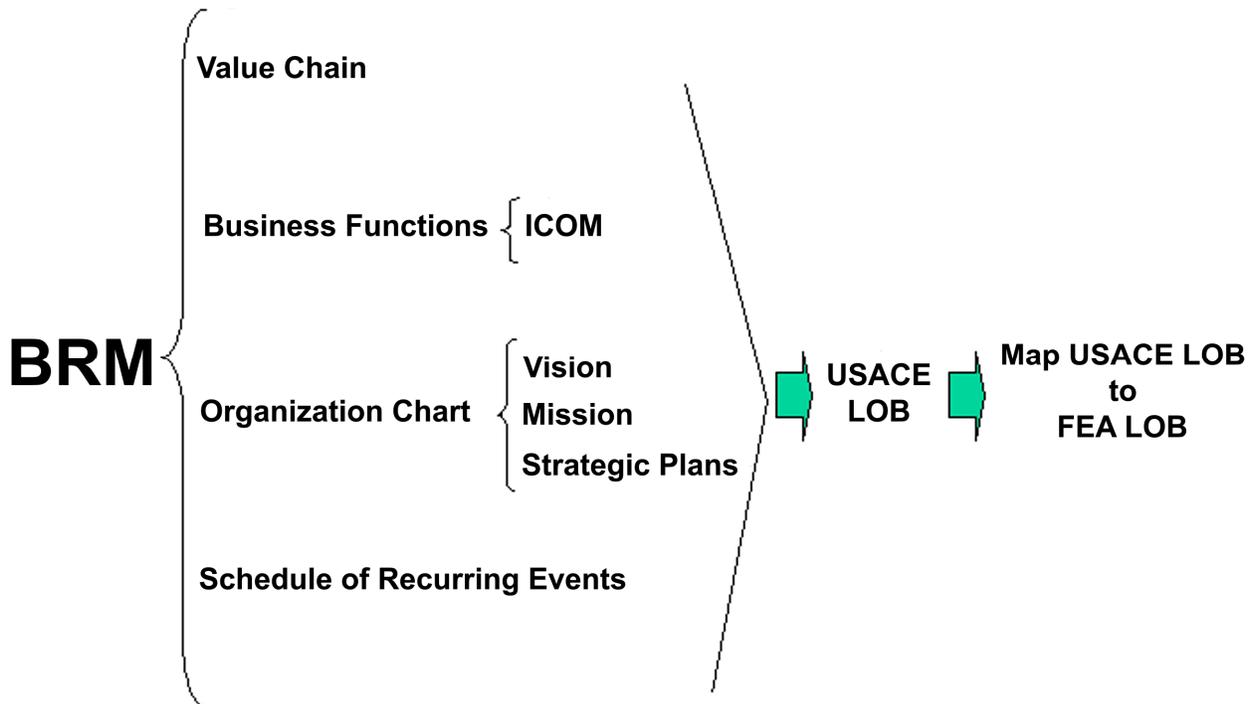
Appendix E – Enterprise-Level IT Investments Mapped to Federal Business Functions



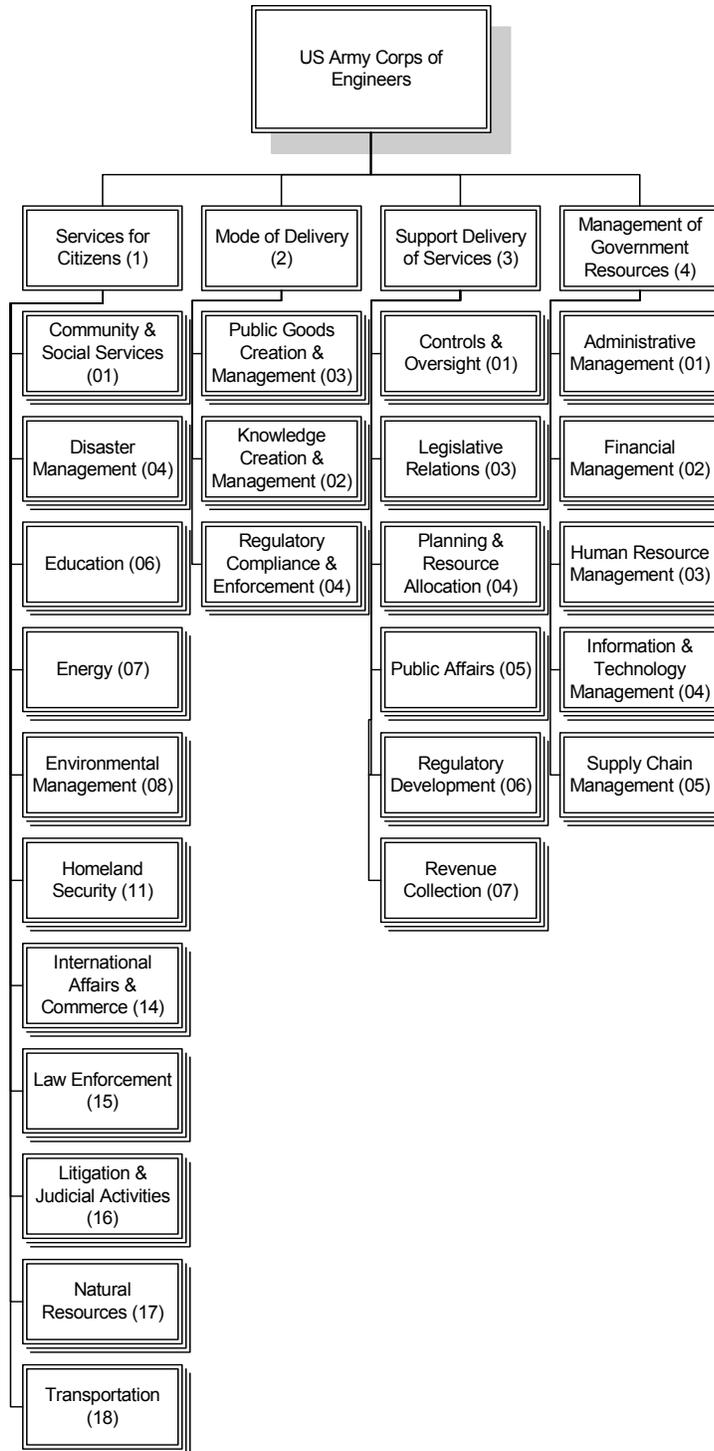


CORPS ENTERPRISE ARCHITECTURE
APRIL 2005

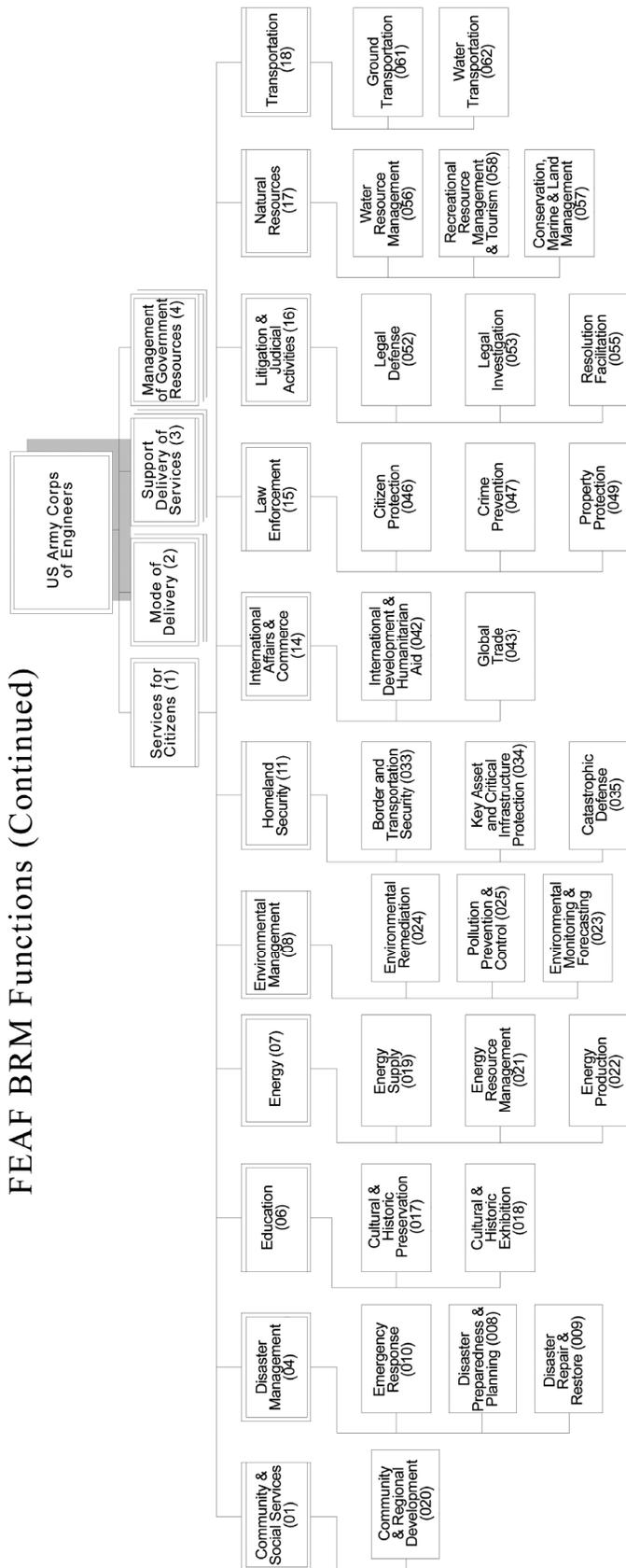
Appendix F – Lines of Business Mapping to the FEA Lines of Business



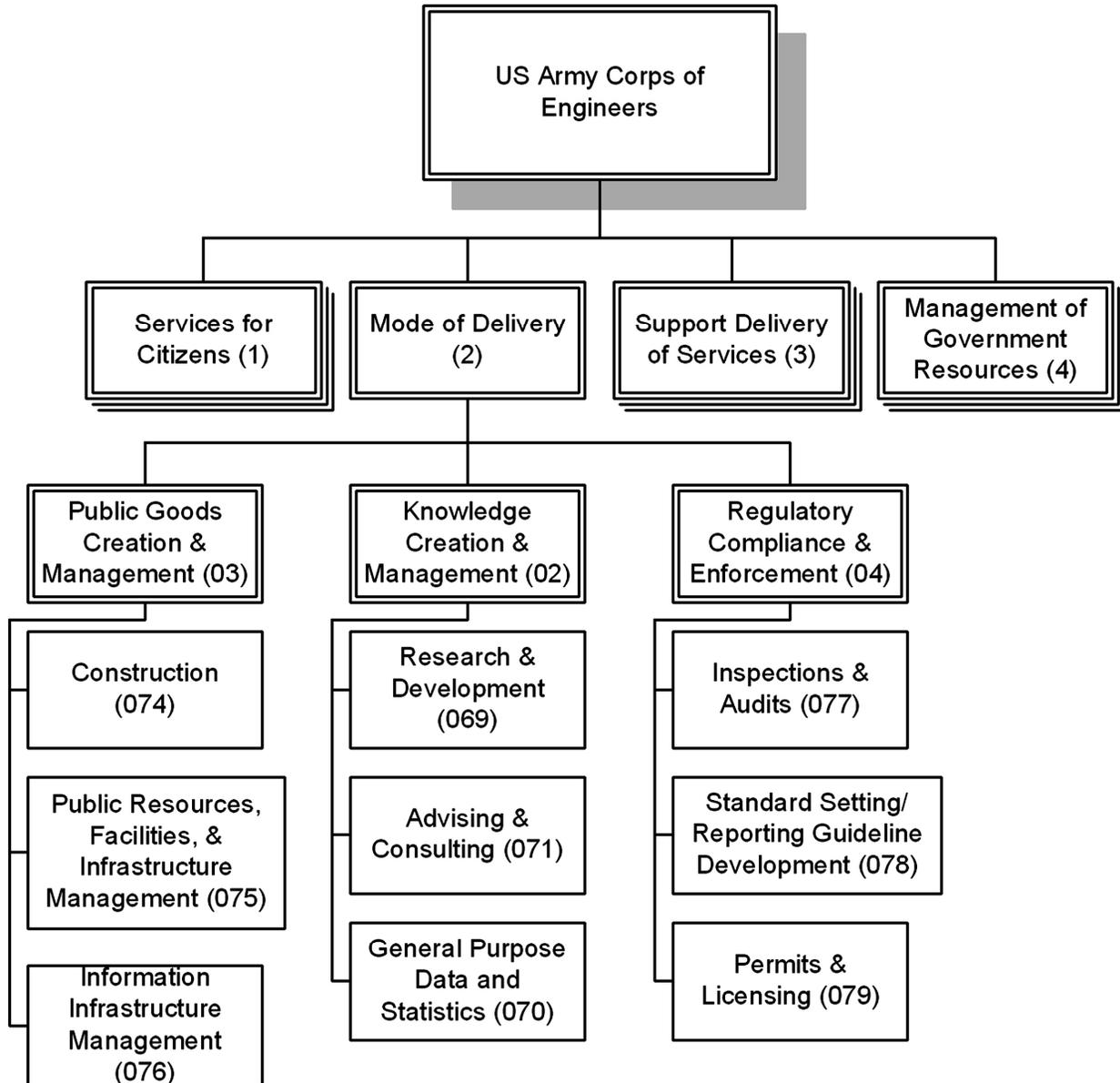
FEAF BRM Functions (Continued)



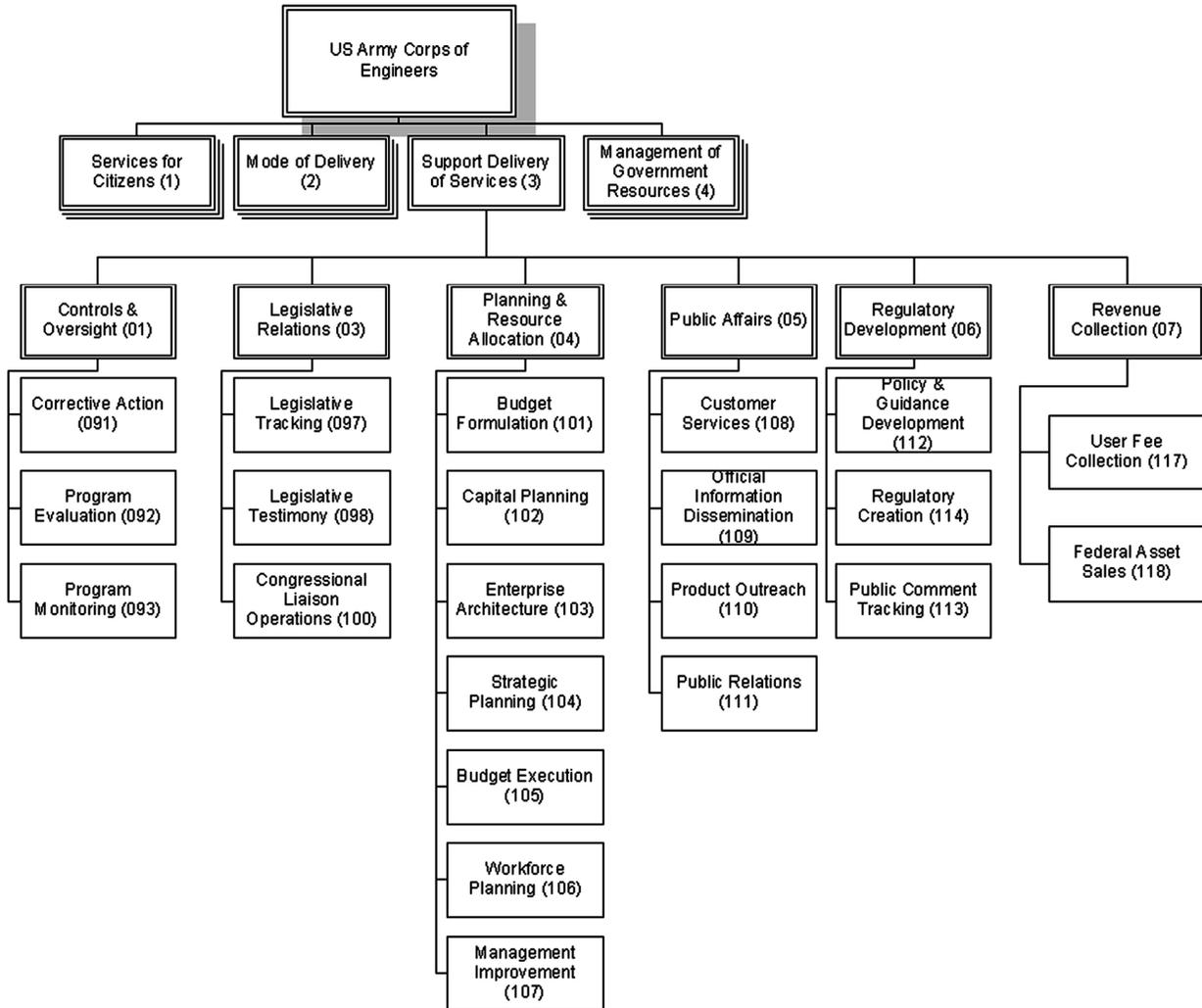
FEAF BRM Functions (Continued)



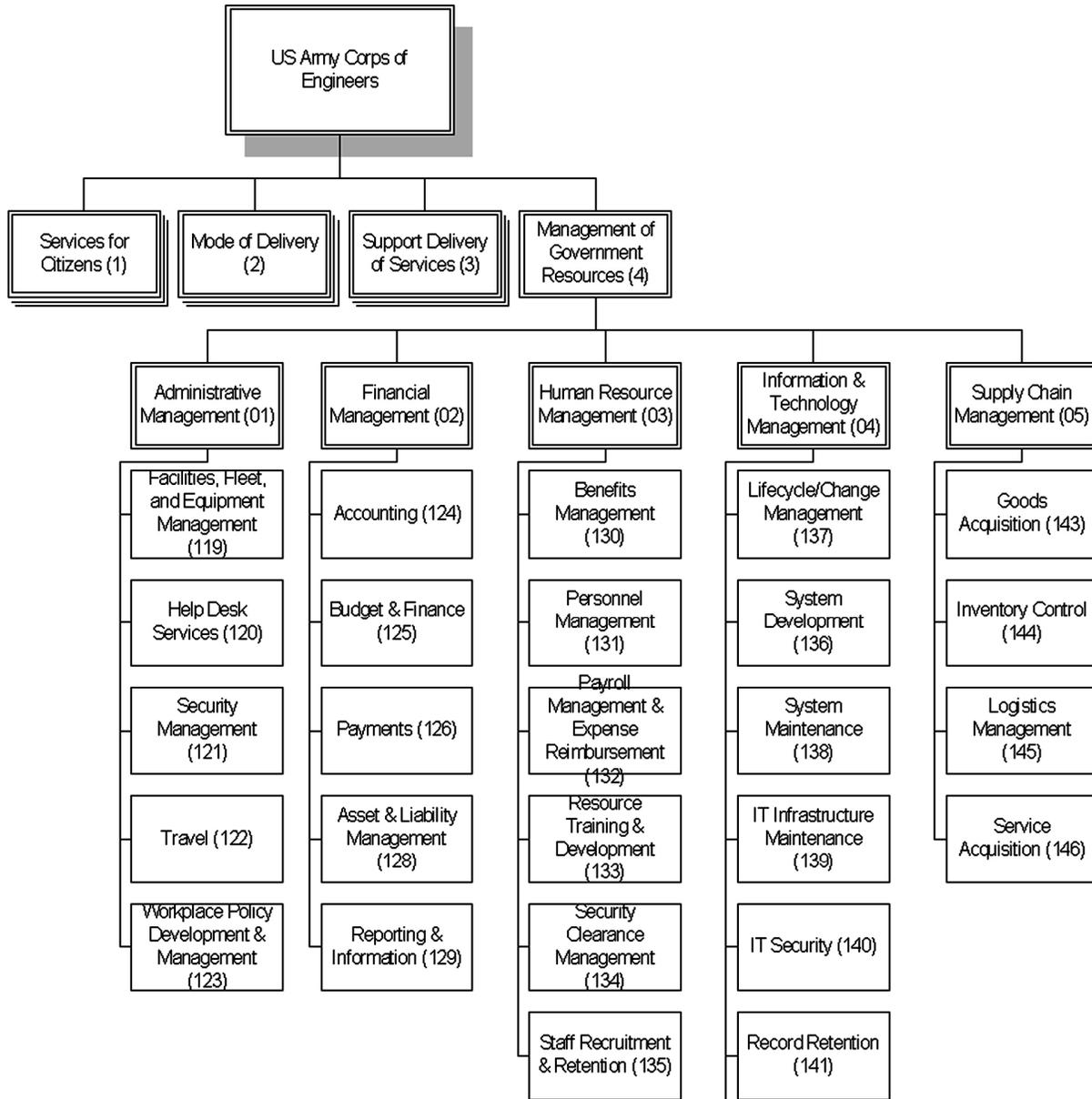
FEA FBRM Functions (Continued)



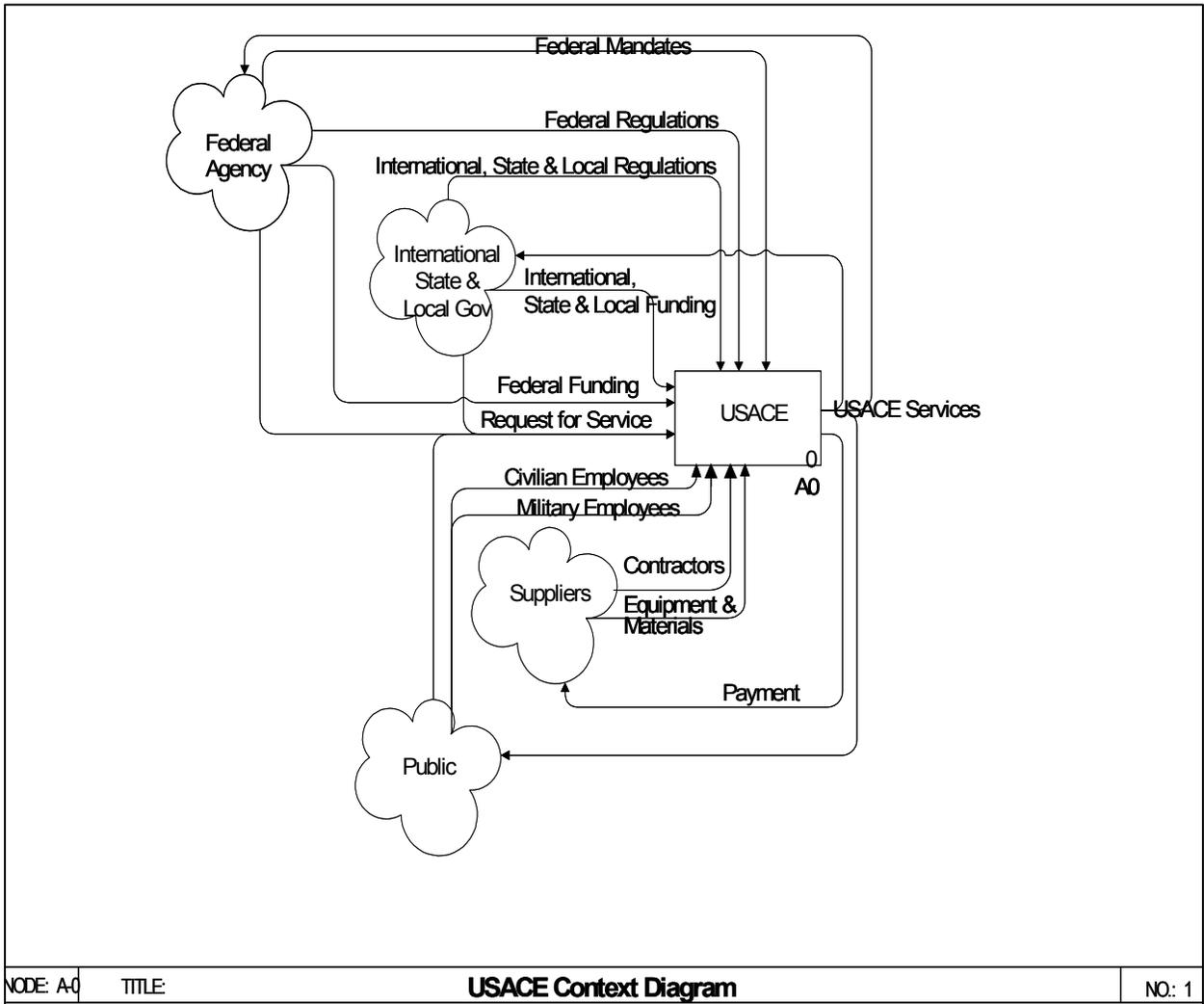
FEA FBRM Functions (Continued)



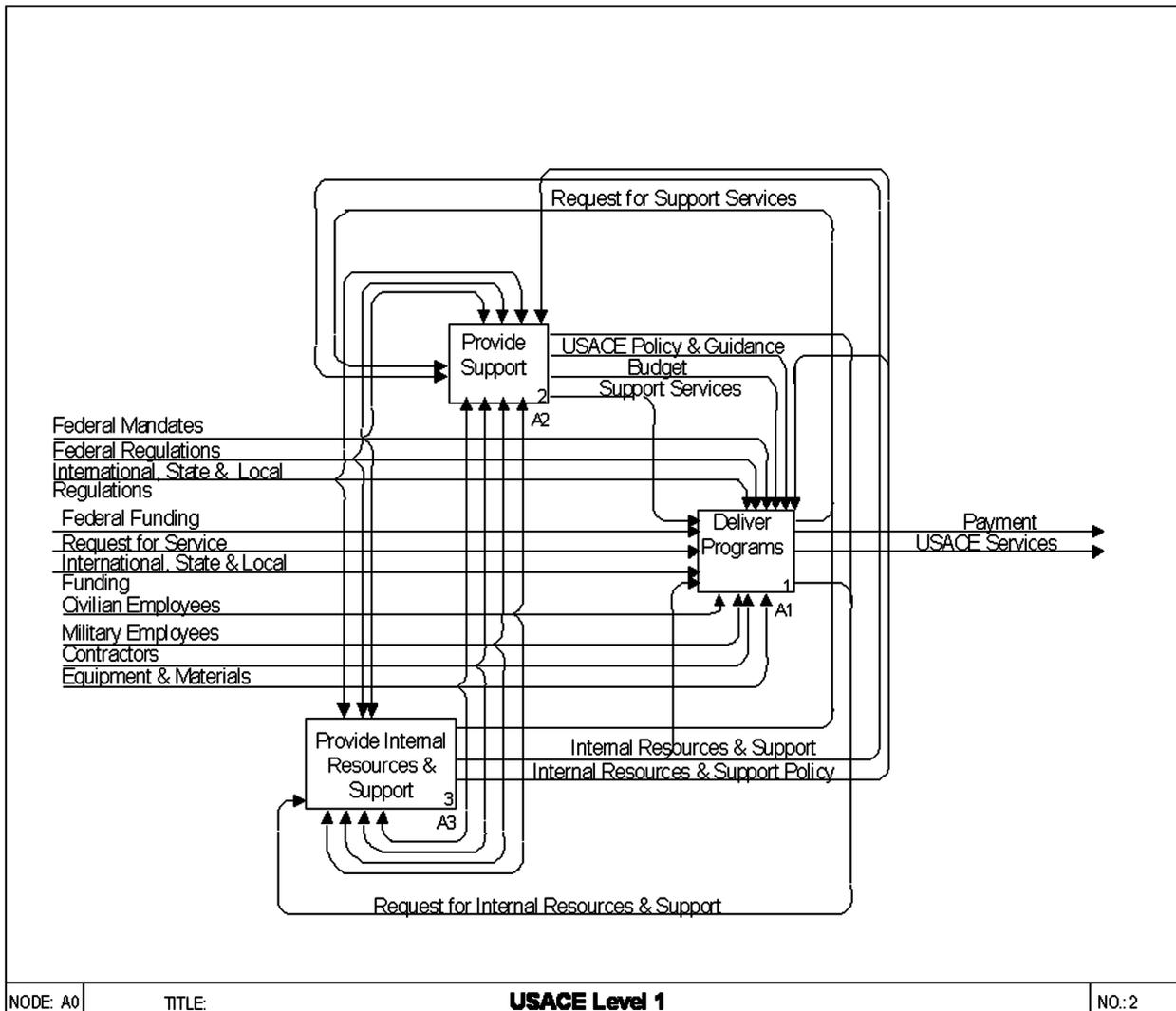
FEA FBRM Functions (Continued)



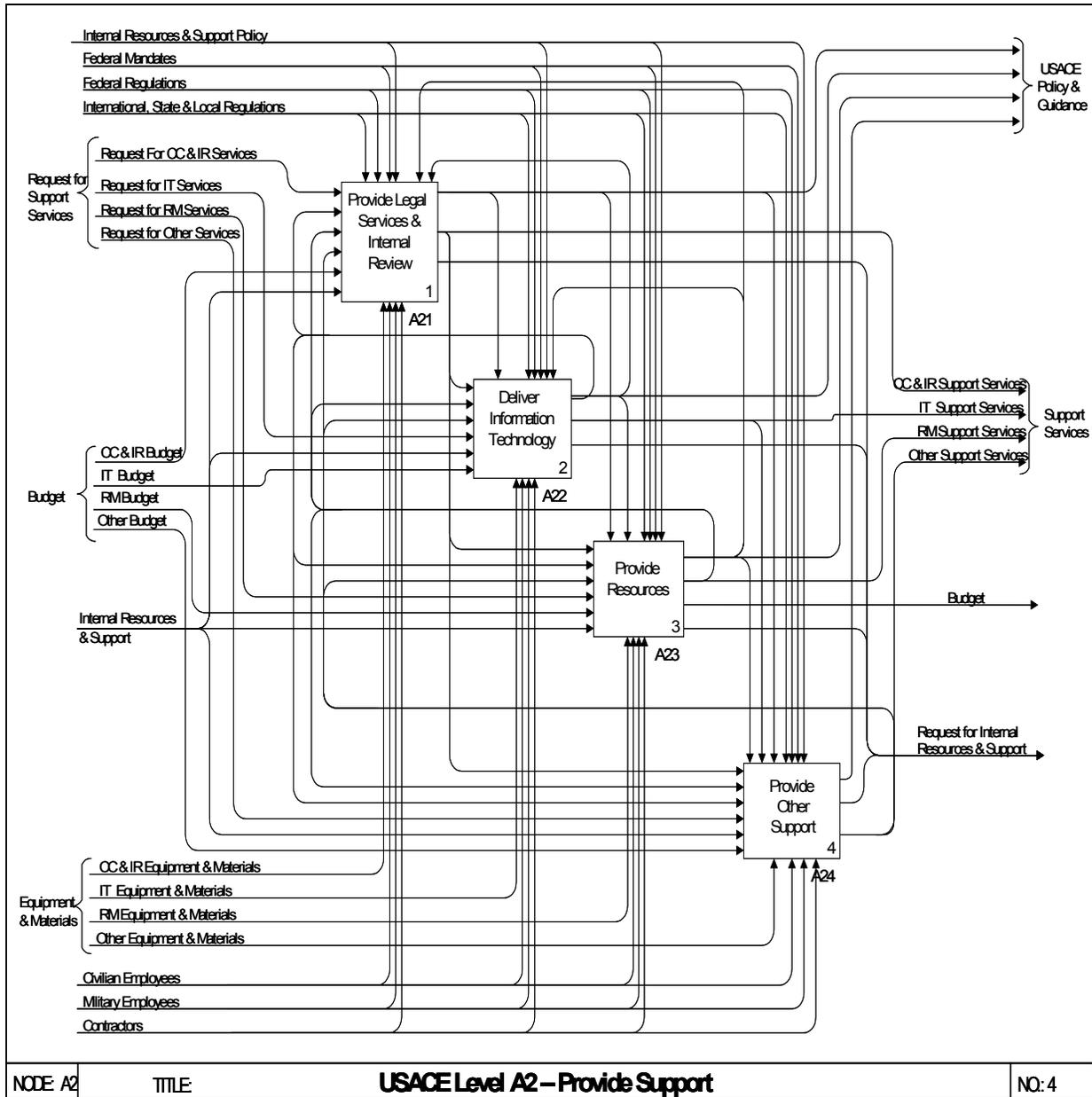
Appendix G – Functional Level ICOM



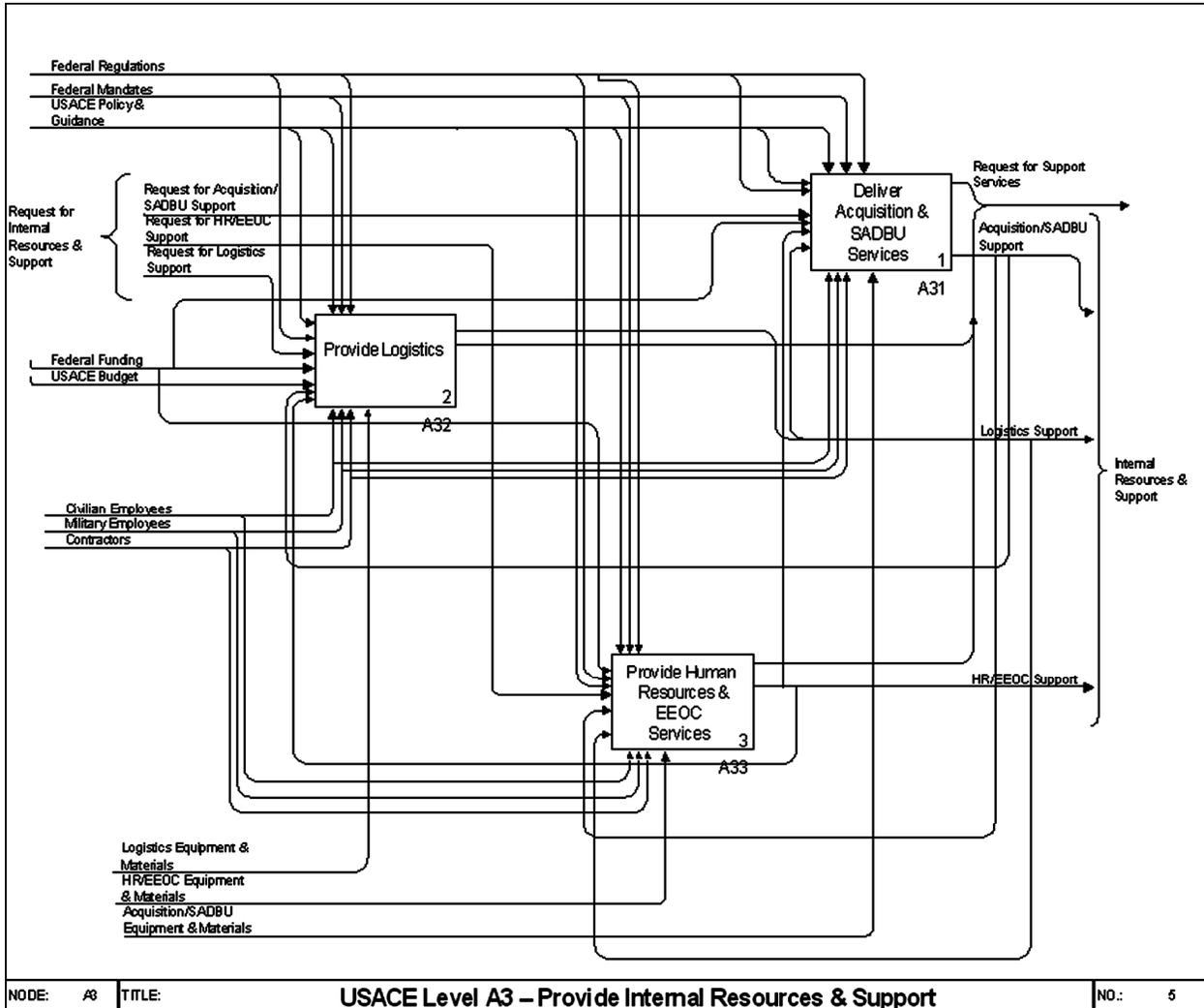
The chart below shows ICOM exchanges between Programs, Support, and Internal functions (See the Value Chain diagram).

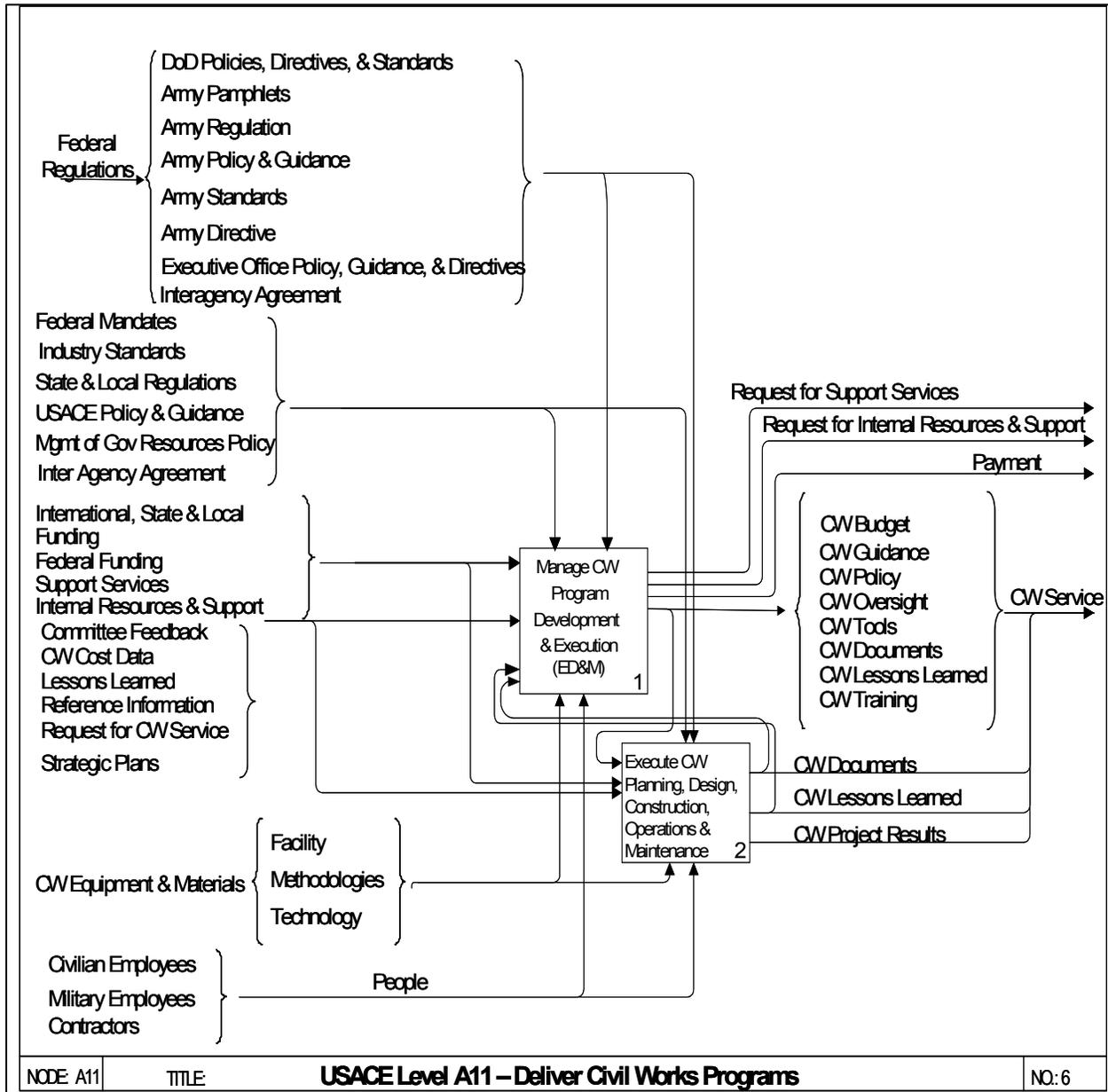


The chart below shows ICOM exchanges between Legal Services & Internal Review, Information Technology Management, and Resource Management (see Value Chain diagram).



The chart below shows ICOM exchanges between Acquisition Management (including the Small and Disadvantaged Business Unit), Logistics Management, and Human Resources Management and the Equal Employment Opportunity Office (see the Value Chain diagram).





Appendix H – Charting the Target Work Environment

Prepared 27 April 2004
Tony Brunner, **CeA** Chief Architect

H.1 Process for Identifying Information Technology Requirements for the Target Work Environment (TWE)

The **CeA** Project Delivery Team (PDT) identified 13 business practices as expressions of end states for the Target Work Environment (TWE). These 13 end states are known

directives extrapolated from the USACE Vision, strategic and tactical business initiatives. The TWE end states are in alignment with the **CeA** guiding principles established as parameters for developing the evolving target architecture. Sculpting and migrating to the TWE will always be a growing and changing process. The descriptions provided here are considered high-level, minimum definitions, intended to provide general direction on Information Technology (IT) investment decisions. More detailed analysis and considerations will be conducted as IT investment decisions are made at the enterprise, regional and local levels.

H.2 USACE Target Work Environment

The TWE focuses on business functions and subfunctions that transcend organizational structure and work location in the future. The optimal USACE organizational structure will evolve through senior-led growth and analysis of the following seven elements: Structure, Strategy, Systems, Shared Values, Stakeholder Values, Style of Leadership, and Skills. For detailed information, refer to the USACE 2012: The objective Organization via 7S Model, found in the Corps Enterprise Architecture (**CeA**), **Appendix A** (reference available: <https://cea.usace.army.mil/>).

The following 13 TWE end states are the linchpin to a successful **CeA**:

1. Enterprise (Corporate-level) Program Asset Management
2. Regional Watershed and Installation Management
3. Protection of USACE Critical Military and Civil Infrastructures
4. Integrated Emergency Management and Homeland Security
5. Enhanced Communications and Information Access Throughout USACE
6. Enhanced Management of Business Processes (Example: Online Applications)
7. Enterprise Management of Manpower Resources
8. Enterprise and Regional Acquisition Strategy
9. Enterprise Management of Knowledge That Includes Best Practices, Registry of Skills, Customer Feedback, Lessons Learned, Corporate Issues Management, etc.
10. Enterprise Processes to Manage Technology and Data

11. Methods for Data Exchange with Government and Industry Partners
12. Internal and External Virtual Teaming
13. One Stop Web Access to USACE Public Information

H.3 CeA TWE End States and Description Summaries

H.3.1. Enterprise (Corporate-level) Program Asset Management

TWE Summary: Business practices in the TWE associated with *Enterprise Program Asset Management* will require IT investments that improve analytical modeling capabilities, and improve collaboration/communications between USACE and other Federal agencies.

H.3.2. Regional Watershed and Installation Management

TWE Summary: Business practices in the TWE associated with *Regional Watershed and Installation Management* will require IT investments that improve USACE enterprise-level automated information system (AIS) interoperability, data sharing, collaboration and communications between USACE and other Federal, state, local and tribal organizations, as well as trusted partners like universities and private industry.

H.3.3. Protection of USACE Critical Military and Civil Infrastructures

TWE Summary: Business practices in the TWE associated with *Protection of USACE Critical Military and Civil Infrastructures* will require IT investments that improve USACE current capabilities for Federal-level data sharing, detection, warning, alert systems and analysis of potential terrorist attacks.

H.3.4. Integrated Emergency Management and Homeland Security

TWE Summary: Business practices in the TWE associated with *Integrated Emergency Management and Homeland Security* will require IT investments that improve Geographic Information Systems (GIS), cross-agency data sharing/application interoperability, mobile communications, tele-engineering, intra-agency modeling, response simulations and other information especially related to watersheds.

H.3.5. Enhanced Communications and Information Access Throughout USACE

TWE Summary: Business practices in the TWE associated with *Enhanced Communications and Information Access Throughout USACE* will require IT investments that improve enterprise-level interoperability among USACE AIS, data warehousing, data transport, collaborative tools, security, and decision support tools.

H.3.6. Enhanced Management of Business Processes (Example: Online Applications)

TWE Summary: Business practices in the TWE associated with *Enhanced Management of Business Processes* will require IT investments that improve AIS component-level interoperability for internal and external users (examples include single sign-on or online applications).

H.3.7. Enterprise Management of Manpower Resources

TWE Summary: Business practices in the TWE associated with *Enterprise Management of Manpower Resources* will require IT investments that ensure state-of-the-art science and engineering automated tools, standard practices and treatment of data as a corporate asset (data warehousing) in support of virtual teaming.

H.3.8. Enterprise and Regional Acquisition Strategy

TWE Summary: Business practices in the TWE associated with *Enterprise and Regional Acquisition Strategies* will require IT investments that maintain and improve regional acquisition-related AIS.

H.3.9. Enterprise Management of Knowledge That Includes Best Practices, Registry of Skills, Customer Feedback, Lessons Learned, Corporate Issues Management, etc.

TWE Summary: Business practices in the TWE associated with Enterprise Management of Knowledge That Includes Best Practices, Registry of Skills, Customer Feedback, Lessons Learned, Corporate Issues Management, etc., will require IT investments that consolidate current AIS and system components which currently provide similar services.

H.3.10. Enterprise Processes to Manage Technology and Data

TWE Summary: Business practices in the TWE associated with *Enterprise Processes to Manage Technology and Data* will require IT investments in the IT infrastructure to bring state-of-the-art computing capabilities to the desktop, and implement a clear path to increased access/use of corporate data via shared data repositories.

H.3.11. Methods for Data Exchange with Government and Industry Partners

TWE Summary: Business practices in the TWE associated with *Methods for Data Exchange with Government and Industry Partners* will require IT investments that improve data collection, analysis and dissemination for internal and external information users.

H.3.12. Internal and External Virtual Teaming

TWE Summary: Business practices in the TWE associated with *Internal and External Virtual Teaming* will require IT investments that promote standard science and engineering tools and processes for internal and external team members to support virtual project management.

H.3.13. One Stop Web Access to USACE Public Information

TWE Summary: Business practices in the TWE associated with One Stop Web Access to Public Information will require IT investments that reduce reporting burdens, streamline business transactions, and provide automated support to decision making through an aggressive migration to Web-based electronic mechanisms.

H.4 Prescribed IT Focus for Supporting the TWE

- Improve communications capabilities between USACE and other Federal, State, University, and tribal organizations and other trusted partners.
- Improve data collection, analysis and sharing between USACE and other Federal, State, University, and tribal organizations and other trusted partners – particularly in areas of watershed management, infrastructure protection, homeland security and GIS.
- Improve collaboration and virtual teaming capabilities – particularly in the area of science and engineering tools/practices standardization.
- Improve USACE analytical modeling capabilities.
- Improve intra-agency modeling and response simulations, especially related to watersheds.
- Bring IT infrastructure state-of-the-art computing capabilities to the desktop.
- Consolidate current USACE AIS and system components providing similar services.
- Improve enterprise-level interoperability among USACE AIS.
- Improve AIS component-level interoperability for internal and external users (examples include single sign-on or online applications).
- Reduce reporting burdens, streamline business transactions through an aggressive migration to Web-based electronic mechanisms.
- Improve mobile communications.
- Improve tele-engineering capabilities.
- Provide decision support tools.
- Maintain and improve regional acquisition-related AISs.

H.5 Examples of Specific IT Initiatives Supporting the TWE

- Improvements in data management (standards, access, etc.).
- Select Data marts warehouses (GIS, homeland security, watershed management, etc.) for internal and external access.
- Increase in Web-based collaboration tools.
- Increase in regional/national IT contracts; decrease in local IT contracts.
- AIS consolidation at system and component level (CADD/GIS, business, lessons learned, etc).
- e-Corps (single sign-on, knowledge management horizontal portal, lessons learned, etc.).

- Standard suite of S&E tools to support virtual engineering.

H.6 Target Work Environment Analysis and References

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture
- PARC Web Page

H.7 Business and Organization Structure

The USACE Business Reference Model (BRM) in the TWE reflects an enterprise-centric approach to program and project management through Regional Business Centers (RBC). Civil Works, Military Programs, and Research and Development will continue to be USACE mission areas (also referred to as primary business functions). Each of these mission areas will additionally include Business Lines (sometimes referred to as Lines of Business). All remaining Business Functions are Support Functions (sometimes referred to as support services).

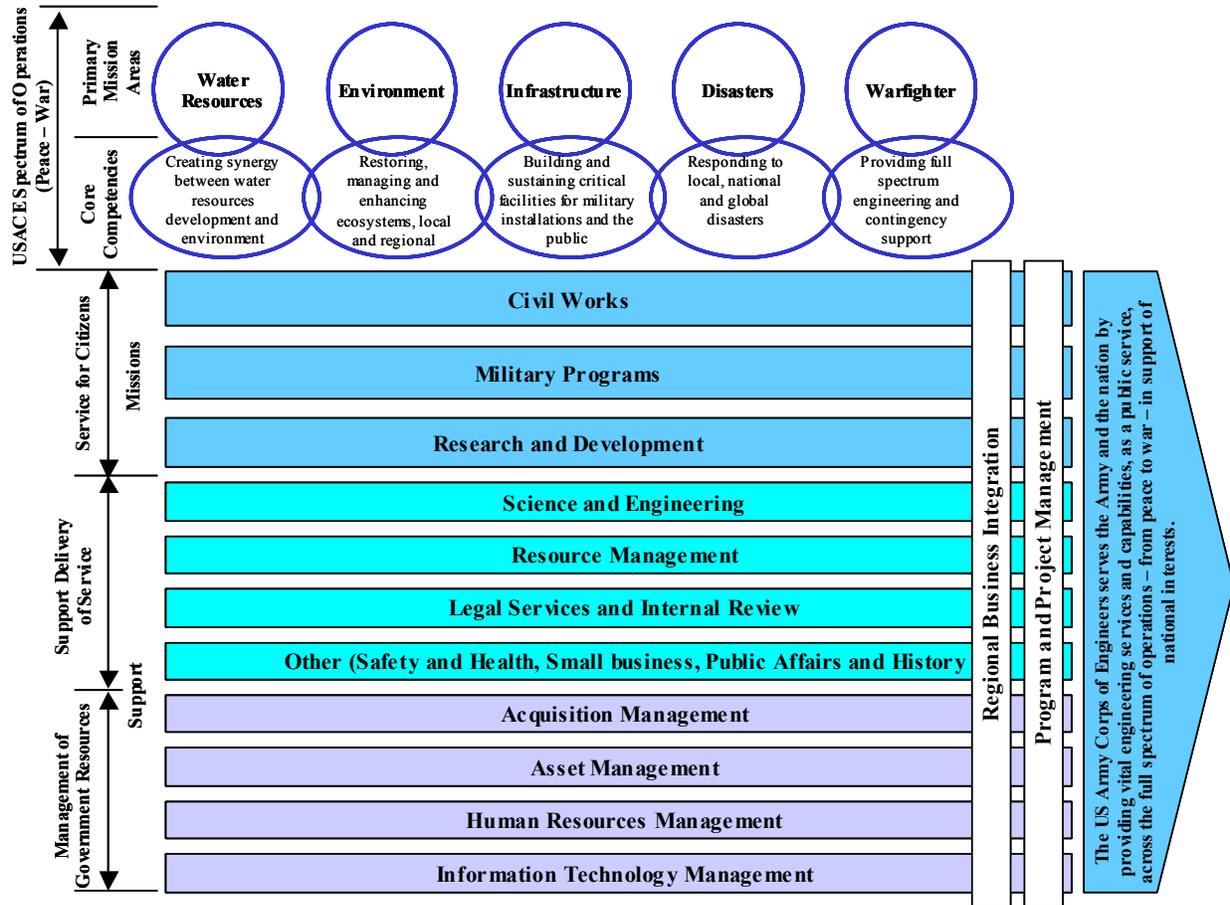


Figure H.1. USACE Target Work Environment Enterprise Statement and Value Chain

H.8 Guiding Principles for Creating the Target Work Environment (Excerpts from 2012 Implementation Plan)

- Act as “One Corps”:** Align and operate as one Corps with the primary responsibility, authority, tasks and activities at each echelon commensurate with the appropriate role. Promote the concept of mutual interdependence throughout the organization while aligning expertise with the work.
- Act as “One Headquarters”:** HQUSACE and the Division echelons are aligned and operate seamlessly as one headquarters and issues are resolved after only one staff level review. The lowest level possible is empowered to action. Functions at each level add value and eliminate redundancies. Program oversight and integration occur at the Washington Headquarters and program management takes place at the Regional level.

- **Washington Headquarters Focus:** Washington Headquarters is focused primarily on strategic learning, planning and direction, national relationships, policy development and creating conditions for success of the entire organization.
- **Division Office Focus:** Division Offices are focused on creating conditions for success that enable the achievement of missions within the RBC through the accomplishment of Command and Control, Regional Interface, Program Management, Quality Assurance and operational planning and management of the RBC.
- **Actualize the RBC:** The RBC is used to utilize regional resources and expertise effectively and efficiently through the concept of mutual interdependence.

H.9 Major Process Changes (Excerpts from 2012 Implementation Plan)

- **National and Regional Program Management:** Appropriations are managed at the national level and regions manage regional programs and funds.
- **Checkbook Funding:** Funding should be provided to enable offices to purchase necessary expertise and services when there is an insufficient requirement for a continuous level of effort or service.
- **Eliminate certification of DD1391:** The ASA-I&E direction to conduct planning charrettes for all Army MILCON projects included in the POM creates a redundant requirement for DD1391 certification. DD1391 certification can still be accomplished at the District level for those projects that have not been programmed based on a planning charrette.
- **Army MILCON Design Directives:** Regions will issue design directives on all Army MILCON projects.
- **Army MILCON Reprogramming:** Regions will request MILCON reprogramming authority and approval directly from OASCIM. Washington level HQs will be informed the action is occurring but will not be in the process flow.
- **Regions Manage Army MILCON Project Funds:** Regions will obtain project funds directly from HQs Washington level Directorate of Resource Management. This includes construction and Planning and Design (P&D) funds. Washington level HQs will manage at the appropriation level and the regions will manage at the project level. P&D funds will be allocated by Washington level HQs on a regional basis. The Regions will allocate and manage on a District basis.
- **Regional Support Centers:** Many of the support functions recommended the establishment of Regional Support Centers for their specific function. This concept has merit on a broad scale and Regions are encouraged to evaluate the concept for all Regional functions, support and mission. It appears that regional processes could be streamlined significantly in some functional areas.

- **Programmatically Fund the “Reconnaissance Phase” of the Civil Works Planning Process:** Establish reconnaissance studies similar to the current Continuing Authorities Program. Congressional action will be required.
- **Provide 100 Percent Federal Funding for the Feasibility Phase of Project Implementation:** Seek Congressional Modification of WRDA 86 to remove the feasibility study cost sharing requirement.
- **Build and Defend the Civil Works Program around Business Lines:** In FY 05, the Corps of Engineers is developing its budget based on the nine water resources business lines. This initiative should be continued.
- **Reconstitute Project Cooperation Agreements (PCAs) as Partnering Agreements executed at the District Level:** This would eliminate months, if not years, from the civil works process and address the number one partner and customer complaint about our civil works process.
- **Actualize the Regional Business Center:** Focus Washington Headquarters and Division Offices on their appropriate missions and align resources to truly actualize Regional Business Centers.

H.10 Organizational Design Concepts (Excerpts from 2012 Implementation Plan)

Regional Business Center (RBC): The Corps is moving toward the RBC objective state defined in the *RBC 2012 Concept Paper*, March 24, 2003. The basic premise is that the Corps will operate more **interdependently** within each region. Each District will no longer need to perform every function; we will have technical centers; regional metrics; regional support functions that serve multiple districts; and one CEFMS database. For example, one CEFMS database for each Region is necessary to actualize the RBC, as it will allow direct charging to projects within a Region, streamline internal funds management processes and promote collaboration. As we define what we do within each functional area, it is essential we recognize our evolving "doctrine" particularly as defined in the role of the RBC. Both Washington headquarters and MSC headquarters processes must be designed to maximize support of District tactical level work, while efficiently leveraging all available resources of the Corps.

Regional Support Teams: Significant cultural changes and minor structural changes are necessary to break the existing three-echelon and competing-stovepipe paradigms necessary to operate as One Corps and One Headquarters. Cultural changes will take place over time as we stop competing internally between programs and begin to behave as **“One agile team, capable of operating virtually as a learning organization.”** The structural change that will support the cultural change is the creation of Regional Support Teams (RSTs), which will link the Washington and Regional Headquarters into one and create synergy among all programs. RSTs will be focused on the execution of programs for major Corps mission areas including Civil Works, Military Construction, Installation/Interagency/International Support, Environmental, Real Estate and Research and Development. The teams will be assigned to the Washington level HQs

and will be duty stationed in Washington but they will represent the voice, concern and conscience of the Regions. They will be empowered to work issues with any level of the USACE organization necessary to resolve the issue in an expeditious and timely manner.

Support Functions: In the context of Executive Direction and Management (ED&M), "mission" equates to direct program oversight, and "support" is the indirect services that facilitate that program oversight. For purposes of this analysis, the General Expense (GE) & Operations and Maintenance (OMA) ED&M resources assigned to Military Programs, Civil Works, Real Estate and Research and Development are assumed to be direct "mission" assets. All other functions are defined as "support."

H.11 TWE Summary Backup Notes

H.11.1. Enterprise (Corporate-level) Program Asset Management

Summary Discussion: Business practices in the TWE associated with *Enterprise Program Asset Management* will require IT investments that improve analytical modeling capabilities, and improve collaboration and communications between USACE and other Federal agencies.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference Civil Works Strategic Plan

1.1.1. Invest in navigation infrastructure when the benefits exceed the costs.

Flood and Coastal Storm Damage Reduction

1.1.2. Invest in flood and coastal storm damage reduction solutions when the benefits exceed the costs.

Hydropower

1.1.3. Invest in hydropower rehabilitation projects when the benefits exceed the costs.

CW Strategic Plan Strategies

- Improve planning processes through Planning Centers of Expertise and enhanced training and development of planners in the Corps, especially in the area of *analytic models*.
- Seek ways to better align and *integrate ongoing water management activities* managed by the Corps.
- Improve the Corps systems-oriented engineering and economic evaluation methodologies. Use and *develop state-of-the-art models*, including economic models, in conducting our analyses and evaluations.
- Increase interagency coordination of system modeling capabilities.

H.11.2. Regional Watershed and Installation Management

Summary Discussion: Business practices in the TWE associated with *Regional Watershed and Installation Management* will require IT investments that improve application interoperability, data sharing, collaboration and communications between USACE and other Federal, state, local and tribal organizations, as well as trusted partners such as universities and private industry.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases

- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

USACE Integrated Strategic Plan

Strategies to Achieve Objective 1.2.

Work with others (tribes, Federal agencies, State and local entities, non-governmental organizations, and regional watershed commissions) in developing integrated water resources solutions at a watershed scale, drawing upon the examples of Coastal America and American Heritage Rivers for success criteria.

- a. There are real water resources challenges facing our Nation, and these challenges must be met – otherwise our Nation’s economic prosperity, environment, security, and quality of life will suffer. To practice the principles of sustainable development, we must approach problems in an **integrated, holistic** fashion – preferably on a watershed scale. We know that this planning must accommodate significant uncertainties and allow for adjustments to future changes in the natural and social environments. **(USACE Integrated Strategic Plan, p. 4)**

Reference CW Strategic Plan:

Strategic Goal 1: Provide sustainable development and *integrated management of the Nation’s water resources*.

1.2.1. As approved and funded, provide a range of assistance to support sustainable regional, basinwide, or watershed planning and activities in partnership with others.

H.11.3. Protection of USACE Critical Infrastructure

Summary Discussion: Business practices in the TWE associated with *Protection of USACE Critical Infrastructure* will require IT investments that improve USACE current capabilities for Federal-level data sharing, detection, warning, and alert systems and analysis of potential terrorist attacks.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference USACE Integrated Strategic Plan: The Corps Emergency Management Program must be ready to prevent all types of hazards and support the Department of Homeland Security. Countering terrorism is a national priority. Terrorism threatens national security through contamination of, or disruption to, infrastructure, such as major water conveyance structures (aqueducts, tunnels, pipelines). Target threat areas include nuclear and radiological facilities, toxic chemicals and explosive materials facilities, transportation systems (navigable waterways and ports), and fixed infrastructure. Since 9/11, the Nation has maintained a heightened state of readiness to protect critical infrastructure. Concerns for water resources infrastructure focus on several things: dam failure causing massive flooding downstream; biological or chemical contamination – especially of water supplies -- and attacks on navigation facilities and hydropower plants. Implications for water resources development include:

- Resources will be diverted from domestic programs to homeland security and defense.
- There is a need to secure critical infrastructure, such as dams, hydropower plants, and reservoirs to protect vital resources for national security and to keep the domestic engine primed and pumping. Increased attention to planning is required to protect water supply systems, including treatment, pumping, and storage facilities.

- Better detection, warning, and alert systems for a terrorist attack are required.
- Water resources project designs must take security considerations into account.
- Planning must be done to assess system vulnerabilities.
- There is a need for centralized catastrophic disaster response coordination at the Federal level.
- Better coordination among the public health and disaster medical systems will be required.
- Need to improve core capabilities of some states and localities to respond to a massive disaster.
- Need improved detection and treatment for chemical and biological agents. Readiness programs must incorporate biological and chemical attack scenarios to a greater degree, especially in large metropolitan areas.
- Improved intelligence gathering and analysis from both domestic and international sources will be needed.
- Changes in emergency management systems and personnel training should be made.

The United States Army Corps of Engineers serves the Army and the Nation at home and abroad by providing vital public engineering services and capabilities across a full spectrum of operations in peace and war in support of national and global interests. Using the Army's command and control structure, we can quickly mobilize a trained force of engineering program managers and problem solvers into a seamless military-civil team to deliver critical infrastructure, engineering-related technical assistance, and coalition-building expertise worldwide. This integrated military-civil blend of expertise provides a flexible instrument for problem solving and the design and implementation of engineering solutions. As such, our expertise contributes to the economic development, security, and revitalization of the U.S. and the nations we support. The robust capabilities of the Corps thus provide an instrument of national policy to preserve and extend peace globally in support of the National Security Strategy.

- a. We help shape the security environment through our many missions across the globe in the infrastructure assistance and development, oriented towards both military facilities and civilian needs such as water, power, and roads. **(USACE Integrated Strategic Plan, p. 3, Footnote 1).**
- b. Known and prospective developments in Army and DoD infrastructure needs also present challenges beyond the capabilities of a single agency. **(USACE Strategic Plan, p. 5).**
- c. Thus, we anticipate the possibility of changes to our assigned mission areas in the years ahead. Some of these potential changes are:
 - (1) Engineering services relating to infrastructure evaluation, recovery, reconstruction, and development in a variety of global regions.

- (2) Technical engineering services relating to critical infrastructure protection within the United States. **(USACE Strategic Plan, p 6)**

H.11.4. Integrated Emergency Management

Summary Discussion: Business practices in the TWE associated with *Integrated Emergency Management* will require IT investments to improve GISs, cross-agency data sharing/application interoperability, mobile communications, tele-engineering, intra-agency modeling, response simulations and other information especially related to watersheds.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference USACE Integrated Strategic Plan: The Corps might work with FEMA on its *map modernization program*.

Goal 4: Reduce vulnerabilities and losses to the Nation and the Army from natural and man-made disasters, including terrorism.

The Corps will provide timely, effective, and efficient disaster preparedness, response, recovery, and mitigation services in flood fighting and through our support of the FEMA and Department of Homeland Security.

Strategies to Achieve Objective 1.2.

Enhance collaborative working relationships with the Environmental Protection Agency, the U.S. Fish and Wildlife Service, the Natural Resources Conservation Service, the U.S. Geological Survey, the FEMA, and others *to share data, models, methods, and other information, especially related to watersheds.*

Goal 4: Reduce vulnerabilities and losses to the Nation and the Army from natural and man-made disasters, including terrorism.

The purpose of this goal is to manage the risks associated with all types of hazards and to increase the responsiveness of the Civil Works Emergency Management Program within the Corps Office of Homeland Security to respond to disasters in support of Federal, State, and local emergency management efforts. Emergency readiness contributes to national security. We have established two objectives to promote effective readiness, response, and recovery.

Seek partnership opportunities with the FEMA to align their mitigation and recovery efforts with the Corps'.

The Stafford Act authorized the Corps to support the FEMA in carrying out the Federal Response Plan, which requires 26 Federal departments and agencies to provide coordinated disaster relief and recovery operations.

Ref CW Strat Plan:

STRATEGIC GOAL 4. Reduce vulnerabilities and losses to the nation and the Army from natural and man-made disasters, including terrorism.

Goal 4. Reduce vulnerabilities and losses to the Nation and the Army from natural and man-made disasters, including terrorism. The purpose of this goal is to manage the risks associated with all types of hazards and to increase the responsiveness of the Civil Works Emergency Management Program within the Corps Office of Homeland Security to respond to disasters in support of Federal, State, and local emergency management efforts. Emergency readiness contributes to national security. We have established two objectives to promote effective readiness, response, and recovery.

Emergency Management Program

- 4.1.1. Attain and maintain a high, consistent state of preparedness.
- 4.1.2. Provide a rapid, effective, efficient all-hazards response.
- 4.1.3. Ensure effective and efficient long-term recovery operations.

Planning Response Team Readiness Index.

PL84-99 Response Team Readiness Index.

Percent of scheduled inspections performed for all non-Federal Flood Control Works in RIP, as required by ER 500-1-1.

Percent of time solutions are developed and implemented (either repaired to pre-flood conditions or possible non-structural alternative) prior to the next flood season.

Percentage of Federal and non-Federal flood control works in Rehabilitation and Inspection Program with a satisfactory condition rating.

Strategies to Achieve Objective 4.1.

- Continue to serve as the lead agency in public engineering in support of the Federal Response Plan.
- Work with the Department of Homeland Security in defining the Corps role with respect to homeland security and defense within the context of an all-hazards Federal Response Plan.
- Promote research and development work units to improve flood damage reduction and disaster recovery plans, processes, and operations, e.g., levee inspection and Advanced Measures programs, and readiness training.
- Improve simulations of our response to disaster scenarios to ensure optimum readiness planning.
- Seek partnership opportunities with the FEMA to align their mitigation and recovery efforts with the Corps.
- Continue to work with stakeholders and State and local emergency management agencies to improve emergency response planning.

H.11.5. Enhanced Communications and Information Access Throughout USACE

Summary Discussion: Business practices in the TWE associated with *Enhanced Communications and Information Access Throughout USACE* will require IT investments that improve enterprise-level interoperability among USACE automated information systems, data warehousing, data transport, collaborative tools, security, and decision support tools.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans

- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference USACE Integrated Strategic Plan:

Objective 5.3. Become a more efficient and effective organization through technology.

Strategies to Achieve Objective 5.3.

- Develop a world-class enterprise-wide IT environment through improved information connectivity within the Corps and with the public, respecting the need to assure information security.
- Ensure that Information Technology systems meet IT security objectives.
- Reduce reporting burdens, streamline business transactions and make decision making more transparent through Web-based electronic mechanisms that promote information access and sharing.

Reference CW Strat Plan:

Goal 5. Be a world-class public engineering organization. Goal 5 is focused on ensuring that the Civil Works mission is performed in a technically skilled manner so as to build respect and confidence in the products and services the Corps delivers today and into the future. Building trust will come from the integrity of our engineering and scientific evaluations and recommendations, the soundness of our management decisions, the transparency of our decision-making process, the reliability and effectiveness of our business processes, and the contributions we make to the state of the art within and across our core technical disciplines. To achieve Goal 5, we must pay attention to people, processes, fiscal responsibility, efficiencies, and technology. The President's Management Agenda helps us focus on major organizational effectiveness aspects central to being a world-class organization: human talent, financial integrity, sound business practices, and the advantages that technology offers, especially to bring government closer to citizens. We have set three objectives to move toward Goal 5. We will draw upon the ongoing plans we have drafted in support of the President's Management Initiatives to make headway toward these objectives.

Percent of personnel that have completed security training.

Percent of sites passing security inspection.

H.11.6. Enhanced Management of Business Processes (Example: Online Applications)

Summary Discussion: Business practices in the TWE associated with *Enhanced Management of Business Processes* will require IT investments that improve automated information system component-level interoperability for internal and external users (examples include single sign-on or online applications).

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference USACE Integrated Strategic Plan:

Goal 5 is focused on ensuring that the Civil Works mission is performed in a technically skilled manner so as to build respect and confidence in the products and services the Corps delivers today and into the future. Building trust will come from the integrity of our engineering and scientific evaluations and recommendations, the soundness of our management decisions, the transparency of our decision-making process, the reliability and effectiveness of our business processes, and the contributions we make to the *state of the art within and across our core technical disciplines*.

Strategies to Achieve Objective 5.2.

- Improve business processes and automated information systems to improve our financial management.

- a. As a largely reimbursable agency, we must continue to embrace up-to-date, businesslike practices in all our customer relations to include matching our capabilities to the needs of customers, in timing, in required services, and in desired degree of participation. **(USACE Strategic Plan, p.5)**
- b. By the same token, we will continuously improve project management and other business processes (PMBP) and how we work throughout all of our mission areas.

H.11.7. Enterprise Management of Manpower Resources

Summary Discussion: Business practices in the TWE associated with *Enterprise Management of Manpower Resources* will require IT investments that ensure state of the art science and engineering automated tools, standard practices and treatment of data as a corporate asset (data warehousing) in support to virtual teaming.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference USACE Integrated Strategic Plan:

“Integrated water resources management is a process that promotes the coordinated development and management of water, land and related resources in order to maximize the resultant economic and social welfare in an equitable manner without compromising the sustainability of vital ecosystems.”

Ref CW Stat Plan

Be a world-class public engineering organization. Goal 5 is focused on ensuring that the Civil Works mission is performed in a technically skilled manner so as to build respect and confidence in the products and services the Corps delivers today and into the future. Building trust will come from the integrity of our engineering and scientific evaluations and recommendations, the soundness of our management decisions, the transparency of our decision-making process, the reliability and effectiveness of our business processes, and the contributions we make to the state of the art within and across our core technical disciplines. To achieve Goal 5, we must pay attention to people, processes, fiscal responsibility, efficiencies, and technology. The President's Management Agenda helps us focus on major organizational effectiveness aspects central to being a world-class organization: human talent, financial integrity, sound business practices, and the advantages that technology offers, especially to bring government closer to citizens. We have set three objectives to move toward Goal 5. We will draw upon the ongoing plans we have drafted in support of the President's Management Initiatives to make headway toward these objectives.

Percent of personnel that have completed security training.
Percent of sites passing security inspection.

Objective 5.1. Be a world-class technical leader.

5.1.1. Develop a Human Capital Strategy* to recruit, maintain, and enhance technical capability in core competencies.

5.1.2. Competitive Sourcing* -- Accomplish inherently nongovernmental work through others in support of mission accomplishment.

5.1.3. Support for Others: Provide public works engineering and construction management services that meet the customer's expectations.

Office of Personnel Management in rating scorecard for the President's Management Initiatives.

Competitive sourcing guidelines established by the Office of Management and Budget.

Score/rating from surveys of customer satisfaction with the quality, cost, and timeliness of public engineering and construction management services provided by the Corps.

Strategies to Achieve Objective 5.1.

Our strategies focus on recruitment, retention, fiscal responsibility and accountability, business process improvements, innovation, and outreach. Providing quality and responsive engineering and scientific services to the Nation and others requires a solid technical foundation. Toward *preserving our technical edge*, we will do the following:

- Develop a Strategic Management of Human Capital Plan for USACE that addresses OPM's Human Capital Accountability and Assessment Framework within the context of corporate planning, competitive sourcing, and technology initiatives.
- Improve recruiting policies and procedures targeted to critical skill areas.
- Implement a Planning Excellence Program to enhance our planning capability and economic evaluations.
- Establish national and regional Planning Centers of Expertise.
- Heed the National Academy of Sciences recommendation to institute independent review on large or controversial projects.
- Support competitive sourcing initiatives proposed by the Administration in concert with the mandates of the Federal Activities Inventory Reform (FAIR) Act of 1998.
- Partner with the Department of Army to streamline and standardize the employment application process for individuals seeking employment with the Corps.
- Improve leadership training and doctrine.
- Preserve our world-class capabilities through a robust Research and Development program, in part oriented to development and application of holistic systems frameworks and watershed models and technologies.
- Improve our technology transfer to promulgate our skills and knowledge more widely.
- Share our knowledge and expertise with others through an active Support for Others Program.
- Improve technology implementation through a Strategy for Management of Science and Engineering Technology (SET).

H.11.8. Enterprise and Regional Acquisition Strategy

Summary Discussion: Business practices in the TWE associated with *Enterprise and Regional Acquisition Strategies* will require IT investments to maintain and improve regional acquisition-related automated information systems.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents

- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture
- PARC Web Page

Reference USACE Integrated Strategic Plan:

There is no official list of the most important environmental challenges facing the country and not enough money to address all of the environmental issues. We know that we need to prioritize. But we can also begin to work with others at the State and local level, as well as with non-governmental organizations, to establish priorities for environmental investments. The best solutions will be those adopted through partnerships to address regional requirements and characteristics.

Streamline Businesses Processes – Especially the Regulatory Process. People want to see the regulatory permitting timeline shortened (especially for Clean Water Act, Section 404 permits) and simplified, a tracking system implemented, and permit decisions tailored to regional challenges. They would like to achieve a better balance between commercial/industrial beneficiaries and community and environmental beneficiaries.

Ref PARC Web Page: *Regional acquisitions will require improvements to acquisition-specific automated information systems.*

H.11.9. Enterprise Management of Knowledge That Includes Best Practices, Registry of Skills, Customer Feedback, Lessons Learned, Corporate Issues Management, etc.

Summary Discussion: Business practices in the TWE associated with Enterprise Management of Knowledge That Includes Best Practices, Registry of Skills, Customer Feedback, Lessons Learned, Corporate Issues Management, etc., will require IT investments that consolidate current USACE systems and system components providing similar services.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture
- PARC Web Page

Reference USACE Integrated Strategic Plan:

Our strength is our public engineering technical expertise in planning, design, construction, engineering management, and project management. This expertise is grounded in solid scientific and interdisciplinary skills and knowledge, as enhanced by demonstrated competence in contract management, contingency and disaster response, real estate services, collaborative processes, and research and development.

Collaborative Approach. Clearly, collaboration is essential to bring together the expertise on natural and human systems over the appropriate geographic area, knowledge of problems that exist, and the range of current and potential uses for water resources. Collaboration can involve several Federal agencies (e.g., Environmental Protection Agency, U.S. Fish and Wildlife Service, Natural Resources Conservation Service, Bureau of Reclamation, U.S. Geological Survey, and land management agencies), State and local agencies, the private sector, and interest groups and can take many forms. Each participating entity will bring its own legal authorities, skills and knowledge, history, and contributions to funding.

Our ability to integrate a wide ranging interdisciplinary capability into a full spectrum engineering capability and our geographic dispersion uniquely enable the Army Corps of Engineers to meet national water resources requirements.

The Corps intends to work within the Administration and with Congress to promote policies and legislation that will be more consistent with the strategic direction presented here. We want to build on our areas of strength and improve our reputation in areas in which we have received criticism. We want to be a world-class public engineering organization – knowledgeable on the latest technologies, capable in the latest skills, trusted as an honest broker and helpful collaborator who provides transparent analyses, a wise investor of taxpayer funds, and an organization that delivers projects on time and within budgets.

Customer satisfaction. Support for Others: Provide public works engineering and construction management services that meet the customer’s expectations. Score/rating from surveys of customer satisfaction with the quality, cost, and timeliness of public engineering and construction management services provided by the Corps.

- Intermittently during the year, issues are raised and discussed at Issues Management Board meetings; this Board is made up of all senior military and civilian leaders at Corps headquarters.
 - a. Known and prospective developments in Army and DoD infrastructure needs also present challenges beyond the capabilities of a single agency. Working closely with our customers, and in alliance with the other stakeholders, we will collaborate in seeking and finding innovative answers to those challenges, mutually leveraging our respective strengths. **(USACE Strategic Plan, p. 5)**
 - b. ...we, like other Federal agencies, must engage in continual improvement and adjustment to changes in the larger world. Adopting the phrase popularized by Peter Senge, we must transform ourselves into a “Learning Organization,” one that is adaptive, flexible, and responsive. (USACE Strategic Plan, p.5)

H.11.10. Enterprise Processes to Manage Technology and Data

Summary Discussion: Business practices in the TWE associated with *Enterprise Processes to Manage Technology and Data* will require IT investments in the IT infrastructure to bring it up to state-of-the-art support capabilities, and implement a clear path to data warehousing corporate data.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan

- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference USACE Integrated Strategic Plan:

3) Bring government closer to citizens through responsive technology;

Civil Works Strategic Plan OBJECTIVE 5.3. Become a more efficient and effective organization through technology (e-government*).

Goal 5 - Be a world-class public engineering organization. Goal 5 is focused on ensuring that the Civil Works mission is performed in a technically skilled manner so as to build respect and confidence in the products and services the Corps delivers today and into the future. Building trust will come from the integrity of our engineering and scientific evaluations and recommendations, the soundness of our management decisions, the transparency of our decision-making process, the reliability and effectiveness of our business processes, and the contributions we make to the state of the art within and across our core technical disciplines. To achieve Goal 5, we must pay attention to people, processes, fiscal responsibility, efficiencies, and technology.

Be a world-class technical leader.

Strategies to Achieve Objective 5.1. Our strategies focus on recruitment, retention, fiscal responsibility and accountability, business process improvements, innovation, and outreach. Providing quality and responsive engineering and scientific services to the Nation and others requires a solid technical foundation. Toward preserving our technical edge, we will do the following:

- Develop a Strategic Management of Human Capital Plan for USACE that addresses OPM's Human Capital Accountability and Assessment Framework within the context of corporate planning, competitive sourcing, and technology initiatives.

- Improve our technology transfer to promulgate our skills and knowledge more widely.
- Share our knowledge and expertise with others through an active Support for Others Program.
- Improve technology implementation through a Strategy for Management of Science and Engineering Technology (SET).

Objective 5.3. Become a more efficient and effective organization through technology. Strategies to Achieve Objective 5.3.

- Develop a world-class enterprise-wide IT environment through improved information connectivity within the Corps and with the public, respecting the need to assure information security.
- Ensure that IT systems meet IT security objectives.
- Reduce reporting burdens, streamline business transactions and make decision making more transparent through Web-based electronic mechanisms that promote information access and sharing.
- Improve government-to-citizen services by leveraging technology and e-government (e-Gov) initiatives.
- Focus IT spending on high-priority modernization initiatives using a modernization blueprint for Enterprise Architecture.
 - a. We do not know the exact nature of the missions that will be assigned to us in the future, but based on experiences extending over many decades (up to and including current events), it is prudent to anticipate that they will run a large gamut of public engineering services. Thus, as an agency, we believe it incumbent upon us to maintain the technical edge to be a world-class public engineering organization throughout multiple disciplines. In addition to engineering specialties, this also includes high-level expertise in fields ranging from the natural sciences to real estate acquisition, financial management, environmental law, and Federal procurement. These in-house technical capabilities will be complemented by the ability to effectively contract for and manage additional capabilities resident in the private sector.
(USACE Integrated Strategic Plan, p.5)

Ref CW Strat Plan:

Objective 5.3. Become a more efficient and effective organization through technology.

5.3.1. Ensure that the Civil Works mission is supported by an information architecture and capital investments in technology aimed at increasing work efficiencies and effectiveness.*

5.3.2. Develop and use electronic means and media to provide timely and easily accessible information about engineering and related services to customers, the public, and other interested parties.*

Standards set by Clinger-Cohen Act and other relevant laws that apply to the Chief Financial Information Officer in the Corps.

Standards set by the Office of Management and Budget.

Commence at least one IT initiative that affects approximately 4,500 citizens per day.

Strategies to Achieve Objective 5.3.

- Develop a world-class enterprise-wide IT environment through improved information connectivity within the Corps and with the public, respecting the need to assure information security.
- Ensure that IT systems meet IT security objectives.
- Reduce reporting burdens, streamline business transactions and make decision making more transparent through Web-based electronic mechanisms that promote information access and sharing.
- Improve government-to-citizen services by leveraging technology and e-government (e-Gov) initiatives.
- Focus IT spending on high-priority modernization initiatives using a modernization blueprint for Enterprise Architecture.

Examples of How the Corps is Improving Government-to-Citizen Services

- The Corps' Navigation Data Center provides the Operations and Maintenance Business Information Link (OMBIL), an electronic system that links and standardizes operational data regarding navigation, flood protection, hydropower, environmental stewardship, recreation, and regulatory issues.
- The Corps' Emergency Management Program operates ENGLink, a GIS-based interactive system for emergency communications, command, and control that enables rapid access to maps and data regarding both baseline information and specific disaster events.
- We have integrated regulatory permits, outgrants, and other types of authorizations and licenses for ease of public access and completion.
- The Corps' Internet-based National Recreation Reservation Service serves as the one-stop recreation reservation system for the public for more than 145,000 recreation sites at over 1700 Federal lakes and parks, including National Parks and other public lands.
- Within the Regional Sediment Demonstration Program, a regional geospatial information system (GIS) is being developed to provide baseline data and historical data sets to facilitate regional sediment management decisions in the Alabama-Mississippi region.

- The Corps' Natural Resources Management Gateway provides a one-stop on-line entry point to a wealth of natural resources information for the general public.
- The Corps is taking the lead in partnership with the Coast Guard, the National Oceanic and Atmospheric Agency, and the River Boat Pilot Association under the Inland Electronic Navigation Chart Program to provide a geospatial one-stop source for marine transportation information consisting of maps of navigation channels and automated information systems related to shoreline and inland navigation.
- The CorpsMap Program will provide one geospatial interface for all nation-level databases, thus allowing any Federal agency to incorporate Corps data.

5.3.1. Ensure that the Civil Works mission is supported by an information architecture and capital investments in technology aimed at increasing work efficiencies and effectiveness.*

5.3.2. Develop and use electronic means and media to provide timely and easily accessible information about engineering and related services to customers, the public, and other interested parties.*

H.11.11. Methods for Data Exchange with Government and Industry Partners

Summary Discussion: Business practices in the TWE associated with *Methods for Data Exchange with Government and Industry Partners* will require IT investments that improve data collection, analysis and dissemination for internal and external information users.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations

- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference USACE Integrated Strategic Plan:

Improve Data Collection, Analysis, and Dissemination. We heard a lot about the need to share data across Federal agencies and with others outside government. Lack of coordination and communication leads to needless duplication of data collection efforts and studies or significant voids, thus limiting the potential for developing solutions to complex problems. Some people would like to see a one-stop data clearinghouse to make water resources data universally available to communities of interest for enhanced coordination, planning, and project development. This would support national assessments and the formulation of regional and watershed plans. In addition, people noted that many agencies are not applying the most advanced technologies and models available. But where the government excels, as in the use of geographic information systems (GIS) technology or modeling, such technology should be more readily available to the general public. Many cited a need to update floodplain studies and maps, taking into account potential dam failures.

H.11.12. Internal and External Virtual Teaming

Summary Discussion: Business practices in the TWE associated with *Internal and External Virtual Teaming* will require IT investments that promote standard science and engineering tools and processes for internal and external team members to support virtual project management.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP

- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference USACE Integrated Strategic Plan:

Enhance collaborative working relationships with the Environmental Protection Agency, the U.S. Fish and Wildlife Service, the Natural Resources Conservation Service, the U.S. Geological Survey, the FEMA, and others to share data, models, methods, and other information, especially related to watersheds.

Trained regional planning and response teams, ready cadres, and in-place contracts, systems, equipment, and facilities provide a level of readiness that reduces risks and raises confidence that help is on the way.

Coastal America provides a model of Federal cooperation among Federal, State, local, and non-governmental entities who have joined forces to search for program and funding linkages around a common goal – improving America’s coasts – in an attempt to counter the piecemeal approach of the past and to leverage existing limited funds so as to stretch the Federal dollar. Organizationally, there are a number of groups that coordinate at different levels: a Principals group of Under or Assistant Secretaries from partner Federal agencies; a National Implementation Team of senior managers from these agencies; a Coastal America office that serves as a hub for national products, multiregional projects, education, and training; nine Regional Implementation Teams; and local Project Teams – all supported by hundreds of non-governmental organizations and thousands of volunteers.

Civil Works Strategic Plan

Establishing interdisciplinary teams.

- a. Known and prospective developments in Army and DoD infrastructure needs also present challenges beyond the capabilities of a single agency. Working closely with our customers, and in alliance with the other stakeholders, we will collaborate in seeking and finding innovative answers to those challenges, mutually leveraging our respective strengths. **(USACE Integrated Strategic Plan)**

H.11.13. One Stop Web Access to USACE Public Information

Summary Discussion: Business practices in the TWE associated with *One Stop Web Access to Public Information* will require IT investments that reduce reporting burdens, streamline business transactions and make decision making more transparent through a significant increase in Web-based electronic mechanism.

References:

- USACE Integrated Strategic Plan
- CW Strategic Plan
- MP Strategic Plan
- RD Strategic Plan
- RE Strategic Plan
- HR Modernization Planning Documents
- 2012 Implementation Plan
- CEEIS Modernization Planning
- IRM Strategic Plan
- 8 OMB Business Cases
- Regional Campaign Plans
- Competitive Sourcing PMP
- CPIC AIS Presentations
- e-Gov Initiatives/USACE e-Gov Reviews
- e-Corps PMP
- DoD Joint Technical Architecture

Reference USACE Integrated Strategic Plan:

Reduce reporting burdens, streamline business transactions and make decision making more transparent through Web-based electronic mechanisms that promote information access and sharing.

Primary Business Function	Initiative	Source Document	Source Document Section	As-Is	To-Be
Programs	Program Management (PMBP)	USACE Campaign Plan	Process, Strategy 1.2 & 1.3	by Project (PROMISE)	by Enterprise (P2 and Regional Management Board)
		MP 2012, May 2003	Goal 6		
		CERE 2012, April 2003	Process, Objectives 1.1, 1.2, 4.1, 3.2-5 Communication Objective 2.2		
	Business Information	USACE Campaign Plan	Process, Strategy 2.3	by Enterprise (OMBIL-+)	by Enterprise (OMBIL-+)
		USACE Campaign Plan	Process, Strategy 2.3	by functional area (FEM, NID, REMIS, etc.)	Enterprise Asset Management
	Inventory	USACE Campaign Plan	Process, Strategy 3.1	by project	managed Watershed Solutions (Regional Watershed Planning Tool)
		CW Strategic Plan FY 2004-2009 <i>(note: plan details As-Is and To-Be as well as implementation strategy)</i>	Strategic Goal 1-3, Section 4 (Goals and Objectives), Section 5 (Implementation & Evaluation)		
	Watershed	USACE Campaign Plan	Process, Strategy 3.3	limited support by project	regional, holistic assessments leading to projects
		USACE Campaign Plan MP 2012, May 2003	Goal 3		
	Environmental Support for Military Installations	USACE Campaign Plan	Strategic Goal 4, Section 4 (Goals and Objectives), Section 5 (Implementation & Evaluation)	by project	1) Integrated life-cycle management of emergency management programs 2) Provide critical infrastructure protection for Civil Works facilities and seamless infrastructure protection within the Corps
		CW Strategic Plan FY 2004-2009 <i>(note: plan details As-Is and To-Be as well as implementation strategy)</i>	Communications, Strategy 4.2	ad hoc issues identification & Resolution	Corporate Issues Management Process
	Corporate Issues Management Process	USACE Campaign Plan	Communications, Strategy 3.1 & 3.2	Ad hoc Communications	Enterprise-wide Communications Process
USACE Campaign Plan		Process, Objective 1.5, 2, 4.2, 4.4, 4.5 Communication Objective 2			
Improve Communications with External Partners, stakeholders, & Customers	USACE Campaign Plan	Process, Strategy 3.2	Duplicate Permit & Mitigation Requirements imposed on non-Federal O&M Sponsors	eliminate duplicate permit and mitigation requirements imposed on non-federal O&M Sponsors; increase using Special Area Management Plans	
	CERE 2012, April 2003				
Regulatory Process (simpler, transparent, consistent)	USACE Campaign Plan				

Primary Business Function	Initiative	Source Document	Source Document Section	As-Is	To-Be
Information Technology	IT Infrastructure	CERE 2012, April 2003 IRM Strategic Plan FY 2003-2008	Process Objective 1.6 Goal 1	by Enterprise (CEEIS)	by Enterprise (CEEIS), enhanced network management, Common Operating Environment, optimized application and web servers Enterprise wide exchange
	Email			Enterprise wide exchange	
Legal Services & Internal Review Resource Management	Technology Insertion	IRM Strategic Plan FY 2003-2008	Goal 2	by business line, multiple legacy systems needing conversion	by Enterprise and with regional collaboration
	Information Assurance	IRM Strategic Plan FY 2003-2008	Goal 3	by business line	Enterprise-wide
	IT Investment Portfolio Management	IRM Strategic Plan FY 2003-2008	Goal 4	by project and business line	linked to Enterprise Mission and business processes
	E-Government	IRM Strategic Plan FY 2003-2008	Goal 5	by project and business line, Limited web-based Information Access	Enterprise-wide
	Financial Budgeting	USACE Campaign Plan		by business line	by Enterprise (P2)
	Manpower	USACE Campaign Plan		by business line	by Enterprise (P2 & Regional Business Centers)
Other Acquisition Management	Streamline Acquisition Process	USACE Campaign Plan MP 2012, May 2003	Process, Strategy 1.1 Goal 6, Objective 2	Programatic planning by project, Web-based database of contract vehicles	1) corporate & regional acquisition approaches; Enterprise-Level Systems augmenting Standard Procurement System (SPS) 2) Incorporate Best Acquisition
	Skills Registry	USACE Campaign Plan MP 2012, May 2003	People, Measurement Objective 1 Goals 4 & 5	Programatic planning by project within civil or military programs	Enterprise-wide skills planning 1) Integrate Civil and Military Programs into Divisional Programs 2) Implement CBR protection technologies 3) Integrate Registry of Skills with Knowledge management systems by program, accessible enterprise-wide 1) Incorporate "Best Customer Feedback Practices" into USACE PMPB toolkit
Logistics Management Human Resources Management	Lessons Learned	USACE Campaign Plan MP 2012, May 2003	People, Strategy 2.1 Goal 6	by project	
	Career-Long Learning	CERE 2012, April 2003 USACE Campaign Plan	Communication 4.5 People, Strategy 2.2	by project, inconsistent	by program, consistent enterprise-

Appendix I – Performance Metrics



Goals and Objectives	Program Objectives	Performance Measures	Strategies
<p>STRATEGIC GOAL 1. Support sustainable development through integrated water resources development and management.</p> <p>Hydropower Objective Future: Invest in environmentally sustainable hydropower infrastructure improvements where economically justified.</p> <p>OBJECTIVE 1.2. Support the formulation of regional and watershed solutions to water resources problems.</p> <p>1.2.1. As approved and funded, provide a range of assistance to support sustainable regional, basin-wide, or watershed planning and activities in partnership with others.</p> <p>Objective 1.3. Reduce the backlog of ongoing, budgeted construction projects.</p> <p>The balance to complete for all projects in construction – known as the “Construction Backlog” – was around \$21 billion in Fiscal Year 2003. Our intent is to deliver project benefits as quickly as possible within available resources or to de-authorize projects that no longer show a positive benefit-to-cost ratio.</p> <p>1.3.1. Deliver project benefits as quickly as possible within available resources.</p> <p>1.3.2. De-authorize projects that no longer show a positive benefit-to-cost ratio.</p> <p>1.3.3. De-authorize projects that no longer have the active support of a local cost-share sponsor.</p> <p>STRATEGIC GOAL 2. Repair past environmental degradation and prevent future environmental losses.</p>	<p>Strategic Goal 1 Provide sustainable development and integrated management of the Nation's water resources.</p> <p>Objective 1.1. Seek water resources solutions that better balance economic, environmental, and quality of life objectives.</p> <p>Objective 1.2. Support the formulation of regional and watershed solutions to water resources problems.</p> <p>Objective 1.3. Reduce the backlog of uncompleted, scheduled work on ongoing, budgeted construction, General projects. The balance to complete for all projects in construction – known as the “Construction Backlog” – was around \$21 billion in Fiscal Year 2003. Our intent is to deliver project benefits as quickly as possible within available resources or to de-authorize projects that no longer show a positive benefit-to-cost ratio or the active support of a local cost-share sponsor.</p> <p>Goal 2 Repair past environmental degradation and prevent future environmental losses.</p>	<p>Navigation 1.1.1. Invest in navigation infrastructure when the benefits exceed the costs. Flood and Coastal Storm Damage Reduction 1.1.2. Invest in flood and coastal storm damage reduction solutions when the benefits exceed the costs. Hydropower 1.1.3. Invest in hydropower rehabilitation projects when the benefits exceed the costs.</p> <p>1.2.1. As approved and funded, provide a range of assistance to support sustainable regional, basin-wide, or watershed planning and activities in partnership with others.</p> <p>1.3.1. Deliver project benefits as quickly as possible within available resources. 1.3.2. De-authorize projects that no longer show a positive benefit-to-cost ratio. 1.3.3. De-authorize projects that no longer have the active support of a local cost-share sponsor.</p>	<p>Remaining BCR (project specific measure).</p> <p>The incorporation of watershed principles into the plan formulation process via guidance and training.</p> <p>Percent change in constant dollar balance to complete programmed work on all ongoing, budgetable construction projects.</p> <p>Strategies to Achieve Objective 1.1.</p> <ul style="list-style-type: none"> Continue to apply the 1983 Principles and Guidelines (P&G) for project development to meet economic standards and further develop mechanisms for evaluating environmental standards of the P&G. Review Corps authorities, policies, and processes to determine those that promote and inhibit integrated water resources management consistent with watershed principles and needs and recommend revisions to Corps authorities as needed. Build on current Corps authorities to promote sustainable development, as well as more integrated water resources management. Promulgate guidance that encourages the formulation of multi-objective economic and environmental projects when desired by non-Federal interests. Conduct outreach to other Federal agencies for collaborative watershed efforts. Improve planning processes through Planning Centers of Expertise and enhanced training and development of planners in the Corps, especially in the area of analytic models. Seek ways to better align and integrate ongoing water management activities managed by the Corps. Align (synchronize) the biannual Civil Works authorization process and annual appropriations process to foster greater integration across agencies. Improve the Corps systems-oriented engineering and economic evaluation methodologies. Use and develop state-of-the-art models. Increase interagency coordination of system modeling capabilities. Facilitate discussions across Federal agencies related to watershed-scale success criteria and performance measures. Seek independent review of large and controversial projects. Enhance the capability of the Corps to perform policy compliance reviews and manage an independent technical review process, e.g. <p>Strategies to Achieve Objective 1.2.</p> <ul style="list-style-type: none"> Work with others (tribes, Federal agencies, State and local entities, non-governmental organizations, and regional watershed commissions) in developing integrated water resources solutions at a watershed scale, drawing upon the examples of Coastal America and American Heritage Rivers for success criteria. Enhance collaborative working relationships with the Environmental Protection Agency, the U.S. Fish and Wildlife Service, the Natural Resources Conservation Service, the U.S. Geological Survey, the Federal Emergency Management Agency, and others to share data, models, methods, and other information, especially related to watersheds. Use budget-based performance measures to rate and rank projects within the Corps Major Subordinate Commands (Divisions), which are organized along watershed lines. Give preference to projects that are designed most effectively to achieve watershed goals. Support the planning of States, tribes, watershed coalitions, and regional planning commissions as appropriate and authorized. Use existing Corps authorities, processes, and tools to promote collaborative planning. Promulgate guidance that fosters watershed-scale planning and management. Optimize the Civil Works Research and Development Program to develop and use tools and processes that enhance watershed-scale <p>Strategies to Achieve Objective 1.3.</p> <ul style="list-style-type: none"> Use resources as efficiently as possible. Prioritize all projects in a business program based on performance. Do not budget for construction projects that lack a favorable benefit/cost ratio or that no longer have the support of local sponsors. Follow the formal process described in Section 1001 of the Water Resources and Development Act of 1986 (amended in 1996) to automatically de-authorize “inactive” projects that have not had funds obligated by Congress for their planning, design, or construction for a full 7 fiscal years plus a 30-month additional evaluation period.
<p>Objective 2.1. Restore degraded significant ecosystems structure, function, process to a more natural condition.</p> <p>The focus of this objective is environmental restoration where the environment has been harmed by development activities associated with Corps projects or by the development activities of others. The objective is to bring the affected resources back to a natural ecosystem functional state.</p> <p>Objective 2.2. Protect the Nation's wetlands to prevent degradation from future development.</p> <p>The focus of this objective is environmental protection. Prevention and protection are preferable to mitigation for environmental losses. Under Section 404 of the Clean Water Act the Corps has a Regulatory Program to protect wetlands threatened by private development by encouraging developers to avoid losses. When losses occur, developers mitigate for the losses.</p> <p>Objective 2.3. Assist in the clean-up of contaminated hazardous, toxic, and radioactive waste sites as authorized or requested by others.</p> <p>The focus of this objective is environmental remediation. The purpose is to repair contaminated land to a state that allows economic development activity to resume on that land. This objective typically does not involve restoring original natural ecological functions to the site.</p>	<p>Ecosystem Restoration 2.1.1. Invest in restoration projects or features that make a positive contribution to the Nation's environmental resources in a cost-effective manner.</p> <p>Regulatory Program 2.2.1. Administer the Regulatory Program in a manner that protects the aquatic environment (assures zero net-loss of wetlands). 2.2.2. Administer the Regulatory Program in a manner that enables efficient decision-making.</p> <p>Environment Program 2.3.1. Achieve the clean-up objectives of the Formerly Utilized Sites Remedial Action Program (FUSRAP). 2.3.2. Assist the Environmental Protection Agency in achieving the objectives of the Superfund Program.</p>	<p>Acres of habitat restoration completed. River miles of habitat restoration completed. Acres/river miles of nationally significant habitat restoration completed per dollar invested.</p> <p>Compliance inspection – percent completion rate for individual Permits (standard permits and letters of permission) each year. Compliance inspection – percent completion rate for General Permits with reporting requirements completed each year. Compliance inspection – percent completion rate for active permitted mitigation sites. Compliance inspection – percent completion rate for all active mitigation banks and in-lieu fee arrangements. Percent rate of resolution of outstanding un-authorized activities, which were unresolved at the end of prior FY. Percent of individual standards permits (excluding those with ESA consultations) issued in 120 days or less. Percent of General Permits issued in 60 days or less.</p> <p>Quantity of contaminated material remediated. Quantity of contaminated material remediated per dollar invested. Customer (Environmental Protection Agency) satisfaction with the quality and timeliness of the Corps cleanup efforts, i.e., they meet quality standards and schedules.</p>	<p>Strategies to Achieve Objective 2.1.</p> <ul style="list-style-type: none"> Strive to achieve zero net loss of wetlands. Fully utilize existing Corps ecosystem restoration authorities (e.g., the Continuing Authorities Program, Section 1135 of the Water Resources Development Act of 1986, Section 204 of the Water Resources Development Act of 1992, Section 206 of the Water Resources Development Act of 1996) to provide the highest environmental return on investment. Fully explore non-structural solutions. Identify programmatic impediments to doing restoration projects and propose modifications consistent with Administration policies and priorities. Foster partnerships with other Federal agencies, tribes, State and local governments, and non-governmental organizations to restore the environment. <p>Strategies to Achieve Objective 2.2.</p> <ul style="list-style-type: none"> Improve the Regulatory Program by establishing a process for consolidated regulatory permits review. Work with others to improve the ecological quality of new wetlands being created as replacements for wetlands destroyed by development. <p>Strategies to Achieve Objective 2.3.</p> <ul style="list-style-type: none"> Provide reliable, efficient, and effective support to assist Federal agencies, States, and others to accomplish their clean-up responsibilities. <p>Examples of Recent Partnership Agreements</p> <ol style="list-style-type: none"> EPA - In July 2002 the Acting Assistant Secretary of the Army for Civil Works signed a Memorandum of Understanding with the U.S. Environmental Protection Agency to restore and clean up urban rivers contaminated by sediment. Ducks Unlimited - The Corps has signed a Memorandum of Understanding with Ducks Unlimited to provide a foundation for collaboration related to the protection, restoration, and management of selected wetlands and associated uplands. The Nature Conservancy - In December 2000 the Corps signed a Memorandum of Understanding with The Nature Conservancy to facilitate effective and efficient management of important biological resources within the context of civil works activities; protect and restore fresh and marine habitats; advance our understanding of biological diversity in these habitats; promote non-structural and other measures to sustain ecosystem functions; encourage sustainable water management; provide for demonstration projects; monitor the rate of endangered species; and promote gathering and sharing of scientific information of mutual concern.

	Goals and Objectives	Program Objectives	Performance Measures	Strategies
<p>4.3.1. FUSRAP Objective. Achieve the cleanup objectives of the Formerly Utilized Sites Remedial Action Program (FUSRAP).</p> <p>4.3.2. Support for Others Objective. Assist the Environmental Protection Agency in achieving the objectives of the Superfund Program.</p> <p>STRATEGIC GOAL 3. Ensure that projects perform to meet authorized purposes and evolving conditions.</p> <p>Objective 3.1. Improve the efficiency and effectiveness of existing Corps water resources projects.</p> <p>3.1.3.2. Ensure that the operation of all Civil Works facilities and management of associated lands, including outgranted lands, complies with the environmental requirements of the relevant Federal, State, and local laws and regulations.</p> <p>3.1.3.3. Meet the mitigation requirements of authorizing legislation or applicable Corps decision document.</p> <p>Hydropower Objectives 3.1.4. Provide reliable power. 3.1.5. Provide peaking power. 3.1.6. Maintain capability to provide power efficiently.</p> <p>Recreation Objectives 3.1.7. Provide justified outdoor recreation opportunities in an effective and efficient manner at Corps-operated water resources projects. 3.1.8. Provide continued outdoor recreation opportunities to meet the needs of present and future generations. 3.1.9. Provide a safe and healthful outdoor recreation environment for Corps customers.</p> <p>Water Supply Objective 3.1.10. In partnership with non-Federal water management entities, manage Corps reservoirs to provide water supply storage in a cost-efficient and environmentally responsible manner.</p> <p>OBJECTIVE 3.2. Address the Operation and Maintenance (O&M) backlog. 3.2.1. Fund high-priority O&M.</p> <p>STRATEGIC GOAL 4. Reduce vulnerabilities and losses to the nation and the Army from natural and man-made disasters, including terrorism.</p>	<p>Goal 3 Ensure that projects perform to meet authorized purposes and evolving conditions.</p> <p>Objective 3.1. Improve the efficiency and effectiveness of existing Corps water resources projects.</p> <p>Objective 3.2. Address the Operation and Maintenance (O&M) backlog.</p> <p>Goal 4 Reduce vulnerabilities and losses to the Nation and the Army from natural and man-made disasters, including terrorism. The purpose of this goal is to manage the risks associated with all types of hazards and to increase the responsiveness of the Civil Works Emergency Management Program within the Corps Office of Homeland Security to respond to disasters in support of Federal, State, and local emergency management efforts. Emergency readiness contributes to national security. We have established two objectives to promote effective readiness, response, and recovery.</p>	<p>Navigation Program 3.1.1. Operate and manage the navigation infrastructure so as to maintain justified levels of service in terms of the availability to commercial traffic of high-use navigation infrastructure (waterways, harbors, channels).</p> <p>Flood and Coastal Storm Damage Reduction Program 3.1.2. Operate and maintain Corps infrastructure to ensure that designed levels of flood protection are realized.</p> <p>Environment Program 3.1.3. Ensure healthy and sustainable lands and waters and associated natural resources on Corps lands held in public trust to support multiple purposes, that is...</p> <p>3.1.3.1. Protect, preserve, and restore significant ecological resources in accordance with master plans. 3.1.3.2. Ensure that the operation of all Civil Works facilities and management of associated lands, including out-granted lands, complies with the environmental requirements of all relevant Federal, State, and local laws and regulations. 3.1.3.3. Meet the mitigation requirements of authorizing legislation or applicable Corps decision document.</p> <p>Hydropower Program 3.1.4. Provide reliable power. 3.1.5. Provide peaking power. 3.1.6. Maintain capability to provide power efficiently.</p> <p>Recreation Program 3.1.7. Provide justified outdoor recreation opportunities in an effective and efficient manner at all Corps-operated water resources projects. 3.1.8. Provide continued outdoor recreation opportunities to meet the needs of present and future generations. 3.1.9. Provide a safe and healthful outdoor recreation environment for Corps customers.</p> <p>Water Supply 3.1.10. In partnership with non-Federal water management entities, manage Corps reservoirs to provide water supply storage and environmentally responsible manner.</p> <p>3.2.1. Fund high-priority O&M.</p>	<p>Percent of time navigation infrastructure with high levels of commercial traffic sustains its functional purpose. Percent of time flood and coastal storm damage reduction infrastructure sustains its functional purpose. Percent of projects maintained at design level. Percent of acres with completed natural resource inventories. Percent of projects requiring Master Plans in accord with current regulations. Percent of all significant findings corrected annually. Percent of all identified major findings corrected annually. Percent of Corps-administered lands that meet the requirements in authorizing legislation or applicable Corps decision documents. Percent of completed projects that have successfully met mitigation goals. Forced outage rate. Physical condition/failure risk index. Annual net benefits per dollar invested (programmatic measure). Customer satisfaction. Facility Condition Index. Acre-feet of storage under contract versus acre-feet available. Percentage of total costs covered by revenues returned to Treasury.</p> <p>Percent change in dollar amount of essential O&M backlog at key facilities.</p>	<p>Strategies to Achieve Objective 3.1.</p> <ul style="list-style-type: none"> Conduct benchmark studies to determine the most efficient level of service. Prioritize critical maintenance requirements using performance measures. Examine and implement ways to reduce operational breakdowns. Develop and apply state-of-the-art technologies. As appropriate and feasible, use adaptive management processes to adjust to changing conditions. Conduct post-audits as authorized and funded. Modify operating plans as justified. <p>Example Reservoir operating plans can be modified to account for changed conditions that occurred over time since the project was originally constructed, as was done on the Green River, KY project. Any changes must necessarily be done within the purview of existing authorities and limits of available funds, or else the Corps must seek new authority or increased appropriations for economically justified and environmentally sound modifications.</p> <p>Strategies to Achieve Objective 3.2.</p> <ul style="list-style-type: none"> Develop a plan to identify high-priority maintenance as a strategy to reduce the Operation and Maintenance backlog. Operation and Maintenance projects in the Civil Works Program will be prioritized based on budget-based performance measures along with studies and construction.

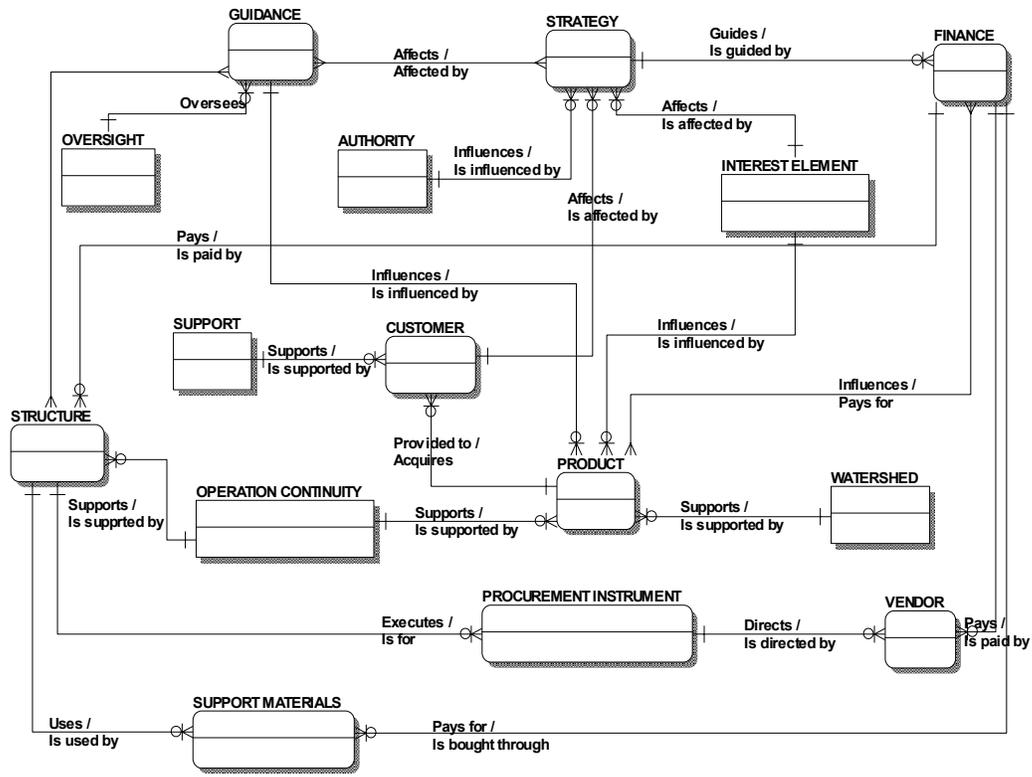
	Goals and Objectives	Program Objectives	Performance Measures	Strategies
<p>STRATEGIC GOAL 6. Be a world-class public engineering organization</p>	<p>Objective 4.1. Prepare and provide for rapid, efficient, and effective all-hazards response and recovery.</p> <p>Objective 4.2. Improve the safety and security of critical water resources infrastructure. The era of high-terrorism brings with it requirements for high security. We must ensure that dams, reservoirs, levees and other flood control works are secure from external threats and malevolent tampering to prevent devastating flooding and contamination of water supplies.</p> <p>Goal 5 Be a world-class public engineering organization. Goal 5 is focused on ensuring that the Civil Works mission is performed in a technically skilled manner so as to build respect and confidence in the products and services the Corps delivers today and into the future. Building trust will come from the integrity of our engineering and scientific evaluations and recommendations, the soundness of our management decisions, the transparency of our decision-making process, the reliability and effectiveness of our business processes, and the contributions we make to the state-of-the-art within and across our core technical disciplines. To achieve Goal 5, we must pay attention to people, processes, fiscal responsibility, efficiencies, and technology. The President's Management Agenda helps us focus on major organizational effectiveness aspects central to being a world-class organization: human talent, financial integrity, sound business practices, and the advantages that technology offers, especially to bring government closer to citizens. We have set three objectives to move toward Goal 5. We will draw upon the ongoing plans we have drafted in support of the President's Management Initiatives to</p>	<p>Emergency Management Program 4.1.1. Attain and maintain a high, consistent state of preparedness. 4.1.2. Provide a rapid, effective, efficient all-hazards response. 4.1.3. Ensure effective and efficient long-term recovery operations.</p> <p>4.2.1. Reduce risks to critical water resources infrastructure.</p> <p>Percent of personnel that have completed security training. Percent of sites passing security inspection.</p>	<p>Performance Measures Planning Response Team Readiness Index. PL84-99 Response Team Readiness Index. Percent of scheduled inspections performed for all non-Federal Flood Control Works in RIP, as required by ER 500-1-1. Percent of time solutions are developed and implemented (either repaired to pre-flood conditions or possible non-structural alternative) prior to the next flood season. Percentage of Federal and non-Federal flood control works in Rehabilitation and Inspection Program with a satisfactory condition rating.</p>	<p>Strategies Strategies to Achieve Objective 4.1. - Continue to serve as the lead agency in public engineering in support of the Federal Response Plan. - Work with the Department of Homeland Security in defining the Corps role with respect to homeland security and defense within the context of an all-hazards Federal Response Plan. - Promote research and development work units to improve flood damage reduction and disaster recovery plans, processes, and operations, e.g., levee inspection and Advanced Measures programs, and readiness training. - Improve simulations of our response to disaster scenarios to ensure optimum readiness planning. - Seek partnership opportunities with the Federal Emergency Management Agency to align their mitigation and recovery efforts with the Corps. - Continue to work with stakeholders and State and local emergency management agencies to improve emergency response planning.</p> <p>Strategies to Achieve Objective 4.2. - Ensure that the infrastructure the Corps operates and maintains is protected through a program of seamless infrastructure protection within the Corps. - Work with the Department of Defense and the Department of Homeland Security to develop infrastructure security standards for all Civil Works projects. - Support infrastructure threat analysis collection. - Implement water resources management policy related to critical safety and security. - Share infrastructure engineering expertise across Federal, State, and local entities.</p>
<p>OBJECTIVE 5.1. Be a world-class technical leader.</p> <p>5.1.1. Develop a Human Capital Strategy* to recruit, maintain, and enhance technical capability in core competencies. 5.1.2. Competitive Sourcing*: Accomplish inherently non-governmental work through others in support of mission accomplishment. 5.1.3. Support for Others: Provide public works engineering and construction management services that meet the customer's expectations.</p> <p>OBJECTIVE 5.2. Improve budgeting and financial performance.*</p> <p>5.2.1. Produce auditable annual Civil Works financial statements that receive an unqualified opinion. 5.2.2. Link the budget directly to performance.*</p> <p>OBJECTIVE 5.3. Become a more efficient and effective organization through technology (e-government*).</p> <p>5.3.1. Ensure that the Civil Works mission is supported by an information architecture and capital investments in technology aimed at increasing work efficiencies and effectiveness.* 5.3.2. Develop and use electronic means and media to provide timely and easily accessible information about engineering and related services to customers, the public, and other interested parties.*</p> <p>* Part of the President's Management Initiatives</p>	<p>Objective 5.1. Be a world-class technical leader.</p> <p>Objective 5.2. Improve budgeting and financial performance.</p> <p>Objective 5.3. Become a more efficient and effective organization through technology.</p>	<p>5.1.1. Develop a Human Capital Strategy* to recruit, maintain, and enhance technical capability in core competencies. 5.1.2. Competitive Sourcing* - Accomplish inherently nongovernmental work through others in support of mission accomplishment. 5.1.3. Support for Others: Provide public works engineering and construction management services that meet the customer's expectations.</p> <p>5.2.1. Produce auditable annual Civil Works financial statements that receive an unqualified opinion.* 5.2.2. Link the budget directly to performance.*</p> <p>5.3.1. Ensure that the Civil Works mission is supported by an information architecture and capital investments in technology aimed at increasing work efficiencies and effectiveness.* 5.3.2. Develop and use electronic means and media to provide timely and easily accessible information about engineering and related services to customers, the public, and other interested parties.*</p>	<p>Office of Personnel Management in rating scorecard for the President's Management Initiatives. Competitive sourcing guidelines established by the Office of Management and Budget. Scoring from surveys of customer satisfaction with the quality, cost, and timeliness of public engineering and construction management services provided by the Corps.</p> <p>Unqualified rating by an independent audit of all relevant financial statements. Percent of business programs that have at least one efficiency measure. Percent of programs (measured in terms of dollars) that have been rated by the Program Assessment Rating Tool (i.e., PARTed).</p> <p>Standards set by Clinger-Cohen Act and other relevant laws that apply to the Chief Financial Information Officer in the Corps. Standards set by the Office of Management and Budget. Commence at least one Information Technology initiative that affects approximately 4,000 citizens per day.</p>	<p>Strategies to Achieve Objective 5.1. Our strategies focus on recruitment, retention, fiscal responsibility and accountability, business process improvements, innovation, and outreach. Providing quality and responsive engineering and scientific services to the Nation and others requires a solid technical foundation. Toward preserving our technical edge, we will do the following: - Develop a Strategic Management of Human Capital Plan for USACE that addresses OPM's Human Capital Accountability and Assessment Framework within the context of corporate planning, competitive sourcing, and technology initiatives. - Improve recruiting policies and procedures targeted to critical skill areas. - Implement a Planning Excellence Program to enhance our planning capability and economic evaluations. - Establish national and regional Planning Centers of Expertise. - Heed the National Academy of Sciences recommendation to institute independent review on large or controversial projects. - Support competitive sourcing initiatives proposed by the Administration in concert with the mandates of the Federal Activities Inventory Reform (FAIR) Act of 1998. - Partner with the Department of Army to streamline and standardize the employment application process for individuals seeking employment. - Improve leadership training and doctrine. - Preserve our world-class capabilities through a robust Research and Development program, in part oriented to development and application of new technologies. - Improve our technology transfer to promulgate our skills and knowledge more widely. - Share our knowledge and expertise with others through an active Support for Others Program. - Improve technology implementation through a Strategy for Management of Science and Engineering Technology (SET).</p> <p>Strategies to Achieve Objective 5.2. - Work with the Department of Defense Inspector General (DODIG) to produce a Chief Financial Officer's Report summarizing performance results for the Civil Works Program that is worthy of an unqualified audit opinion from the DODIG. - Improve business processes and automated information systems to improve our financial management. - Work with the Defense Finance and Accounting Service to ensure that financial reporting requirements are met. - Develop the annual Civil Works budget on the basis of business program performance measures and targets. Budget development will utilize a performance-based budgeting process to set budget priorities within and across Civil Works business programs.</p> <p>Strategies to Achieve Objective 5.3. - Develop a world-class enterprise-wide information technology environment through improved information connectivity within the Corps and with the public, respecting the need to assure information security. - Ensure that information technology systems meet IT security objectives. - Reduce reporting burdens, streamline business transactions and make decision making more transparent through web-based electronic mechanisms that promote information access and sharing. - Improve government-to-citizen services by leveraging technology and e-government (E-Gov) initiatives. - Focus Information Technology (IT) spending on high-priority modernization initiatives using a modernization blueprint for Enterprise Architecture.</p> <p>Examples of How the Corps is Improving Government-to-Citizen Services -The Corps' Navigation Data Center provides the Operations and Maintenance B Information Link (OMBIL), an electronic system that links and standardizes open regarding navigation, flood protection, hydropower, environmental stewardship, and regulatory issues. -The Corps' Emergency Management Program operates ENSLink, a GIS-based system for emergency communications, command, and control that enables rapid maps and data regarding both baseline information and specific disaster events. -We have integrated regulatory permits, outgrants, and other types of authorization licenses for ease of public access and completion. -The Corps' Internet-based National Recreation Reservation Service serves as a recreation reservation system for the public for more than 145,000 recreation sites 1700 Federal lakes and parks, including National Parks and other public lands. -Within the Regional Sediment Demonstration Program, a regional geospatial information system (GIS) is being developed to provide baseline data and historical data sets. -The Corps' Natural Resources Management Gateway provides a one-stop on-line interface for the public to access information about the Corps' natural resources. -The Corps is taking the lead in partnership with the Coast Guard, the National C... -The CorpsMap Program will provide one geospatial interface for all nation-level...</p>

Appendix J – Description of Baseline and Target Enterprise Data Environments



J.1 Baseline Enterprise Data Model

A USACE Baseline Enterprise Data Model, derived from the USACE Information Systems Plan prepared in 1986, discloses that many of the data classes are still valid today. While there may be some modifications to definitions, most of the terms are still appropriate.



*** USACE BASELINE ENTERPRISE DATA MODEL**
July 2003
**Based on current documentation available, discussions, the EA Repository and web site research.*

Figure J.1. USACE Baseline Enterprise Data Model, July 2003

J.2 Baseline Enterprise Data Classes

Table J.1 identifies the 64 data classes in use by USACE-wide Automated Information Systems (AIS) for the past 20 years. Definitions for the Baseline Data Entities follow; however, definitions for the data classes still require review and validation.

Table J.1. Baseline Enterprise Data Classes

1. Policy, Regulation, Law	33. Manpower
2. Strategy, Goals and Objectives	34. Financial Status
3. Command Performance Analysis	35. Mission Training
4. Audits and Reviews	36. Civilian Personnel
5. Inspections	37. Military Personnel
6. Efficiency Improvement	38. Equal Employment Opportunity (EEO)
7. Organization	39. Legal
8. Stationing Analysis	40. Security
9. Army Facilities Budget	41. Contract/Purchase Order
10. Civil Works Budget	42. Safety
11. Command Operating Budget	43. Public Information
12. Military RDT&E Budget	44. Administrative Information
13. R&D Project Status	45. Customer
14. Military Engineering	46. Interest Element
15. Agreement	47. Internal Regulations, Publications, Other
16. Environmental	48. Expendable Property
17. Civil Works Planning Studies	49. Accountable Property
18. Civil Works Operations	50. Hydrologic
19. Vendor	51. Climatic
20. Technical Engineering	52. Authorizing Documents
21. Studies	53. PRIP Budgets
22. Design Project	54. Law Enforcement
23. Construction Project	55. Intelligence
24. Real Property Utilization	56. Information Systems Plans
25. Real Property Management	57. CW Maintenance
26. Real Estate Acquisition and Disposal	58. Paperwork Management
27. Army Operations and Maintenance	59. Investigations
28. Regulatory	60. Payroll
29. Emergency Operations Plans	61. Travel
30. Emergency Operations Status	62. Federal Engineers Budget
31. Mobilization Plans	63. Family Housing Utilization
32. Mobilization Status	64. Waterborne Commerce Statistics

Fifteen enterprise data entities were identified as common to USACE-wide AISs: ACTIVITY, AGREEMENT, FINANCE, COMPLIANCE, DOCUMENT, EVENT, GUIDANCE, LOCATION, ORGANIZATION, PARTY, PRODUCT, PROJECT, PROPERTY, RESOURCE, EVENT. These data entities are defined in Table J.2.

Table J.2. USACE Baseline Data Classes mapped to USACE Enterprise Data Classes

BASILINE DATA CLASS	ENTERPRISE DATA CLASS	DEFINITION
	ACTIVITY	A name process, function, or task that occurs over time and has recognizable results. Activities combined to form business processes. A task or series of tasks performed over a period of time.
Army Operations & Maintenance	ACTIVITY	
Civil Works Maintenance	ACTIVITY	
Civil Works Operations	ACTIVITY	
Inspections	ACTIVITY	
Military Engineering	ACTIVITY	
Mission Training	ACTIVITY	
Technical Engineering	ACTIVITY	
Paperwork Management	ACTIVITY	
	AGREEMENT	An arrangement between parties.
Agreement	AGREEMENT	
Contract/Purchase Order	AGREEMENT	
	FINANCE	The estimate of costs and expenses, including underlying rates and unit prices, and quality units of output or service used to plan the total cost of the project.
Army Facilities Budget	FINANCE	
Civil Works Budget	FINANCE	
Command Operating Budget	FINANCE	
Federal Engineers Budget	FINANCE	
Military RDT&E Budget	FINANCE	
PRIP Budgets	FINANCE	
Payroll	FINANCE	
	COMPLIANCE	Obedience to request, command, etc., or the capacity to yield. It is the act or process of complying with a desire, demand, or proposal or to coercion or to conforming in fulfilling official requirements
Climatic	COMPLIANCE	
Efficiency Improvement	COMPLIANCE	
Environmental	COMPLIANCE	

BASELINE DATA CLASS	ENTERPRISE DATA CLASS	DEFINITION
Family Housing Utilization	COMPLIANCE	
Hydrologic	COMPLIANCE	
Law Enforcement	COMPLIANCE	
Legal	COMPLIANCE	
Safety	COMPLIANCE	
Security	COMPLIANCE	
Manpower	COMPLIANCE	
Military Personnel	COMPLIANCE	
	DOCUMENT	Something written, etc., that provides record or evidence of events, circumstances, etc.
Authorizing Documents	DOCUMENT	
Emergency Operations Plans	DOCUMENT	
Information Systems Plans	DOCUMENT	
Internal Regulations, Publications, Other	DOCUMENT	
Mobilization Plans	DOCUMENT	
Public Information	DOCUMENT	
	EVENT	A significant occurrence or happening that represents a fundamental observation of physical reality represented by a point in time.
Audits and Reviews	EVENT	
Emergency Operations Status	EVENT	
Financial Status	EVENT	
Mobilization Status	EVENT	
Research and Development Project Status	EVENT	
Waterborne Commence Statistics	EVENT	
	GUIDANCE	A statement of direction provided by corporate management.
Policy, Regulation, Law	GUIDANCE	
Regulatory	GUIDANCE	
Strategy, Goals & Objectives	GUIDANCE	
Administrative Information	GUIDANCE	
Equal Employment Opportunity	GUIDANCE	
	LOCATION	A specific place.

BASELINE DATA CLASS	ENTERPRISE DATA CLASS	DEFINITION
Travel	LOCATION	
	ORGANIZATION	Defined functional components of the USACE used to accomplish the USACE mission. An administrative structure with a mission.
	PARTY	An organization, person or group involved in an enterprise as a participant or as an accessory.
Organization	PARTY	
Vendor	PARTY	
Civilian Personnel	PARTY	
Customer	PARTY	
	PRODUCT	Something resulting from or necessarily following from a set of conditions. Something that is produced by an activity, especially by an industrial process.
Civil Works Planning Studies	PRODUCT	
Command Performance Analysis	PRODUCT	
Intelligence	PRODUCT	
Investigations	PRODUCT	
Stationing Analysis	PRODUCT	
Studies	PRODUCT	
	PROJECT	An undertaking with a defined starting point and objectives. Projects depend upon a finite period of time and resources by which the objectives are accomplished.
Construction Project	PROJECT	
Design Project	PROJECT	
	PROPERTY	Land, improved or unimproved, along with natural resources.
Accountable Property	PROPERTY	
Expendable Property	PROPERTY	
Real Estate Acquisition & Disposal	PROPERTY	
Real Property Management	PROPERTY	
Real Property Utilization	PROPERTY	
	RESOURCE	Any factors, except time, which are required or consumed to accomplish a task or activity. Resources can be quantified and defined. This could include, but is not limited to manpower, equipment, expenses and materials.
Interest Element	EVENT	
Other		

J.3 Baseline Enterprise Data Objects

The baseline data objects were defined and developed with narrow-focused scope to ensure completeness at the higher levels of data administration as part of the management strategy to allow more thorough examination of data in the future by individual business functional areas.

The primary source for identifying baseline data objects was the 1984 Information System Plan (ISP). This document identified 64 data classes and presented a basic, high-level Entity Relationship Diagram (ERD) of data exchange. It was determined that these data objects represented at least 80% of corporately shared data and that no changes would be required to the data and their definitions at this time.

Sources of information to analyze current data use and data management practices included:

- Existing USACE Data Repositories
- The 1984 ISP
- Discussions with the previous USACE Data Administrator
- Discussion with the previous USACE Model Manager
- DRM Team meetings and discussions

J.4 Create, Read, Update, Delete (CRUD) Matrix

An existing CRUD matrix that represents the use of the USACE data classes by major business functions was validated and is used as the initial source of an up-to-date CRUD Matrix for the USACE Baseline data class mapping. This modified, notional baseline CRUD Matrix is considered a template to be completed and validated by business owners in the near future. Figure J.2 is a representative sample of the CRUD Matrix.

J.5 Observations and Issues Related to the Baseline Data Environment

Issues related to the Baseline Data Environment that warrant further exploration were identified. The following lists specific vision statements or strategic goals that the enterprise data model addresses and the observations/issues associated with the baseline data environment:

- Establishment of an effective standardized and interoperable Information Technology (IT) data environment.

Data Impact: Need for uniformity of data structures; standards defined and applied; data management processes and procedures defined and applied; data access clearly defined and applied; data changes effectively communicated. On a timely basis, enterprise input to data changes.

- Become a citizen-centered E-Government agency. Electronic government is one of the five key elements of the President's Management and Performance Plan. A "digital agency" where many of our processes, activities, and interactions are done in an electronic manner.

Data Impact: Need to realize virtual team/project management; knowledge management utilized.

- Manage and present structured and unstructured data. The Information View does not deal with just raw data, but all types of information derived from data to include text, documents, presentation graphics, engineering drawings, imagery, video and audio.

Data Impact: Need for inclusion of geospatial data as enterprise data; availability of geospatial data to all. Uniformity of data structures; standards defined and applied; data management processes and procedures defined and applied.

- Facilitate the sharing of knowledge across our traditional stovepipes.

Data Impact: Need for a repository of enterprise data/metadata; processes and procedures for sharing; adequate access and security. Data Impact: Enable data to facilitate the Common Delivery Framework (CDF).

- Web-enable data for sharing purposes. A Web-accessible library of software resources and technical guidance that comprise the "raw materials" that USACE developers, contractors and partners will use to develop specific science and engineering applications and suites of applications, called Product Lines and Product Suites.

Data Impact: Need to enable a flexible, timely Web presentation of information derived from enterprise business and geospatial data.

- Collaboration with other Federal agencies and industry is key to the successful sharing of information and technology

Data Impact: Need to use commercial off-the-shelf (COTS) and Government off-the-shelf (GOTS) data structures and data (or universal data structures) wherever and whenever possible.

- Improve the effectiveness of existing Corps water resources projects in adaptive ways.

Data Impact: Need to provide the means to respond to the need for environmental issues quickly in a number of varied means and methods.

- Be a world-class technical leader + Develop a Human Capital Strategy to recruit, maintain, and enhance technical capability in core competencies.

Data Impact: Need to develop and populate a knowledge management and document presence on the Web.

- Provide an integrated enterprise across USACE science and engineering functions.

Data Impact: Need to standardize data at the enterprise level; provide an enterprise glossary; provide a knowledge management capability; standardize data structures; minimize the possibility of data inconsistency; maximize data quality and availability.

- Providing a common baseline for Science and Engineering (S&E) models to interoperate to improve the delivery of information and technology.

Data Impact: Need to provide for universal data structures; facilitate standardization; facilitate data communication.

- Enable data to facilitate the CDF.

Data Impact: Need to provide for universal data structures; facilitate standardization; facilitate data communication.

- Supports E-Government goals by embracing the World Wide Web Consortium Internet-based standards for interoperability and security, providing the baseline for all systems, new and old, to work together to improve how technology and information are delivered to customers, business partners, and employees.

Data Impact: Need to provide for universal data structures; facilitate standardization; facilitate data communication.

- Become involved in the collaboration among other Federal agencies and industry including NOAA, USGS, USDA, EPA, Microsoft, ESRI in terms of data sharing

Data Impact: Need to provide for universal data structures; facilitate standardization; facilitate data communication.

- Develop a standard approach to accessing, organizing, and managing geospatial information, real-time monitor information, time-series data, meteorological data, hydrographic data, etc., as defined by CDF. CDF also provides a common approach to accessing hydrologic, coastal, and environmental S&E model.

Data Impact: Need to integrate geospatial data into enterprise data; share geospatial data on the enterprise level. Provide knowledge management capabilities related to enterprise geospatial data.

- Use the processes of reengineering to facilitate the identification of technology, functionality and information components required across USACE mission areas.

Data Impact: Need to provide for easy means of changing data structures and content.

- Modernizing legacy S&E software to accomplish future operating requirements is one alternative to the status quo approach. This approach involves the recoding of each S&E application/model to modern standards that facilitate operating in an enterprise environment. Legacy S&E software currently uses hundreds of differing technologies (dating back to the early 70's), which are unable to operate directly with an enterprise solution.

Data Impact: Consistent with the emphasis on processing functions, need to “facilitate operating in an enterprise environment” that involves data concerns that should be shareable, flexible for changes and easily understood between business processes and business units and different agencies.

- Develop data structures and processes designed for more timely decision support.

Data Impact: Need to develop universal data structures that are flexible, easy to understand and amenable to change.

- Develop data structures and functions designed to reduce cost for information sharing.

Data Impact: Need to develop a repository of common data; share data definitions and domains; control data; decide data changes in an enterprise manner.

- Develop data structures and functions designed for the S&E Technology (SET) Business Processes that provide the strategies for corporate management by USACE of all the technologies that support science and engineering applications.

Data Impact: Need to incorporate Geographic Information Systems (GIS) into standard business data processing. In addition, CDF is the operational platform that supports the SET strategy. The USACE Technology Committee and USACE leaders support this strategy. A Strategic Plan has been developed for CDF that provides overall direction and guidance for developing and maintaining USACE CDF of processes and reusable components that are applied throughout the development and delivery of USACE technologies.

- The CDF is not focused on creating data, but rather managing the use of data. Therefore, the data supported by the CDF already exists at all levels - Federal,

State, and local. After identifying and prioritizing the data sources, we plan to coordinate with the agencies that own the data to develop a plan for access.

Data Impact: Need to develop and use common data definitions, structures and knowledge management processes and procedures.

- CDF defines the rules, standards, and conventions as well as the shareable functionality through common software libraries needed to improve how we deliver and insert technology.

Data Impact: Consistent with the emphasis on processing functions, need to “facilitate the capability to operate in an enterprise environment” that involves data objects that should be shareable, flexible. These data objects should be amenable to rapid change and easily understood between business processes, business units and different agencies.

- The standard for geospatial information for USACE, the Spatial Data Standard for Facilities, Infrastructure, and Environment (SDSFIE), is an implementation of the Federal Geographic Data Committee (FGDC) standard as well as an ANSI standard. The SDSFIE will be the CDF standard for geospatial information.

Data Impact: Need to integrate GIS into the mainstream enterprise data architecture.

- The Corps enterprise data has been partitioned into "publicly accessible" data sets or segments, and private or enterprise data sets. "Publicly accessible" data sets comprise data generally available for the public good, such as the data on the availability of space in recreation areas; data available for public safety, such as water control data; and data available for public planning, such as data on the progress of the South Everglades Restoration Project. Publicly accessible data sets are logically and physically "quarantined" from "production" enterprise data sets supporting daily mission operations.

Data Impact: Make data readily available to authorized users in a format and presentation easily understood and accessed. Provide knowledge management capabilities; improve vertical and horizontal communications between all echelons and functional areas.

- Need to be able to identify, correct and standardize inconsistent or erroneous data in the environment.

Data Impact: To the extent reasonable, ensure that data is entered only one time. Develop processes and procedures for routinely measuring data quality.

J.6 Target Data Environment for Mission-Critical AIS

Figure J.3 provides a list of the USACE Baseline Data Classes mapped to USACE Target (or Enterprise) Data Classes.

J.7 Conceptual, High-level Target Enterprise Entity Relationship Diagram

The USACE Target Enterprise Data Model is displayed in Figure J.4.

J.7.1 Conceptual Target Enterprise ERD (explosion of the LOCATION Entity for Conceptual Detail)

The data concept within this diagram allows one to relate any description of location and its accompanying data to any party or project. It allows the user the capability to define a location (e.g., country, state, county, city, non-incorporated jurisdiction, etc.). There is a heavy use of data typing within the model along with providing historical entity and rationale data (the reason entities) that can also be added for tracking of database events, over time.

Through the association of LOCATION to Party (e.g., individual (e.g., POC, Contractor, subcontractor, employee, etc.) or Organization (e.g., vendor, customer, District office, Congress, etc.) to any location (Figure J.5), it also allows the user the capability to define LOCATION as a telephone, physical address, a set of coordinates or even a cell phone. Through the relationships expressed through the model, any user could query any combination of these at any time for results the combination of which are exponential.

By isolating specific types of data to entities that they directly characterize (attribution) and by placing those in proximity to each other (database structure) based on type of query, use and frequency, these will be more maintainable, efficient, and accessible.

J.7.2 Conceptual Target Enterprise ERD (explosion of the PARTY Entity for Conceptual Detail)

The data concepts embedded in PARTY are the same (Figure J.6). There is a strong emphasis on data typing and the provision for rationales. Through the data and data relationships of PARTY, every type of data object (e.g., man, woman, employee, contractor, congressman, vendor, EPA, etc.) can easily (and as a by-product of the well-structured database) be related to the other. Through this set of data and relationships, any individual can be related (of a certain type) to any other.

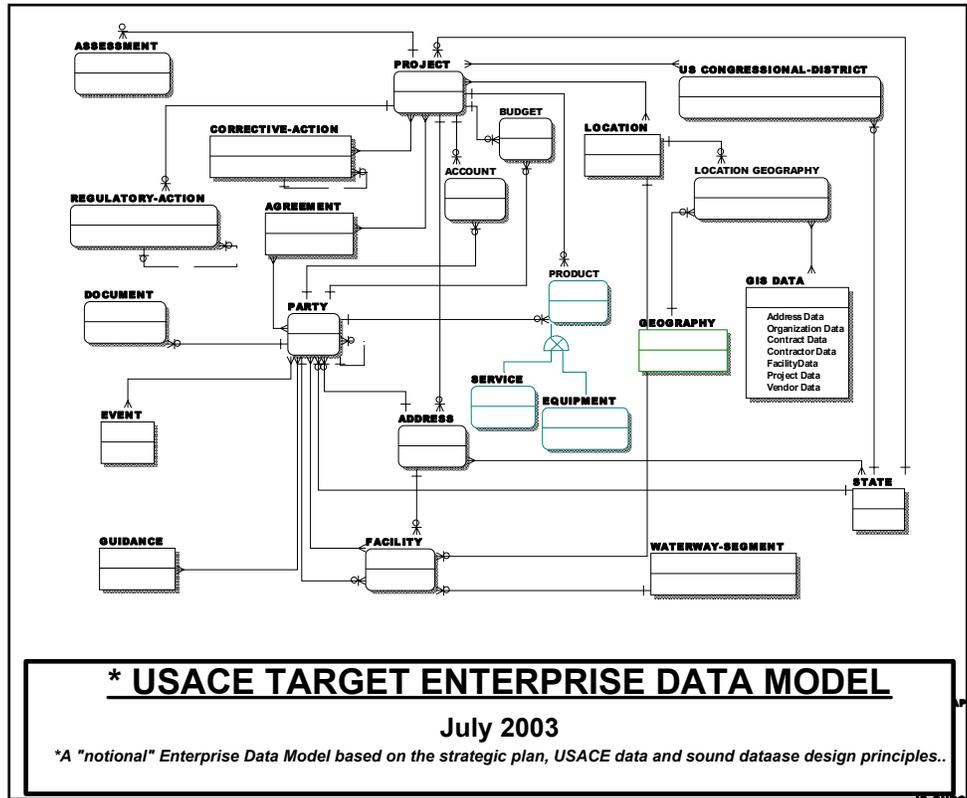


Figure J.4. USACE Target Enterprise Data Model

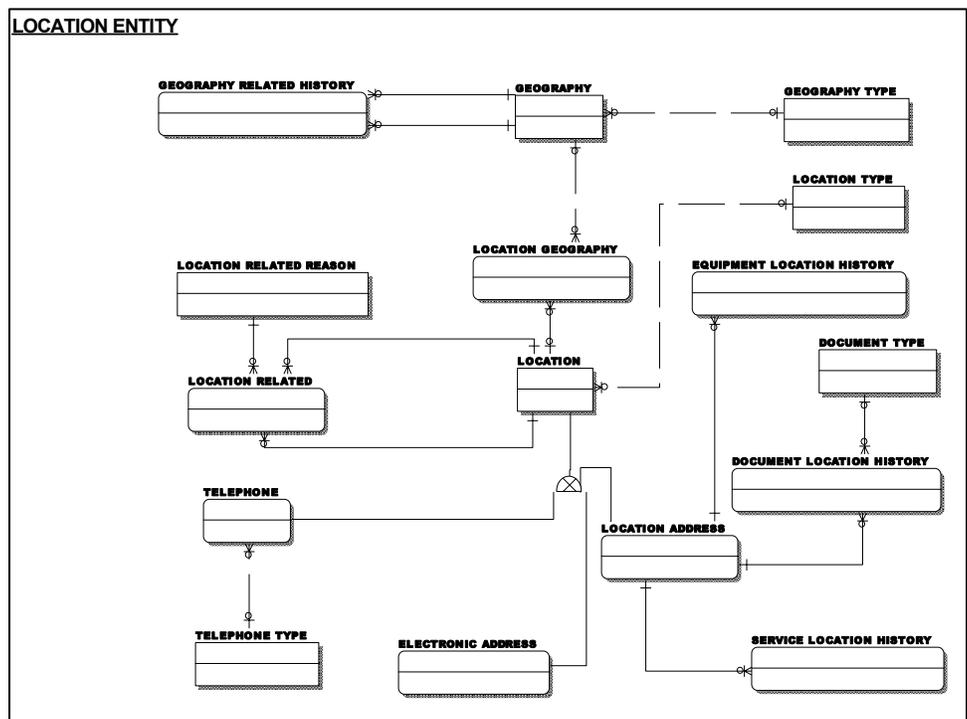


Figure J.5. LOCATION entity

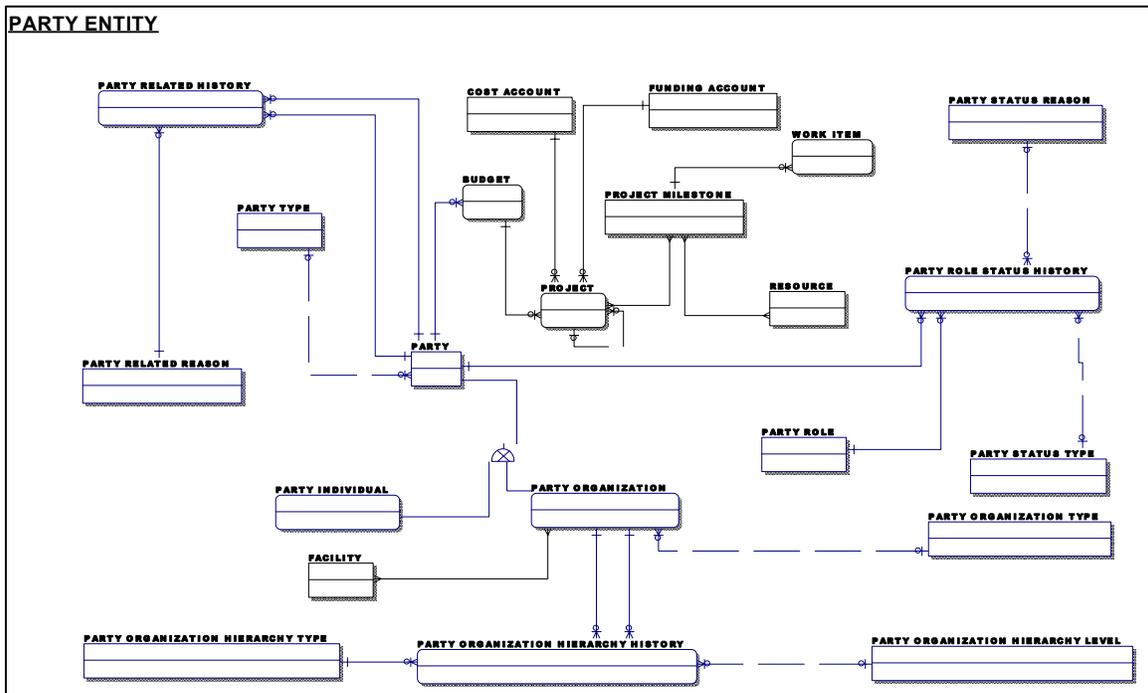


Figure J.6. PARTY entity

Combining these two concepts, we can see how any PLAYER of any TYPE can have any ROLE and be located in any country and have any number of ways of being located by address. As a concept, typing (with subsequent subtyping), making the provision for rational capturing and relating data in “small packages” that are frequently used together in a database while separating out “dissimilar” data from the database, produces efficient, maintainable database structures that provide substantial information even about its own operation.

J.8 Eight Enterprise Systems Studied as Part of ERD Analysis

J.8.1 REMIS

Description:

REMIS, a real estate database, has approximately 300 tables whose production content handles approximately 10,000 land tracts and is replicated in 33 Districts. These replicated structures, as with PROMIS/P2, are closely integrated with and share tables with the CEFMS database.

REMIS to CEFMS:

The REMIS database is used by the referenced 33 Districts to store and maintain project, funding request and funding allocations associated with the associated CEFMS funding account and project data. Project and Purchase Request data are periodically shared with CEFMS for funding processing and approval (each District maintains their own data and performs this same function).

REMIS data and any Purchase Request are compared to CEFMS stored and maintained project data work code data and fund account data, the result of which is communicated back to the REMIS database. CEFMS stores and maintains all funding data for programs and projects and must allocate these funds based on budgets, programs, projects, resources, requests and authorized work items.

CEFMS to REMIS:

Fund allocation data and request status data are interfaced from CEFMS to REMIS. The database is used to record and maintain data on USACE civil works real property inventory, status of acquisition, management, and disposal of land and space by USACE and other agencies. In this way, the database stores and maintains complete and accurate project and real property data, which is made available for business processing through the shared REMIS/CEFMS tables.

Location:

A full and exact copy of the REMIS database is maintained within 33 Districts.

REMIS data types are:

- Acquisition data
- Address data (Electronic mail, Employee address, Addressee)
- Agreement data (Interagency agreement, Local cooperation agreement)
- Asset data
- Authority data
- Budget data (Allotment, Appropriation, Obligation)
- Contract data
- Event data (Superfund event)
- Finance data (e.g., Accounting data, General ledger correlation, Billing, collection, claim, payment, cost account, check, Fiscal station, Invoice, Foreign currency, Payment method, Remittance, Outgrant, Outgrant area associative)
- Fund data (Funding account, Funding authority, Funding authorization document location master)
- Legal data (Legal advice, Legal description, Litigation)
- Location data (Country, County, County location, State, Electronic mail, Employee address, Work item location, Tract location, Map)
- Compliance data (Outgrant compliance inspection)
- Party data (Addressee, Litigation adverse party, employee, Manufacturer, Operating agency, Organization, Attorney, Contractor, Department, Customer,

Employee, Point of contact, Financial institution, Payee, Installation, Tenant, Real property owner)

- Guidance (Policy)
- Product data (Manufactured item, Work item, Survey Task, Work breakdown element, Work categorization, Work item milestone, Work phase, Work phase status, Function)
- Program data
- Project data (Milestone)
- Property data (Real property, Motor vehicle)
- Inventory data (Purchase request, Receipt voucher, Receiving report)
- Real property acquisition data
- Real property ownership data
- Resource data (Training course, Training program, Resource plan)
- Contract data (Solicitation, Bid offer data)
- Tract data (Tract map, Tract survey)
- Warehouse inventory resource data

J.8.2 CEFMS

Description:

CEFMS is the USACE fully operational, integrated database that supports CEFMS business processing. It contains data for a fully operational online, interactive financial management system that integrates USACE business processes and supports the management of all types of project work and project funding and provides operational and management information for decisionmaking.

CEFMS is a totally integrated, relational database system that supports General Fund Accounting, Funds Control, Time & Attendance Processing and Labor Distribution, Accounts Payable, Accounts Receivable, Disbursing/Collections, Debt Management, Travel Management, Acquisition, Asset Management, Inventory, Personnel/Manpower, Budget Formulation and Execution, and Financial Reporting.

CEFMS' data integration with the REMIS database allows revenues and expenses to be produced for the real properties of USACE, which are then tracked through the data and reported on. This database integration is managed through Oracle database links for remote connectivity as well as collocated, fully shared tables residing in the same database. The database has the functionality for real-time updating, when necessary.

The data within the CEFMS relational database is used by CEFMS applications for project financial execution and management at the District level. This data includes project-funding data, obligation data, capital and project expenditure data, and

disbursement data associated with individual authorized projects. It also supports General Fund Accounting, Funds Control, Time & Attendance Processing and Labor Distribution, Accounts Payable, Accounts Receivable, Disbursing/Collections, Debt Management, Travel Management, Acquisition, Asset Management, Inventory, Personnel/Manpower, Budget Formulation and Execution, and Financial Reporting; and it provides accounting for commitments through cash outlays, including all revenues, expenses, and US Standard General Ledger updates by transaction. The data in CEFMS supports cost accounting as well as Activity Based Costing.

The entry of data into the CEFMS database is a single source data entry with National Institute of Standards and Technology (NIST) approved electronic signature capability. This single-source data entry provides real-time data on project, contract, and financial status so users have accurate, reliable information for providing technical and professional services. Security of the data is maintained as CEFMS allows only authorized users to view/input data from multiple locations at any time because access is through the USACE CEFMS Web site.

Standardized data input is allowed from authorized users to view/input data from multiple locations at any time through the utilization of single-source data entry and NIST-approved electronic signature capability. CEFMS integrates financial data with other Corps of Engineers standard automated systems and interfaces with other DoD standard systems. It also provides real-time data on project, contract, and financial status so users have accurate, reliable information for providing technical and professional services.

In terms of data transfers, CEFMS provides external, Annual Financial Statement data to the Department of Energy (e.g., Western Area Power Administration) and other transfers of accounting data to the DoD on a monthly basis, among others.

The CEFMS database (Table J.3) is normally available during regular business hours. However, it will be unavailable at night due to scheduled processes, which update and backup the database. It may also be unavailable on weekends for computer maintenance.

Table J.3. CEFMS Database Locations

CEFMS Database Locations:			
FOA	Name	FOA	Name
A0	Huntsville Engineering and Support Center	J1	Far East District
B0	Mississippi Valley District	J2	Japan District
B1	Memphis District	J3	Honolulu District
B2	<i>New Orleans District</i>	J4	Alaska District
B3	St Louis District	K0	South Atlantic Division
B4	Vicksburg District	K2	Charleston District
B5	Rock Island District	K3	Jacksonville District
B6	St Paul District	K5	Mobile District
E0	North Atlantic District	K6	Savannah District
E1	Baltimore District	K7	Wilmington District
E2	Washington District	L0	South Pacific Division
E3	New York District	L1	Los Angeles District
E4	Norfolk District	L2	Sacramento District
E5	Philadelphia District	L3	San Francisco District
E6	New England	L4	Albuquerque District
E7	Europe District	M0	Southwestern Division
G0	Northwestern Division	M2	Fort Worth District
G2	Portland District	M3	Galveston District
G3	Seattle District	M4	Little Rock District
G4	Walla Walla District	M5	Tulsa District
G5	Kansas District	N0	Transatlantic Programs Center
G6	Omaha District	P0	Gulf Region Division
H0	Great Lakes and Ohio River Division	Q0	Water Resources Support Center
H1	Huntington District	S0	HQ USACE
H2	Louisville District	T0	USACE Finance Center
H3	Nashville District	U1	Topographic Engineering Center
H4	Pittsburgh District	U2	Cold Regions Research & Engineering Lab
H5	Buffalo District	U3	Construction Engineering Research Lab
H6	Chicago District	U4	Waterways Experiment Station
H7	Detroit District	W2	Humphreys Engineering Center Support Activity
J0	Pacific Ocean Division		

CEFMS data types are:

- Property data (Accountable Property, Expendable Property, Real Estate Acquisition and Disposal)
- Document (Administrative Information)

- Agreement
- Budget (Army Facilities Budget, Civil Works Budget, Federal Engineers Budget, PRIP Budget)
- Product (Army Operations and Maintenance, Civil Works Operation, Civil Works Planning Study, Command Performance Analysis, Military Engineering)
- Authority (Authorizing Document)
- Account (Financial Status, Command Operating Budget, Payroll)
- Agreement (Contract, Purchase Order)
- Project (Design Project, Manpower, Construction Project)
- Resource (Environmental)
- Party (Organization, Party Civilian Personnel, Customer)
- Project (R&D Project Status)
- Event (Travel)

J.8.3 OMBIL Plus

J.8.3.1 Description:

The Corps is the sole Federal provider of water transportation data (designated by the Office of Management and Budget (OMB)). Additionally, the Corps is the single source for project output and activity data regarding the Operations and Maintenance business programs of Navigation, Hydropower, Recreation, Environmental Compliance, Natural Resources and Flood Damage Reduction. The Corps' customers for these data sources include parties such as the United States Customs, Department of Transportation (DOT), Commerce Department, Environmental Protection Agency, Department of Energy, State DOTs and the National Academy of Science as well as the U.S. Congress. The Corps plays a central role in providing the required coordination and oversight of these data and information transfers in order to ensure the data is accurate, useful, fully maintained and archived.

OMBIL Plus, as a database, houses data used to generate and provide O&M Managers results-oriented, efficiency-based performance information in support of O&M management decisions.

OMBIL is deployed Corps-wide with management information relevant to all O&M business function areas. There are processes that run against the database that extract performance-based management information from various transaction-based O&M systems as well as budget and financial systems, place that information into an Oracle8™ database and provide that information on the Corps intranet in a graphical format for review and analysis by users of the OMBIL Plus data.

There are three primary technical components in OMBIL. The first is the O&M transaction systems (e.g., Natural Resources Management System, Hydropower

Spreadsheets, etc.) that were modernized and became the transaction-based O&M business function feeder system. Second is the data mart. This is where information from the O&M business function feeder systems and resource information from the budget and financial systems are summarized. The third component is the O&M Business Information graphical user interface where users may review various components of the data mart. The OMBIL design team developed the feeder systems and O&M Business Information such that all transactions and analyses can occur using Web technology. This means that the O&M users need only a Web browser to enter their data and review their performance-based management information.

J.8.3.2 OMBIL Data Mart:

The OMBIL Plus database is an integrated data warehouse that merges data related to financial, activities, inventory and outputs to create performance measures of efficiency and effectiveness. The OMBIL Plus database (Operations and Maintenance Business Information Link) supports the OMBIL Plus System. This system is designed to standardize and integrate data whose source was data from 11 legacy systems that provided business information, performance and data for the Corps Civil Works Operations and Maintenance community.

It is an Oracle™ relational database and houses extracted information from each of the O&M systems and resource information from the budget and financial systems. Extraction routines are developed to query each of the feeder systems to generate rollup information on a monthly basis for the data mart. These extraction routines are designed to operate on a set schedule, such that in the first 5 days of each month, all feeder systems are accessed for monthly information from the previous month.

J.8.3.3 O&M Business Information:

To present the data mart information to the user quickly and graphically, the data mart information is extracted from the Oracle relational data mart into a multidimensional database, where it can be presented to the user through the Corps intranet. The user only needs to run the O&M Business Information data is a Web browser. The data is presented in this manner to greatly enhance the business community's ability to holistically view all aspects of the business data and information from the eleven diverse legacy systems data.

Internal Corps managers use these data to monitor and evaluate performance nationally, throughout the organizational hierarchy from Headquarters down to the project level. This information also provides data that the Corps reports to OMB and Congress on the efficiency and effectiveness of the Corps' Civil Works Program.

In summary, OMBIL data provides the data capabilities for USACE of:

- Combining and storing different types of USACE operational data with the Corps' corporate financial data
- Storing and maintaining data used to generate performance information for all organizational levels

- Storing and maintaining data on real-time lock delays for the towing industry to manage their fleets
- Storing and maintaining waterborne commerce data for trend analysis for business projections for commodity movements
- Storing and maintaining port and dock inventory data
- Storing and maintaining hydropower and power production data
- Storing and maintaining public applications for permit data
- Storing and maintaining Joint Permits with the state government data
- Storing and maintaining plan data for towboat and shipping operation data
- Storing and maintaining national-level data for evaluating performance indicators relevant to program and project goals

J.8.3.4 Location:

OMBIL Plus data is provided from a central (HQUSACE), nationally consistent source at one time, eliminating multiple individual project submissions, reduction of workload, and of varying data submission and inconsistent formats.

OMBIL data types are:

- Agreement data (Contract, Project site organization cooperative agreement)
- Corrective action data (Citation)
- Party data (Organization, Facility, Employee, Facility organization, Assessment team person, Person)
- Assessment data (Finding, Internal assessment, External assessment, Manual assessment, Manual finding, Nonmanual finding)
- Location data (United States Congressional District, Project site congressional district, State, District, Division, Metropolitan statistical area)
- Project data (Project site)
- Contract data (Project site contract)
- Compliance (Regulatory action data)
- Product data (Turbine generator unit)
- Resource data (Waterway segment, Power plant)

J.8.4 P2 (Promis)

J.8.4.1 Description:

P2 is a corporate enterprise Web-based COTS database and software product that enables project teams to work in a virtual manner on projects through a single corporate database utilized for decision support capability, utilizing on-line analytical processing

(OLAP) tools to display USACE management information in various data views. The database (and its processing system) is a COTS database system that manages all program and project data in the U.S. Army Corps of Engineers. The database will store and maintain data that will be used for program and project scoping, developing and tracking critical path networks, assigning resource estimates, comparing estimated costs to actual costs, performing earned value analysis, and maintaining a historical record of a project. In terms of its data content, it will provide a standardized, integrated set of data to be used to develop business information to support USACE management of projects and their allocated resources.

P2 is predicated on the same data architecture concepts as CEFMS, REMIS and RMS, and OMBIL and shares data with them. It is a relational database that contains data structures that are compatible with USCAE mission-critical systems. Its databases are the Oracle relational database and the Oracle multidimensional database (data warehouse). The data it contains is designed to address capabilities for identifying and tracking project scopes, schedules, programmed amounts, costs, contracts, contract modifications and technical performance requirements for management and control of individual projects through planning, design, construction, operation and rehabilitation. In addition, the P2 database will store and maintain summary data from individual projects in support of Federal authorization and appropriations processes.

P2 transfers or shares data with most of the mission-critical systems mentioned in this document. Of particular important is the interface between P2 and CEFMS. It interfaces at various levels with multiple instances of CEFMS. The data interface and transfer are designed to significantly reduce manual entry and maintenance of work items and increase the quality of data in both CEFMS and P2. The interface with CEFMS is used to populate CEFMS with project, task and work item data in CEFMS from data initially entered in P2. This data is in a standardized format for the work item structure in CEFMS as it uses it for creating Purchase Requests and Commitments (PR&Cs). Project work items, task work items (Assets Only) and PR&Cs will be created in CEFMS that correspond to the Work Breakdown Structure (WBS), activities, and resource estimates developed in P2. Once PR&Cs are created through the P2 to CEFMS interface, CEFMS completes the data creation processes and approval actions. Actual costs in CEFMS will be returned to P2 through the interface to the corresponding WBS elements and activities.

J.8.4.2 Location:

This is a centrally located database system at the CEEIS Central Processing Center.

P2 data types are:

- WBS data
- Resource data
- Project (Schedule, Task, Assignment, Cost Estimate, Project model, Activity, Project status, Project version)
- Products and relationship data

- Budget (Project Budget)

J.8.5 RMS

J.8.5.1 Description:

The Resident Management System (RMS) is a quality management and contract administration system designed by a resident engineer to help his staff do their job. The system provides an efficient method to plan, accomplish and control contract management by integrating job-specific requirements, corporate technical knowledge, and management policies. Many of the reports produced by RMS such as pay estimates, quantity variations and modification documents, are the actual documents required and used during daily operations. In addition, a wide range of management reports has been specifically designed to help field personnel evaluate project status and identify appropriate actions.

RMS downloads CEFMS financial data, including appropriation data, authorized funding, funded work items, ordering work items, obligations, and PR&Cs, for all funding registers. RMS maintains a construction-phase CWE and all CWE elements, for each funding source.

Except for unusual cases, there should be only one RMS database for each District. Use of a single RMS database for each District is important because it helps make possible the effective electronic exchange of data between RMS and other systems. These other systems include the new procurement system, SPS, as well as CEFMS and P2, each of which has a single, District-wide database. Database maintenance/system administration for RMS is also made much easier with use of a single consolidated District-wide RMS database.

For the initial version, data will flow from RMS to P2. (Note: this presumes that the project has been loaded into P2!) This will make construction-phase information (e.g., pending modifications, awarded modifications, CWE updates, schedule information, progress, other issues) available to the P2-using project delivery team members at the District headquarters. Once the information is in P2, customers and program managers can access this construction-phase information.

Construction contract management is a very data/information intensive business. As such, RMS is an automated construction management/quality assurance database system that is PC-based, client-server oriented and designed primarily for the daily requirements of USACE field construction personnel. Its primary features include capabilities to support construction planning, contract administration, quality assurance, payments, correspondence, submittal management, safety and accident administration, modification processing, and management reporting. The database entry is through RMS and will also have fully automated single-entry data exchange/communications capabilities with CEFMS, P2 and other Corps-wide systems. Through use of specialized modules, it has the capability to exchange design, scheduling and construction.

J.8.5.2 Location:

RMS exists at the field office (contractors) and at the District offices.

RMS data types are:

- Agreement (Contract, Solicitation, Bid offer, Local cooperation agreement, Inter agency agreement, Work item agreement) data
- Authority (Program authorization) data
- Budget (Budget authorization account master, Labor payroll account, Funding account, Funding authority, General ledger, Fund, Cost account, Allotment, Appropriation, Obligation) data
- Product data
- Document (Funding authorization document location master, Transfer document, Travel order, Travel voucher) data
- Resource (Employee position, Employee training, Training course, Training session, Warehouse inventory resource) data
- Product (Equipment, Service) data
- Account (Pay period, Payee, Payment method, Billing criteria, Accounting phase, Customer order item, Invoice, Receipt voucher) data
- Location (Electronic mail, Contractor payment address, Employee address, Work item location) data
- Party (Assignee institution, Field operating activity master, Point of contact, Operating agency, Organization, Authority person, Addressee, Contractor employee, Manufacturer, Installation, Fiscal station, Financial institution, Employee, Customer, Department, Bargaining unit, Work item organization, Attorney) data
- Property (Personal property, Real property) data
- Guidance (Policy) data
- Agreement (Procurement order master) data
- Program data
- Project (Task, Milestone, Work item milestone, Labor charge, Work breakdown element, Work categorization, Work categorization component, Work directive item, Work item, Work phase, Work phase status) data
- Event (Superfund event) data

J.8.6 FEMS

J.8.6.1 Description:

FEMS is a COTS and GOTS product used by USACE for effective equipment maintenance. It combines database and application systems as a maintenance function

that combines people, processes, data and communications in the maintenance of the USACE equipment inventory. For FEMS, “equipment” includes everything that must be maintained (e.g., facilities, large and small pieces of equipment, buildings, grounds, river banks, dikes, revetments, roofs and walls, lock chambers and navigation channels).

FEMS is a COTS application and database system that is used by each service (Army, Navy, and Air Force) to fulfill each of their unique mission requirements by integrating a number of plant maintenance functions into a coherent maintenance management program.

J.8.6.2 Interfaces and Data Transfer:

FEMS interfaces with the CEFMS. Wherever possible the interface will be accomplished using database links. However, there will be some cases where the data will not be updated real time. In these cases, data will be stored and a database link will be established periodically to update data on the other system(s). FEM will utilize its standard interface infrastructure applications to control the physical transmission of data to and from CEFMS databases. It connects to the CEFMS database through the Interface Information (INTINFO) application.

The INTINFO interface uses FEM database log table(s) to serve as a transaction history and process control mechanism for data going in both directions. Data being sent to or received from another database will be first placed in a log table and then processed. For outgoing data from FEM, FEM will put data in a log table based on actions on other FEM tables. FEM will send data from log tables in FEM to the log tables in the CEFMS databases. CEFMS will process data in the log tables and update the appropriate CEFMS tables.

For selected incoming data to FEM, CEFMS will place data in FEM log tables and FEM will update the appropriate FEM tables. In other cases, FEM will access CEFMS tables directly and pull the required data. The paragraphs below describe each of the major interface processes between FEM and CEFMS Purchase Request data (materials and services data) input into the FEMS database for specific line item data for that request. This data is passed to the CEFMS system via the interfaces applications mentioned above. From these documents, the CEFMS database system constructs PR&Cs whose data are then approved, certified and obligated. At the completion of this process, the CEFMS database system sends the Purchase Order, along with Vendor data, to the FEMS database for updating. When the purchase items are received, Purchase Receipt data is input into CEFMS who transfer it to FEMS via the interfaces.

FEMS Data Types:

Data included in FEMS includes, but is not limited to:

- Capital depreciation data
- Equipment preventative and corrective maintenance data
- Equipment installation data

- Facility modification data
- Equipment calibration data
- Inventory data
- Property budget data
- Maintenance budget data
- Asset catalog classification data
- Equipment data
- Equipment hierarchy data
- Operating location data
- Location data

J.8.7 CWMS

J.8.7.1 Description:

The Corps Water Management System (CWMS) database system is a modernization of the data and data management used by applications that support USACE decision-support analysis, and information dissemination associated with the Corps water resources water control management mission. The data in this database CWMS directly supports all Corps water resources management decision-making processes related to reservoir regulation, flood control, hydropower, navigation, water quality, water supply, environmental, recreation, irrigation, fish and wildlife and other project related water resources. As the data acquisition, storage, maintenance and data management repository associated with the CWMS application system, it supports modeling and decision making in the course of regulating more than 500 dam and reservoir projects. The CWMS is an enterprise, nationwide integrated database and a completely integrated system spanning data, hardware and software that allows user access to virtually any data and information in the database associated with water management.

Customer-users of CWMS are the 400 to 500 water control management technical staff of the Corps. Customer-consumers of the information managed and served by CWMS for other agency and public use are the myriad other Federal and non-Federal agencies, utilities and water vendors, navigation interests, and the public, numbering in the several thousands during normal hydrometeorology conditions, rising to tens of thousands during emergency flood or low-flow hydrometeorology events.

CWMS will provide reservoir project status of water level, releases, and river system stages for existing and forecast operations to ENGLink. CWMS output is formatted to ENGLink requirements.

The Corps is modernizing the CWMS database system through an effort that includes the following components: data acquisition and validation; database; data

dissemination; forecasting and decision support modeling; and control and visualization interfaces.

Types of incoming real-time data include:

- River stage data
- Reservoir elevation data
- Gage precipitation data
- WSR-88D spatial precipitation data
- Quantitative precipitation forecasts (QPF) data
- Hydrometeorological parameter data

These data are used to derive the hydrologic response throughout a watershed area, including short-term future reservoir inflows and local uncontrolled downstream flows. CWMS is deployed to operate 24/7 in each of the Corps District/Division offices (41) with water control management responsibilities. This project modernizes to a standard suite of software and workstations, a prior loosely coordinated system “Water Control Data System.”

CWMS supports the President’s Management Agenda “Expanded Electronic Government,” specifically addressing the goal: “Share information more quickly and conveniently between the Federal and state, local, and tribal governments,” CWMS provides Web-based, Internet-accessible standardized water management information of riverflows, stages, and reservoir operation plans. CWMS outputs have been designed for joint exchange and use among Federal agencies, including the National Weather Service, U.S. Bureau of Reclamation, U.S. Geological Survey, Tennessee Valley Authority, and several other Federal agencies.

J.8.7.2 Location:

CWMS is deployed to operate 24/7 in each of the Corps District/Division offices (41).

CMWS data types are:

- CWMS name data
- CWMS ts spec data
- Budget (Funding) data
- Project (Gage, Gage parameter, Time series value, Rt interval, Rt parameter, Rt duration, Rt parameter type) data
- Party (Office, Rt physical element) data
- Location (Physical location, Point location, Rt county, Rt state, Rt time zone) data
- Resource (Rt cbt name, Rt class code) data
- Product (Rt equipment) data

- Rt goes name data
- Rt nws hb5 name data
- Rt shef name data
- Rt unit data
- Rt usgs name data
- St valid value data

J.8.8 ENGLink

J.8.8.1 Description:

Initially, event data about each particular disaster was not collected into a central repository for logistics management purposes, post-event analysis, or need-forecasting purposes. The ENGLink data system (Web-enabled information presentation) provides information for performing real-time Command and Control/logistics management during USACE's response to civil or military disasters/emergencies (excluding war). This system also provides the data for disaster or "element interest" data analysis, USACE performance measurement and the forecasting of staff and supply needs in response to particular types of emergencies. The ENGLink database itself has been further protected against data loss through the implementation of the physical standby database (Dataguard). ENGLink data are available for processing for the following purposes:

- Stores and maintains data for reporting on missions, events and Situation data.
- Stores and maintains data on schedules and tracks personnel and equipment during the period of disaster response.
- Stores and maintains data event information.
- Stores and maintains data for GIS and provides maps, location queries, models, geographical analysis.
- Stores and maintains data for status tracking of projects, rosters, and communications equipment.
- Stores and maintains data for training and allows remotely located personnel.
- Stores and maintains data for a library that contains plans, guidance, and other documents.
- Is a data warehouse that stores and maintains data for historical data on past emergencies and associated USACE performance metrics, resources deployed, etc.

Accessibility to this data is Web-based and real-time for critical information. Data entered represents a single data entry point that standardizes and integrates methods of data collecting, analysis, forecasting and presentation.

J.8.8.2 Location:

ENGLink data types are:

- Goods & service requirements data
- Staff deployment data
- Staff training data
- Logistics management data
- Water flow data
- Flood condition data
- Emergency activity data
- Disaster cost data
- Disaster expenditure data
- Disaster cost estimate data
- Disaster response support data
- Disaster modeling data

J.8.9 Geospatial Data

J.8.9.1 Description:

Geospatial tabular data, which is an all-encompassing term that refers to data, referenced (directly or indirectly) to a location on the earth and the systems that generate and process the data. Systems that employ geospatial data include GIS, Land Information Systems (LIS), Remote Sensing or Image Processing Systems, Computer-Aided Design and Drafting (CADD) systems, Automated Mapping/Facilities Management (AM/FM) Systems, and other computer systems that employ or reference data using either absolute, relative or assumed coordinates such as hydrographic surveying systems. The process and linkages of the geospatial databases to REMIS are as follows:

- Generates a Spatial Data Standards- (SDS-) compliant personal cadastre real estate geodatabase.
- Generates SDS-compliant cadastre real estate tables, relationships between tables, and domain values within the geodatabase.
- Adds the geographic features (e.g., tracts, outgrant boundaries, disposal boundaries, encroachment boundaries, and fee boundaries) from existing ArcInfo shape files or coverages to the geodatabase.
- Links the geodatabase to the REMIS Oracle database to retrieve the appropriate records to populate the SDS-compliant cadastre real estate tables in the personal geodatabase. This tool provides a one-way link to REMIS; it does not

make changes, updates, or deletions to the REMIS database. REMIS users will continue to enter and modify data using the existing REMIS interface.

- Allows the user to manually input attribute data into the tables (e.g., for attributes that are not in the REMIS database or are not populated in the REMIS database).
- Populates the area and perimeter attributes based on the geospatial data.
- Adds the geographic features (e.g., tracts, outgrant boundaries, disposal boundaries, encroachment boundaries, and fee boundaries) from existing ArcInfo shape files or coverages to the geodatabase.
- Populate the Cadastre Geodatabase with GIS Geospatial Data.

J.8.9.2 A Cadastre Real Estate GIS Database Design

The Cadastre Real Estate GIS database design was developed to be part of an Enterprise GIS implementation. Figure J.7 illustrates the components considered in the database design, which addresses the needs of not only the Corps' Real Estate Division, but of all business programs that utilize cadastral real estate data. The activities that are conducted by the business programs, such as Navigation, Flood Control, and Real Estate, determine the geospatial and tabular data included in the database design. The geospatial and tabular data must use a spatial data standard to provide uniformity among offices. The SDS is the Corps of Engineers official spatial data standard.

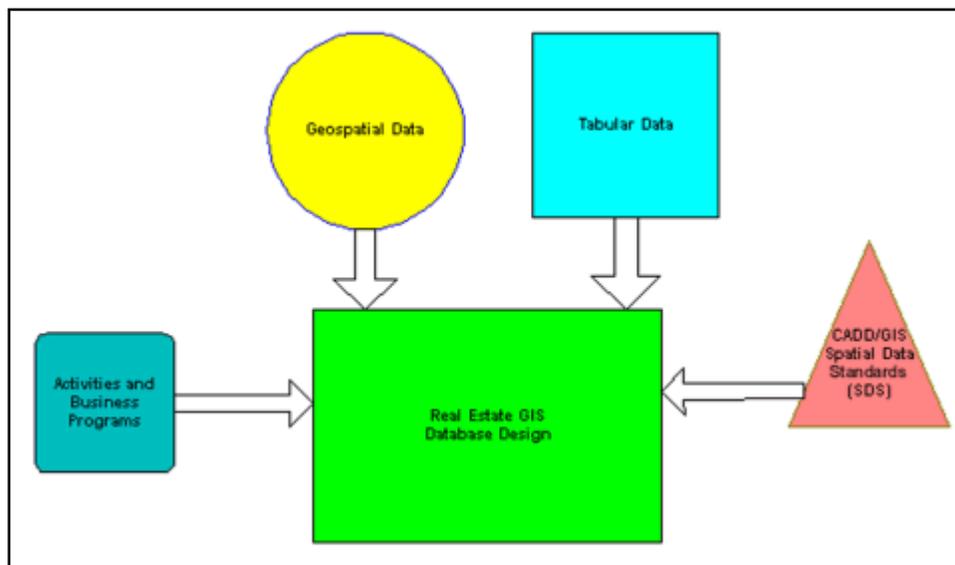


Figure J.7. Components considered when developing the Cadastre Real Estate GIS database design

J.8.9.3 Business Programs

The Real Estate GIS database design was developed by examining the needs of all business practices within the Corps that utilize real estate data developed the Real Estate GIS database design. Input from Corps Project, District, Division, and Headquarters offices was solicited through workshops, e-mail distributions, and focus groups. A real estate GIS needs assessment report developed for the Rock Island District was also utilized (Stanley Consultants 1999). The intent was to develop a design that would address the needs of most programs and users by determining the theme and attributes needed to describe the real estate cadastral data.

J.8.9.3 Real Estate Geospatial and Tabular Data

The database incorporates both geospatial and tabular data (Figure J.8). Geospatial features are geographically referenced to a real-world location (the spatial part of the database). Each geospatial feature has an "attached" attribute table containing pertinent data (the tabular or nonspatial part of the database). NOTE: Geospatial information was extracted from <http://el.erdc.usace.army.mil/gdaf/realestate/tables.html>

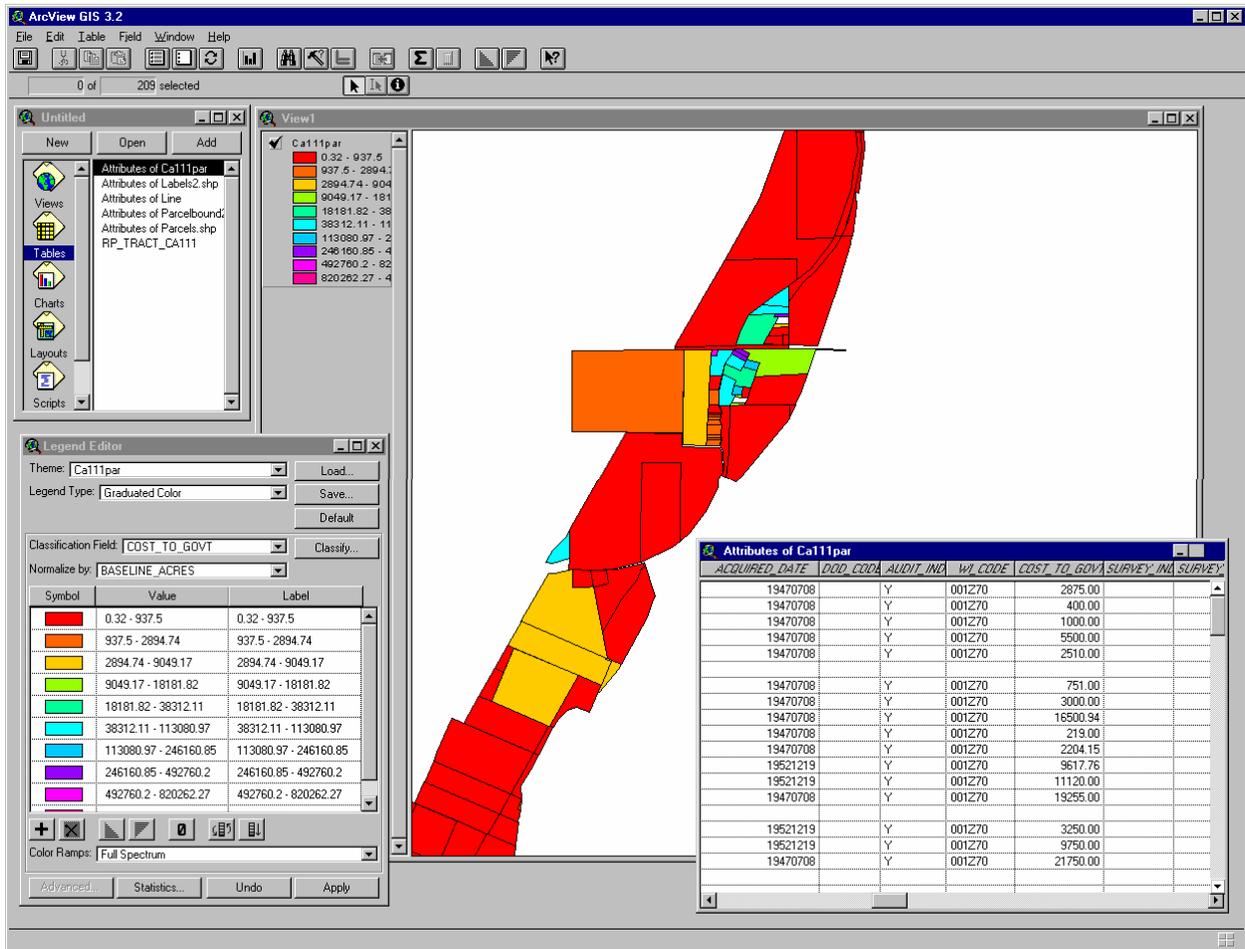


Figure J.8. Sample view of the database, showing the geospatial and tabular data

Geospatial data types and SDS tables are:

- Acquisition Fee and Less-Than-Fee Tracts
- Out grants
- Disposals
- Encroachments
- Fee Boundaries
- Deed Information

Appendix K – Description of the Data Sharing Framework

K.1 Data Sources

At the base of the Data Sharing Framework (DSF) is the Data Source layer (Figure K.1), which includes the basic raw data that USACE applications require, such as Oracle databases, Excel tables, binary files, or image files. These sources are stored and maintained in varying formats on distributed servers within many different organizations and are governed by intraagency security, management, and infrastructure policies and constraints within their native environments. Other Government organizations such as USGS, NOAA, and EPA maintain data commonly used by USACE applications. Commercial vendors such as ESRI, Pixxures, and ICubed provide access to data required by USACE applications on a subscription basis.

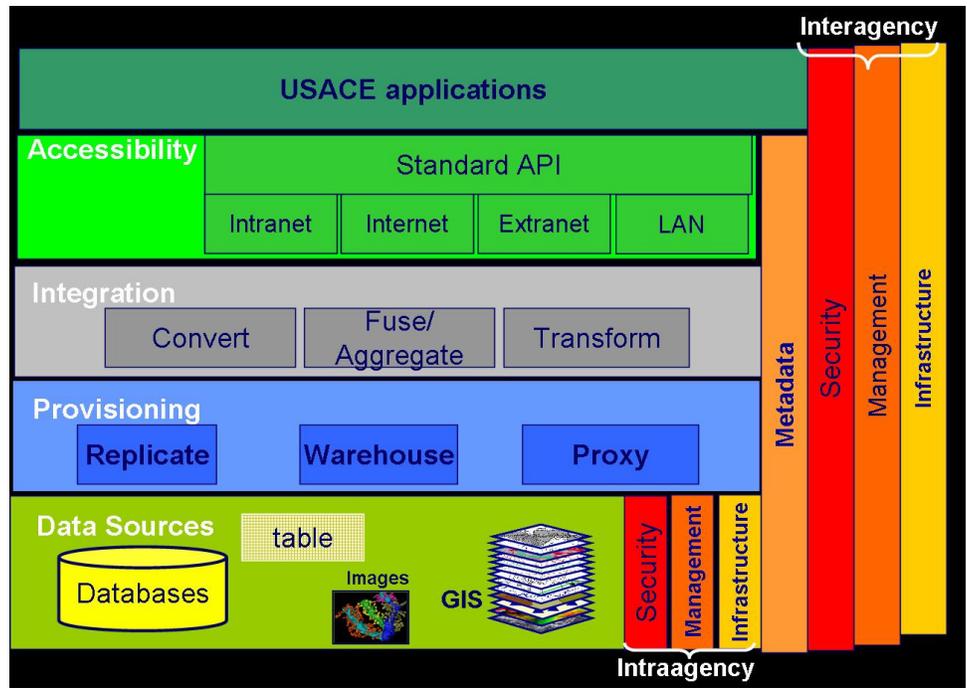


Figure K.1. Common Delivery Framework

USACE applications often share common data requirements, although in inconsistent formats. Examples of data requirements include financial data, environmental data, hydrologic data, meteorologic data, infrastructure data, topographic data, property data, etc. This document provides a categorization of commonly used data, descriptions of data sources by category, and mechanisms for accessing each data source. The

categories are based on the application (service) types defined in the Service Component Reference Model (SRM) of the **CeA**.

K.2 Provisioning

At the Provisioning level (Figure K.1), individual data sources are prepared for delivery to distributed applications. The DSF supports three approaches to provisioning: replicating the data source on an in-house server, warehousing specific data sources on an in-house server, and providing a proxy mechanism for direct delivery of the data from the source.

K.2.1 Data Replication

Replication involves the physical copying of the data from one data source to another. When direct programmatic access to a required external data source is unavailable, or if the data must be available 24/7, the data source can be replicated on an in-house server. This approach requires a plan for periodic updates of the data source, as well as software and hardware maintenance. The primary advantage of this approach is that USACE applications are not dependent on other agencies' data access strategies; however, USACE incurs the cost of maintaining copies of their data.

K.2.2 Data Warehousing

A Data Warehouse is an enterprisewide repository that replicates data from publication tables on different servers/platforms to a single subscription table. This implementation effectively consolidates data from multiple sources. Data are extracted from heterogeneous sources and translated to required formats, and the resulting data is loaded into tables within the data warehouse. Automated data staging tools facilitate the data extract, and manage data transformation, data merging, and aggregation. Warehousing requires a plan for periodic updates of the data sources, as well as software and hardware maintenance. The primary advantage is that USACE is not dependent of other agencies' data access strategies. The main disadvantage is that USACE incurs the cost of maintaining copies of other agencies' data and/or duplicate copies of USACE data sources.

The USACE CorpsMap database is an example of a warehouse approach to data provisioning. The CorpsMap geospatial database, which resides on a USACE Central Processing Center server, includes a comprehensive nationwide base map consisting of numerous data layers such as GDT Dynamap, USGS National Map, USACE Navigation Data Center Data layers, and many others.

K.2.3 Data Proxy

The proxy approach involves the introduction of a proxy component which acts as an intermediary between USACE applications and data sources. The proxy effectively hides the details of the data location, encoding schemes, and communication protocols from the client application. Web services will be used to implement the proxy approach. A Web service provides a single point of programmatic access to data sources for use

by multiple applications. Web service implementation guidelines are provided in the Technical Architecture. Although a Web service may be developed and maintained by USACE, the data it delivers is stored and maintained by the agency that owns the data. In cases where a Web service delivers data from external sources, Service Level Agreements (SLA) must be established with other agencies to ensure the availability, stability, and performance of the data services within specified constraints.

The Common Delivery Framework (CDF) provides a Web Service Registry of available USACE Web services. Access to the Registry is controlled by user-id/password login at <https://cdfportal.usace.army.mil>. Currently, fourteen data services are registered and available for use:

1. Meso West Surface Conditions Service
2. METAR Surface Conditions Service
3. NCDC-NOAA Historic Monthly Precipitation Data Service
4. NOAA Estuarine Bathymetry Data Service
5. USGS National Elevation Data (NED) Service
6. EPA STORET data service
7. NOAA Tidal Data Service
8. USGS Historic Stream Flow Service
9. USGS Real Time Stream Flow Service
10. National Inventory of Dams Data Service
11. USGS National Land Cover Dataset Service
12. USDA STATSGO Data Service
13. USGS Space Shuttle Radar Topographic Map Service
14. ESRI ArcWeb Services

K.3 Integration

Data sources vary significantly in format, structure, and content; therefore, some level of preprocessing is needed to properly adapt the data for its most effective use. The Integration layer (Figure K.1) provides mechanisms for tailoring data to meet the needs of specific applications, such as data aggregation or fusion services, coordinating conversion services, subsetting services, or format conversion services.

K.3.1 Data Conversion

Data conversion refers to the act of changing the format of a specific data source to accommodate the required data format of a specific application.

K.3.2 Data Fusion

Data fusion refers to the use of techniques that combine data from multiple sources and gather that information in order to achieve inferences, which will be more efficient than if they were achieved by means of a single data source.

K.3.3 Data Aggregation

Data aggregation involves the gathering of individual data sources into a single access mechanism. Common aggregation mechanisms include:

- Aggregation Web Service - acts as a proxy service for locating and consuming other Web services listed in the Data Proxy section.

K.4 Accessibility

The Accessibility layer (Figure K.1) defines the network gateways and the interface information necessary for application developers to access data sources via the DSF. Data sources are connected to the DSF by publicly accessible Internet gateways, a publicly accessible but restricted Extranet gateway, an internally accessible Intranet gateway, as well as local area networks. Application Programming Interfaces (API) provide a set of routines, protocols, and tools that application developers use to access DSF data. Thus, one consistent set of data access tools is developed and provided to application developers to access specific data sources.

All of the Web services available via the DSF are currently operating on the USACE Web Farm via Extranet gateways currently restricted to .mil and .gov users.

K.4.1 Application Program Interface

An API is a series of software routines and development tools that compose an interface between a computer application and lower-level services and functions (e.g. the operating system, device drivers, and other low-level software). APIs serve as building blocks for programmers putting together software applications. In the context of the DSF, an API provides a consistent set of data access functions that applications can call to acquire data. It allows application developers to access data without having intimate knowledge of the details of the data format. Thus, application development is faster and more consistent. Also, as data formats change, the API can be updated once to reflect that change, instead of updating every application that accesses the data. Development of an API is recommended to expedite input/output of data formats for which an industry-supported API does not exist, such as the eXtensible Model Data Format (XMDF) and the Data Storage System (DSS).

K.4.2 Internet

The Internet refers the worldwide network of computer networks that use the TCP/IP protocols to facilitate data transmission and exchange. Data sources and access mechanisms whose audience is the general public should use the Internet gateway. Technical details of the USACE Internet gateway are provided in the **CeA-TRM**.

K.4.3 Intranet.

The Intranet refers to a computer network that is restricted to a specific group of users. Data sources and access mechanisms whose intended audience is restricted to an internal group of users should use the Intranet gateway. Technical details of the USACE Intranet gateway are provided in the **CeA-TRM**.

K.4.4 Extranet.

The Extranet refers to the extension of an organization's Intranet out onto the Internet, that is to allow selected users to access the organization's private data and applications via the World Wide Web. Data sources and access mechanisms whose intended audience includes other partnering organizations outside of USACE, such as USGS or EPA, should use the Extranet gateway. Technical details of the USACE Extranet gateway are provided in the **CeA-TRM**.

K.4.5 LAN.

A local area network (LAN) refers to a local computer network for communication between computers, such as a network connecting computers and word processors and other electronic office equipment to create a communication system between offices. Data sources and access mechanisms whose intended audience includes a small group of users within close geographic proximity should use a LAN. Technical details of LANs are provided in the **CeA-TRM**.

K.5 Metadata

Metadata is required to describe data content, format, and access methods. According to the Defense Discovery Metadata Specification (DDMS), metadata standards are required to support the net-centric goals of data visibility, which depend on the ability of users and systems to find and access a wide range of data assets through a consistent and flexible search, or discovery capability. The term data asset refers to any entity that is composed of data, including services that provide access to data. A common specification for the description of data assets supports a comprehensive capability that can locate all data assets across the Enterprise regardless of format, type, location, or classification.

Common metadata standards:

- The Federal Geographic Data Committee (FGDC) Metadata standard is the approved content standard for digital geospatial metadata. It provides a common set of terminology and definitions for geospatial data elements including content, quality, condition, and other characteristics.
<http://www.fgdc.gov/metadata/metadata.html>
- Defense Discovery Metadata Specification (DDMS) defines discovery metadata elements for resources posted to community and organizational shared spaces. The DDMS specifies a core set of information fields that are to be used to describe any data or service asset that is made visible to the Enterprise. The

DDMS will be employed consistently across the Department's disciplines, domains and data formats. <http://diides.ncr.disa.mil/mdreg/user/DDMS.cfm>

- UDDI (Universal Description, Discovery, and Integration) is a standard metadata specification for distributed Web-based information registries of Web Services. UDDI registries are used to promote and discover distributed Web services. Designed to assist software developers in finding available services, it contains all the information necessary to describe a service, how it is used, and where it is located. <http://www.uddi.org/specification.html>
- WSDL (Web Services Description Language), a standard metadata specification for describing Web services based on eXtensible Markup Language (XML), contains all of the information needed to interact with a Simple Object Access Protocol (SOAP) service, such as input parameters, type, and number for method input, as well as the output parameters, type and number for method output. It also contains the URL address of the SOAP service, and the SOAP encoding scheme that is used. <http://www.w3.org/2002/ws/desc/>

K.6 Security

Security issues pervade every layer of the DSF. The security measures imposed on the DSF must be able to interoperate with the varying levels of security associated with individual data sources, especially external sources. If we think of the DSF as a collection of nodes that represent common access to data, with links between those nodes representing network connections, the primary security issues deal with controlling access to the various nodes. Three methods of access control defined in the DSF are network gateways, encryption, and authentication.

K.6.1 Network Gateways.

One method of access control is performed through the selection of network gateways (Internet, Extranet, Intranet, LAN). Since the DSF operates on a collection of network servers homed to one of two Internet gateways, the Corps of Engineers Enterprise Infrastructure Services (CEEIS) Internet gateway or the Defense Research and Engineering Network (DREN) gateway, security measures are well-defined for those gateways. Security devices, including gateway router, stateful firewall, VPN concentrator, intrusion detection devices, site intrusion detection devices and site firewalls, are monitored 24/7. Access to the USACE computer resources is limited to users who have a valid requirement, through the use of hardened passwords and permissions. Information Assurance Vulnerability Alerts are monitored by HQ USACE and Department of the Army for strict compliance. To filter hostile traffic, virus packages from Antigen, Norton and McAfee are used. Routine hardware/software upgrades, backups, and monitoring of usage metrics are provided.

K.6.2 Encryption.

A second required security measure for Web applications involves the use of Secure Sockets Layer (SSL) encryption. The DSF requires the use of SSL encryption to ensure

that all traffic, including user-ids and passwords, is encrypted as it passes between the client application and the server.

K.6.3 Authentication.

All applications that interface with the DSF are required to go through an authentication process. This is the first line of defense to manage access to the DSF as well as control the use of computational and networking resources. Authentication is the process of assuring that someone is who they say they are.

Common authentication mechanisms:

- CDF Authentication Web Service - provides a standard method for controlling access to specific components of the DSF. The service authenticates based on a set of authentication sources, which are managed sets of user-ids and passwords. Once users (a user can be a person or an application) are authenticated, access rights to specific DSF components are defined through the use of user communities and profiles.

Available Authentication Sources:

- Corps User-Id and Password System (U-PASS)
- Army Knowledge Online (AKO) user-id and password system.
- Common Access Cards (CAC). As the DoD continues the issuance of CACs, the DSF will extend the authentication service to include the CAC as an authentication source. This will increase security by ensuring that the user actually has in his or her possession a DoD-issued CAC and associated digital certificates.

K.7 Management

The Management layer encompasses those activities that control the maintenance of components within the DSF as well as processes associated with it, such as standards, service level agreements, change control, and monitoring of components. A network-based framework for data delivery demands a managed process to ensure quality of service. We must be prepared to manage the assimilation of ever-changing technology into our business process. Standards, which govern data content and format as well as data transfer protocols, provide the basis for storing and delivering data from disparate sources.

K.7.1 Data Standards.

Data standards govern data content, format and transfer protocols. The following standards are recommended for use by all USACE data managers.

K.7.2 Data content standards:

- Spatial Data Standard for Facilities, Infrastructure, and Environment (SDSFIE) is the required standard for geospatial data.
<https://tsc.wes.army.mil/products/TSSDS-TSFMS/tssds/html/>
- Architectural/Engineering/Construction Computer-Aided Design and Drafting (A/E/C CADD) Standard is the required standard for architectural, engineering, construction design data.
<https://tsc.wes.army.mil/products/standards/aec/intro.asp>

K.7.3 Data format standards:

- eXtensible Model Data Format (XMDF) is the recommended standard file format for computational modeling data. XMDF provides a fast, efficient, and simple methodology for storing, accessing, and sharing data used in numerical simulation. <http://www.wes.army.mil/ITL/XMDF/>

K.7.4 Web Services Standards.

All DSF Web services were developed according to the World Wide Web Consortium (W3C) standards including:

- *XML* – XML is designed to improve the functionality of the Web by providing more flexible and adaptable information identification. It is called extensible because it is not a fixed format like HTML (a single, predefined markup language). Instead, XML is actually a metalanguage—a language for describing other languages—which lets you design your own customized markup languages for limitless different types of documents.
- *SOAP* – SOAP uses a combination of XML-based data structuring and the Hyper Text Transfer Protocol (HTTP) to define a standardized method for invoking methods in objects distributed in diverse operating environments across the Internet. Client applications make remote procedure calls to SOAP “services,” which are basically code libraries/objects with exposed methods. According to the W3C specification, SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML-based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses.
- *WSDL* – WSDL is a specification for describing Web services based on XML. A WSDL file contains all of the information needed to interact with a SOAP service, such as input parameters, type, and number for method input, as well as the output parameters, type and number for method output. It also contains the URL address of the SOAP service, and the SOAP encoding scheme that is used. The WSDL file serves as a contract between the client application and a service provider. If a service provider publishes a WSDL file for a specific service, and

the WSDL is not valid for use with the said service, then the provider is not meeting the obligations of this contract.

- *UDDI* – The UDDI is a specification for distributed Web-based information registries of Web Services. UDDI registries are used to promote and discover distributed Web services. Designed to assist software developers in finding available services, it contains all of the information necessary to describe a service, how it is used, and where it is located.

K.7.5 Service Level Agreements.

An SLA is a formal contract between a service provider and a service consumer that guarantees quantifiable network performance at defined levels. The contract outlines key performance measures, such as service availability, server response time, service repair time, service technical support, within which the service provider agrees to operate and deliver its services. An SLA should also specify exceptions in terms of failures, network issues outside the control of the service provider, denial of service, and scheduled maintenance. It is critical that SLAs are developed for the DSF services that provide access to external data sources to ensure the reliable availability of the data sources to which our services connect.

K.7.6 Monitoring.

Monitoring provides the capability to track various metrics about each DSF service, such as:

- Is the service operational?
- Who is using the service?
- When is the service most often used?
- How long does it take for the service to complete a request?
- How much data are being sent to and returned from the service?

This information is valuable for security and maintenance reasons and provides the quantification necessary to monitor SLAs.

Common monitoring functionality:

- A Usage Monitoring Service is provided as a DSF Web service and must be referenced as an object in all DSF services.

K.7.7 Configuration Management.

Configuration Management (CM) involves the tracking and control of software development and related activities, such as multiple developers working on the same code at the same time, targeting multiple platforms, supporting multiple versions, and controlling the status of code (for example beta test versus real release). While process management and control are necessary for a repeatable, optimized development

process, a solid configuration management foundation for that process is essential. The Institute of Electrical and Electronics Engineers (IEEE) provides a standard for Software CM Plans, IEEE 828-1998.

With respect to the DSF, a well-defined CM process ensures that changes/updates to data access mechanisms are properly managed and assures users that data access will be stable and consistent. Commercial tools are available to assist in performing CM. The software CM associated with the USACE corporate Web Services that provide access to multiple data sources leverages two tools: PerForce (<http://www.perforce.com>) and SourceGear Vault (<http://www.sourcegear.com/vault/index.asp>).

K.7.8 Operations and Maintenance.

Day-to-day operations and maintenance of corporate data will be the responsibility of the Web farm administrators, Central Processing Center and Western Processing Center administrators, and the data owners. Responsibilities include:

- database administration
- testing of proposed new services/databases
- updating of existing services/databases
- coordination with data owners/service providers
- technical assistance in service/database development
- hardware/software upgrades
- software backups
- usage metrics monitoring/analysis
- systems administration
- hardware/software configuration
- operating system installation and maintenance
- server/desktop end user support and technical assistance
- application support

K.7.9 Testing.

A Test Plan describes the basic functional requirements of all DSF services as well as a set of procedures for testing the services operations.

K.7.10 Technical Transfer.

The DSF is transferred to users in the following ways:

- Short (1-2 hour) seminars provide a basic overview of the DSF

- Workshops (1-2 days) include the basic overview, technical details, demonstrations, and user feedback
- Technical guidance documentation describes how to develop and consume DSF services, set up a development environment, etc.
- A Web portal provides the mechanism for organizing technical documentation, presentations, meeting minutes, related articles, services, and reusable applications/libraries.
- The DSF A-Team manages the day-to-day operations and maintenance of the Registry, the technical documentation associated with registered services, as well as technical assistance in service/application development.

Appendix L – Detailed Description of the Data Categorization

L.1 Science and Engineering Data



The interdisciplinary nature and increasing complexity of science and engineering (S&E), the environment, water resources issues, and the built environment, require the use of computerized tools/applications that can incorporate information from a broad range of scientific disciplines. These tools range from COTS software, such as Bentley MicroStation Computer-Aided Design software and ESRI ArcGIS Geographic Information Systems software, to GOTS software, such as ERDC Numerical Models (NUMMODS) and HEC Corps Water Management System (CWMS), to custom applications developed in-house for some specific purpose. Data to support the S&E environment is categorized as follows:

- Cost Engineering
- Structural Engineering
- Construction Specifications
- Design
- Hydro
- Environmental
- Infrastructure
- Climate
- Soils
- Landform
- Land Use/Vegetation
- Maps/Imagery

The following paragraphs describe specific sources and access mechanisms for S&E data.

L.1.1 Engineering

Cost Engineering data is available from the following sources:

- Computer Aided Cost Engineering System (CACES) – automated tool that assists cost engineers in preparing budgetary and detailed construction cost estimates for USACE projects

- Construction Equipment Ownership and Operating Expense Schedule – EP 1110-1-8 supports cost engineers in preparing budgets and detailed construction cost estimates for Military, Environmental, and Civil Works projects.

L.1.2 Structural Engineering

Structural Engineering data is available from the following sources:

- Pavement Computer Assisted Structural Engineering (PCASE) – a set of 35 tri-service interactive computer applications that aid engineers in the design and evaluation of transportation systems; guide users in the design and evaluation of airfields, roads and railroads according to the Unified Facilities Criteria. - <http://www.pcase.com>
- Computer-Aided Structural Engineering (CASE) - a set of computer-aided tools for use in the design and analysis of common Corps structures such as dams, bridges, beams, miter gates, etc. - <http://case.wes.army.mil>

L.1.3 Construction Specifications

Data related to construction specifications is available from the following sources:

- SpecsIntact (SI) – an automated specification processing system for producing and maintaining a master set of construction guide specifications and for developing project-specific specs from the SI masters. <http://specsintact.ksc.nasa.gov/>

L.1.4 Design

Data related to design is available from the following sources:

- CADD Library of Design - a Web-based system of project designs, generic details, and standard symbols - <http://cadlib.wes.army.mil/>

L.1.5 Hydro

The Hydro category includes data that describe the physical conditions, boundaries, flow, and related characteristics of the earth's waters. Hydro data is available from the following sources:

- **USGS Real Time Stream Flow.** USGS provides real-time daily stream flow data for thousands of stream/river sites across the U.S. The data are collected by automatic recorders and manual measurements at field installations across the Nation. Real-time data typically are recorded at 15- to 60-minute intervals, stored onsite, and transmitted to USGS offices every 4 hours via satellite, telephone, and/or radio. The data can be downloaded from the USGS Web site, <http://nwis.waterdata.usgs.gov/nwis/rt>. Programmatic access to the data is provided via a Common Delivery Framework (CDF) Web service at <https://cdfportal.usace.army.mil>.

- **USGS Historic Stream Flow.** USGS provides historic average daily stream flow data for thousands of stream/river sites across the U.S. The data are collected by automatic recorders and manual measurements at field installations across the Nation. Once a complete day of readings are received from a site, daily summary data are generated and stored in the database. Recent provisional daily data are updated on the Web site once a day when the computation is completed. The data can be downloaded from the USGS Web site, <http://waterdata.usgs.gov/nwis/discharge>. Programmatic access to the data is provided via a CDF Web service at <https://cdfportal.usace.army.mil>.
- **NOAA Tidal Data.** NOAA's Center for Operational Oceanographic Products and Services (CO-OPS) collects, analyzes and distributes historical and real-time observations and predictions of water levels, coastal currents, and other oceanographic data from thousands of sites throughout the U.S. The data can be downloaded from the NOAA Web site, http://co-ops.nos.noaa.gov/data_res.html. Programmatic access to the water level data in terms of 6-minute interval measurements, hourly measurements, high/low waters and daily heights is provided via a CDF Web service at <https://cdfportal.usace.army.mil>.
- **Inland Electronic Navigation Charts.** IENCs are geospatial data sets covering the Nation's inland waterways. Based on the International Hydrographic Office S-57 hydrographic data exchange standard, IENCs represent the Transportation Water Navigation layers of the Geospatial One Stop. Access to IENCs in S-57 format and in .shp file format, provided at <http://www.tec.army.mil/echarts/inlandnav/>.
- **Corps Water Management System.** CWMS provides tools and information needed to accomplish the water management mission, including reservoir and river system status monitoring, flow regulation, and decision support. CWMS facilitates access to and sharing of water management-related information among District, Division, HQUSACE staff, and staff of cooperating Federal, State, and local agencies. <http://cwms.hec.usace.army.mil/cwcinfo/cwc.html>.

L.1.6 Environmental

The Environmental category includes data that describe the physical, chemical, and/or biotic factors that influence the quality of life of an individual or community.

Environmental data is available from the following sources:

- **EPA STORET** - The EPA STORET data management system contains water quality data collected from 1999 till present, as well as archived data that has been migrated from a legacy data management system. The system includes biological, chemical, and physical data on surface and ground water collected by Federal, State, and local agencies, Indian Tribes, volunteer groups, academics, and others. Each sampling result is accompanied by information on where the sample was taken when the sample was gathered, the medium sampled, the name of the organization that sponsored the monitoring, why the data were gathered, sampling and analytical methods used, the laboratory used to analyze

the samples, the quality control checks used when sampling, handling the samples, and analyzing the data, and the personnel responsible for the data. STORET data can be downloaded via the EPA Web site, <http://www.epa.gov/storet/about.html>. Programmatic access to STORET data is provided via a CDF Web service at <https://cdfportal.usace.army.mil>.

- **Environmental Residue-Effects Database (ERED)** - The USACE/EPA ERED is a compilation of data, taken from literature, where biological effects (reduced survival, growth, etc.) and tissue contaminant concentrations were simultaneously measured in the same organism. Currently, the database is limited to those instances where biological effects observed in an organism are linked to a specific contaminant within its tissues. The database contains data from 736 studies published between 1964 and 2001, for a total of 3,463 distinct observations. ERED data can be downloaded via the USACE ERDC Web site, <http://el.ercdc.usace.army.mil/ered/index.html#misc>. Programmatic access to ERED is provided via a CDF Web service at <https://cdfportal.usace.army.mil>.
- **DOE Risk Assessment Information System (RAIS) database** - The Department of Energy sponsors the RAIS, which includes Risk-based Preliminary Remediation Goal calculations, risk calculations, toxicity database, and ecological benchmarks. The database of chemical-specific toxicity values contains the human health toxicological information needed to perform risk evaluations and assessments. The database contains information from the EPA Integrated Risk Information System, the Health Effects Assessment Summary Tables, EPA Provisional Peer Reviewed Toxicity Values database, and other information sources. RAIS toxicity data can be downloaded from the RAIS Web site, http://risk.lsd.ornl.gov/tox/tox_values.shtml. Programmatic access to the RAIS toxicity database is provided via a CDF Web service at <https://cdfportal.usace.army.mil>.
- **USACE Biota-Sediment Accumulation Factor (BSAF) database** - The BSAF database provides data for use in evaluations of the suitability of dredged sediments for disposal at open water sites in theoretical bioaccumulation potential estimations according to procedures given in the implementation manuals for regulating dredging. BSAF data can be downloaded from the USACE ERDC Web site <http://el.ercdc.usace.army.mil/bsaf/bsaf.html>. Programmatic access to the BSAF database is provided via a CDF Web service at <https://cdfportal.usace.army.mil>.

L.1.7 Infrastructure

The Infrastructure category includes data that describe USACE Civil Works structures such as dams, locks, etc. Infrastructure data is available from the following sources:

- National Inventory of Dams (NID) – USACE-maintained database of dams located in the U.S. which includes information for over 78,000 dams supplied by 17 Federal agencies and all 40 states. A CDF Web service provides programmatic access to the NID - <https://cdfportal.usace.army.mil>

- Corps of Engineers Bridge Inventory System (CEBIS) - an automated database system that includes the inventory, structural condition, and appraisal results for Corps-owned bridges.
- Digital Project Notebook (DPN) – an Internet map-based digital application that presents information on all USACE Civil Works projects; the DPN database includes project information such as name, type, purpose, status, funding amount, and location, as well as maps and photographs, referenced to a map display. Users can query projects based on geographic area, type, category class, status, funding, and/or name. <http://crunch.tec.army.mil/dpn>.

L.1.8 Climate

The Climate category includes data that describe the general state of the earth's atmosphere, including precipitation, temperature, wind, barometric pressure, etc. Climate data is available from the following sources:

- University of Utah MesoWest - a CDF Web service provides programmatic access to this data <https://cdfportal.usace.army.mil>
- METAR current surface conditions - a CDF Web service provides programmatic access to this data <https://cdfportal.usace.army.mil>
- NCDC precipitation - a CDF Web service provides programmatic access to this data <https://cdfportal.usace.army.mil>

L.1.9 Soils

The Soils category includes data that describe the unconsolidated materials above the bedrock of the earth. Soils data is available from the following sources:

- USDA STATSGO - a CDF Web service provides programmatic access to this data <https://cdfportal.usace.army.mil>.

L.1.10 Landform

The Landform category includes data that describe the visible surface of the earth's crust, including bathymetry data, hypsography data, and topography data. Landform data is available from the following sources:

- USGS National Elevation Data - a CDF Web service provides programmatic access to this data <https://cdfportal.usace.army.mil>
- NOAA Estuarine Bathymetry - a CDF Web service provides programmatic access to this data <https://cdfportal.usace.army.mil>

L.1.11 Land Use/Vegetation

The Land Use/Vegetation category includes data that describe man's use of earth's land and the plant life of the earth. Data is available from the following sources:

- USGS Land Use/LandCover - a CDF Web service provides programmatic access to this data <https://cdfportal.usace.army.mil>.

L.1.12 Maps and Imagery

The Maps and Imagery category includes graphic representations of various types of data, primarily used as background maps in USACE applications. Data sources include:

- USGS Space Shuttle Radar Topo Maps (SRTM) - a CDF Web service provides programmatic access to this data <https://cdfportal.usace.army.mil>
- ESRI ArcWeb services - available via CDF administrator
- CorpsMap – provides access to a corporate database of map layers through a Web-mapping interface.
- Base Map data – consists of over 300 layers residing within the CEEIS Central Processing Center (CPC)
- DoD Commercial Satellite Imagery Library (CSIL) – National Geospatial Agency (NGA)-managed library of commercial satellite imagery purchases within DoD; USACE participation in CSIL program allows access to imagery that has previously been purchased by DoD at no additional cost.

L.2 Real Estate Data

The Real Estate category includes data related to the appraisal, planning and control, acquisition, leasing, management, and disposal of land.

The Real Estate Management Information System (REMIS) is the USACE information system designed to provide District Real Estate offices a uniform method of recording, storing, retrieving, and reporting information related to USACE real estate transactions and activities. An Oracle database supports REMIS. REMIS supports the functional areas of work assignment, real property management, planning, appraisal, acquisition, management, disposal, accountability, cost sharing, relocation assistance, personnel management, environmental program management, mobilization, legal services and claims, solicitation, SA utility, and homeowners assistance. REMIS is developed within an Oracle relational database management system environment. The following sections describe types of data available from the REMIS database.

L.2.1 Relocation Assistance

The Relocation Assistance Program (RAP) provides the following data about displaced persons or RAP applicants and their associated application, benefits, payments, and appeals:

- RAP Displaced Person data – contains information about individuals, partnerships, corporations, and/or associations for whom the acquisition of real property by the Government (for a Government project or installation or a local cooperation project) results in displacement.

- RAP Application data – contains information about the eligibility of, and decisions relating to, an individual’s application for assistance under the RAP.
- RAP Benefits data - contains information about the amount of compensation requested by a RAP Applicant, and the compensation approved by the Corps for incidental conveyance expenses (e.g., taxes), incidental moving expenses, replacement housing expenses, or business/farm relocation expenses.
- RAP Payment data - contains information about all disbursements made by the Government to a RAP Applicant.
- RAP Appeal data - contains information about an applicant’s appeal of the Government’s decision on the applicant’s petition for relief under the RAP.

L.2.2 Real Property

Real Property data include all the various elements of real property that define or identify the characteristics of Corps-managed real property, including planning, project, tract, location, map, survey, legal description, ownership, marketable resource, and related personal property.

- Property Plan data - contains information about the process of planning a real estate project or installation.
- Tract Related Personal Property data - contains information about items of personal property, such as fixtures or equipment, which are an integral part of real property and, if removed, could significantly diminish its value.
- Civil Project/Military Installation data - contains information that describes the congressionally authorized civil project or military installation.
- Tract data - contains information describing a specific tract of land, or area, relating to a project or military installation.
- Property Location/Acreage data - contains specific information that identifies the location and acreage of real property owned or managed by the Corps.
- Map data - contains information about a map created by the Corps of Engineers that concerns some aspect of real property.
- Survey data - contains information about the boundaries and quantity of a piece of land as ascertained for project or tract purposes by a qualified land surveyor with supportive documentation.
- Legal description data - contains information about a written descriptive statement of a specific parcel of land.
- Ownership data - contains information about each individual or party who is holding or has held title to a tract of real property associated with a Corps project or military installation.

- Marketable Resources data - contains information about those elements of the land which, when extracted or separated from the land, have a value (e.g., precious metals, fossil fuels).

Real Property Accountability data includes information pertaining to the inventory of Corps-owned or Corps-managed real property, including information about signed hand receipts, and data pertaining to GSA Form 1166 and Army Form 242.

- Employee Hand Receipt data – contains information linking a Corps employee to the improvements on Government-owned real property for which the employee is accountable.

L.2.3 Management

Real Estate Management data includes information concerning the authorization of use of U.S. Government real property by an outside party.

- Outgrant data – contains information about a documented, formal agreement between the Government and a third party, whereby the Government agrees to grant the use of land to the third party for a specified purpose and period of time.
- Compliance Inspection data - contains information about inspections performed on outgrants to ascertain compliance with the terms and conditions of the outgrant.
- Utilization data - contains information concerning the periodic investigation of project lands to assure the highest and best use of Government real property according to approved plans.

L.2.4 Acquisition

Acquisition data includes information related to methods for acquiring property for Corps real estate projects and installations.

- Property Title Contract data – contains information that establishes, certifies, or ensures the title to real property owned or managed by the Corps is recorded on the Title Evidence Data record (Property Title Contract Data record).
- Temporary Permit data - contains information about an action by the Government (Corps of Engineers) to increase its interest in a tract of real property by acquiring a temporary permit to use the property.
- Lease Request to GSA data - contains information about a request by the Government (Corps of Engineers) to lease space on behalf of the Corps.
- Direct Purchase data – contains information about an action taken by the Government to increase its interest in a piece of real property and information about a real property owner's voluntary agreement with the Corps to sell a tract of land for specific valuable considerations.

- Condemnation data - contains information about litigation initiated by the Government by which real property is acquired for public use through the power of eminent domain.
- Real Property Title data - contains information that shows the lawful evidence of real property ownership, as found in official public records.
- Payment Authorization data - contains information about funds used for acquisition of real property by the Corps.
- Negotiation History data - contains information related to communications conducted in reaching a negotiated purchase settlement or agreement with the owner.

L.2.5 Appraisal

Appraisal data includes information about an opinion or estimate of the value of lands, property, or interests owned or managed by the Corps.

L.2.6 Improvement

Improvement data includes information about property improvements to buildings, facilities, structures, etc.

L.2.7 Cost Sharing

Cost Sharing data includes information that describes a civil project to be undertaken jointly between the Corps of Engineers and a local sponsor.

L.2.8 Disposal

Disposal data includes information about the disposal of real property in which the Government no longer has an interest.

L.3 Financial Data

Financial Management is supported by two Automated Information System (AIS) components: Corps of Engineers Financial Management System (CEFMS) and Corps of Engineers Enterprise Management Information System (CEEMIS). The Financial Category includes data used to manage USACE financial activities. The Corps of Engineers Financial Management System (CEFMS) is the AIS that provides all USACE financial management functionality. CEFMS data is stored in an Oracle database and is categorized as follows:

- Funding
- Commitments
- Obligations
- Expenditures/Disbursements

- Travel
- Labor/Payroll

L.4 Emergency Operations Data

USACE Emergency Preparedness and Response Program (EPRP) provides public works and engineering support during times of natural or man-made disaster. As the system for all emergency management reporting, information sharing, and emergency response, EPRP consists of two components: ENGLink Interactive and Deployable Tactical Operations Systems (DTOS). The system tracks a wide range of information, including status of disaster events, situation reporting, and available resources.

ENGLink Interactive is a Web-enabled database system that processes information for performing real-time Command and Control and logistics management during disasters or emergencies. An Oracle data warehouse supports ENGLink. Data is categorized as follows:

- Project (emergency)
- Scientific
- Financial
- Geographical/geospatial
- Personnel

L.5 Asset Management Data

The Asset Management Category includes data used to manage USACE facilities, equipment, personal property, infrastructure, and vehicles. The following sections describe the data available for asset management.

L.5.1 Facilities and Equipment

The Facilities and Equipment Maintenance System (FEMS) is the corporate AIS for managing facilities and equipment within the Corps. FEMS is a customization of the COTS Computerized Maintenance Management System, MAXIMO Enterprise Base Systems (MRO Software, Inc.). FEMS integrates several plant maintenance functions into a cost-effective asset management program, including capital depreciation, equipment preventative and corrective maintenance, equipment installation, facility modification and equipment calibration. It provides capabilities to track life cycle costs of all assets and provides a corporate standard for the maintenance business process. FEMS data is stored in an Oracle database in a server farm at the Corps of Engineers Enterprise Infrastructure Services (CEEIS) Processing Centers.

L.5.2 Personal Property

The Automated Personal Property Management System (APPMS) provides automated support for the authorization, acquisition, inventory, and disposal processes associated with personal property. APPMS is a Web-enabled application that interfaces with FEMS, the Vehicle Information Management System (VIMS) and CEFMS to manage all personal property capital assets owned or leased by USACE.

L.5.3 Infrastructure

The Asset - Infrastructure category includes data for dams, bridges, and other built environment projects. The following sources of data support infrastructure:

- The National Inventory of Dams (NID) serves as the official repository under the congressionally authorized National Dam Safety Program. NID includes information for over 78,000 dams supplied by 17 Federal agencies and all 50 states.
- The Corps of Engineers Bridge Inventory System (CEBIS) is an automated system that includes the inventory, structural condition, and appraisal results for Corps-owned bridges. CEBIS supports the Federal Highway Administration's National Bridge Inventory.
- The Digital Project Notebook (DPN) is a Web-based geo-referenced view of Corps projects, including assets associated with each project.
- CorpsMap is a Web-based Corps "atlas," providing access to geospatial resources across multiple asset repositories throughout USACE.

L.5.4 Vehicles

The Vehicle Information Management System (VIMS) provides usage and tracking for all Corps-owned and GSA rental vehicles.

L.6 Acquisition Management Data

The Acquisition Management category includes data used to manage USACE construction and engineering acquisitions. USACE maintains two corporate AIS to assist in acquisition management: the Architect/Engineer Contract Administration Support System (ACASS) and the Construction Contractor Appraisal Support System (CCASS).

- ACASS is an automated database of information on A-E firms, including performance evaluations, qualifications, and contract awards. ACASS, a DoD-wide system for which USACE is the executive agent, implements the requirements for maintaining qualification files on A-E firms in Federal Acquisition Regulation (FAR) 36.603 and for preparing and distributing performance evaluations on A-E firms in FAR 36.604. ACASS data is stored in an Oracle database.

- CCASS is an automated database of performance evaluations on construction contractors. CCASS, a DoD-wide system for which USACE is the executive agent, implements the requirements for preparing and distributing performance evaluations on construction contractors in FAR 36.201. CCASS data is stored in an Oracle database.

L.7 Business Management Data

The Business Management category includes data that supports enterprisewide project management, Civil Works Operations and Maintenance, and construction management. The following sections describe data associated with Business management.

L.7.1 Project Management

The Program/Project Management Information System (P2) is an enterprise tool that enables effective management of projects in the USACE core mission areas, Civil Works, Military, and Environmental. P2 provides structure and support that enhances the USACE project management business processes, maximizes decision support capability using a single database, and utilizes the Internet to the maximum extent possible. P2 allows USACE to develop and track work through network analysis systems using the critical path method, manage resources to the individual, resource allocation/leveling, collect and calculate performance management data, and report all project and program data to the Project Delivery Teams. P2 is server-based and comprises a suite of COTS software packages including Primavera Systems, Oracle, and Project Partners. Project information is maintained within an enterprise-level database residing within the CEEIS CPC.

L.7.2 Operations and Maintenance

The Operations & Maintenance Business Information Link Plus (OMBIL) is the USACE collector and provider of Corps Civil Works business output and performance data within the USACE business areas of navigation, hydropower, recreation, flood damage reduction, environmental stewardship and regulatory. Types of data provided by OMBIL include Civil Works Maintenance, Civil Works Operations, Command Performance Analysis, Efficiency Improvement, Environmental, Regulatory, Safety, and Waterborne Commerce Statistics. The AIS uses a data warehouse to merge financial, activity, inventory and output data to create performance measures of efficiency and effectiveness.

L.7.3 Construction Management

The Resident Management System (RMS) is a system used for construction quality management and contract administration, and helps to standardize construction business practices throughout USACE. Capabilities include pre-award construction planning including work-load forecasting, contract administration including preparation of modifications, preparation of payment estimates, correspondence preparation, scheduling of construction and updates, submittal register preparation and updating, quality assurance/control management, performance measurement, and safety program

oversight. Data-related features include the ability to enter data one time for all functions, compilation of data for various construction management reports, data exchange capability with District offices and contractors, electronic data exchange with other USACE corporate systems including P2, CEFMS, and CCASS. RMS is a client/server-based GOTS system which uses Windows, Oracle database technology, C++ language, and Citrix data access.

Appendix M – Business Reference Model



The Business Reference Model, the first component of the Federal Enterprise Architecture, is an analytical tool to help Federal agencies responsibly and accurately plan and budget for their capital investments, initially for information technology (IT). Version 2.0 provides an organized, hierarchical construct for describing the day-to-day business operations of the Federal government.

M.1 Programs

USACE programs that directly provide Service for Citizens, which includes the delivery of citizen-focused, products and services on behalf of the United States Government.

M.1.1 Civil Works

The Civil Works missions fall into four broad areas: water infrastructure, environmental management and restoration, response to natural and man-made disasters, and engineering and technical services to the Army, DoD and other Federal agencies.

Manage Civil Works Program Development and Execution. Program management develops the Civil Works Budget and supports the Major Subordinate Commands in resolution of project issues pending in Headquarters. Program execution is monitored and assessed, and procedures and guidance for program and project management functions are provided.

Execute Civil Works Planning, Design, Construction, Operations, and Maintenance. Through authorities related to navigation, the Corps plans, develops, and constructs new navigation channels, locks and dams, inland waterways, ports, and harbors through river deepening, channel widening, jetty construction, lock expansion, dam operations, and dredged material disposal activities.

Navigation. The Navigation Program is responsible for providing safe, reliable, efficient, and environmentally sustainable waterborne transportation systems for the movement of commercial goods, for national security needs, and for recreation.

Recreation. This program provides a safe and healthful outdoor recreation environment for present and future customers and the Corps workforce in an effective and efficient manner as an ancillary benefit of flood prevention and navigation projects.

Emergency Response. This program provides rapid, effective, efficient all-hazards response. It ensures effective and efficient long-term recovery with emphasis on the Nation's water resources infrastructure and reduces risks to critical water resources infrastructure. The water resources infrastructure provided by the Corps supports

homeland security and the swift return to normalcy from devastating natural disasters.

Environmental Restoration. This program remediates and restores the Nation's water and land resources within watersheds and coastal zones using an analytic framework that balances human needs with those of nature. The Corps' Environmental Protection, Restoration, and Management Program emphasizes environmental stewardship, ecosystem restoration, mitigation, environmental compliance, and research and development.

Water Supply. Careful management of the Nation's water supply is critical to limiting water shortages and lessening the impact of droughts. The Civil Works Program has the authority for water supply as part of projects that serve navigation, flood protection, and hydroelectric purposes.

Regulatory. The Civil Works Regulatory Program acts as a steward of lands and waters managed by the Corps by balancing aquatic ecosystems with allowing reasonable use of private property and infrastructure development. The Regulatory Program is responsible for issuing permits for construction and dredging in the Nation's navigable waters, including wetlands.

Support for Others. Through the Support for Others Program, the Corps provides reimbursable technical assistance and management expertise to Indian Nations, the DoD, other Federal agencies, State and local governments, private U.S. firms, and foreign nations to complement their expertise.

Special Emphasis: Homeland Security. The USACE Homeland Security Office is responsible for USACE civil emergency management and critical infrastructure protection programs.

Hydropower. This program maintains a high degree of hydroelectric generation unit availability at Corps multipurpose projects as an additional benefit of projects built for navigation and flood control.

Flood and Coastal Storm Damage Reduction. This program is aimed at saving lives in the event of floods and storms and reducing the property damage they cause. Flood protection authorities provide for dams and related hydropower construction and operation, levee construction, large-scale pumping systems, and the protection and stabilization of shorelines through beach replenishment.

M.1.2 Military Program

The Military Programs mission is to provide engineering, construction, and environmental management services for the Army, Air Force, other assigned U.S. Government agencies, and foreign governments.

Environmental Restoration. Environmental Restoration prevents or minimizes environmental damage that may have occurred as the result of the military's realistic

training requirements. It also restores areas that have been contaminated by hazardous or radioactive waste or munitions. The programs help protect public health and safety by helping installations comply with applicable Federal and State regulations and by seeking innovative solutions to environmental problems.

Military Construction. Today the Corps contributes to the defense mission and the Army vision by building Communities of Excellence from which Army power can be projected worldwide, including such structures as ranges and other training facilities, barracks, dining halls, hospitals, and workplaces and quality-of-life facilities such as recreation centers, commissaries and exchanges.

Installation Support. The mission of the Installation Support Division, a Headquarters element of the US Army Corps of Engineers, is to provide Headquarters USACE staff support and direct real property facilities management and installation support activities for the Directorate of Military Programs, and perform related services for the Army and the Assistant Chief of Staff for Installation Management. Installation Support Division personnel work on behalf of installations to ensure that key technical services provided by USACE have the right policy and program backup. This includes everything from master planning to business processes to engineering operations and even to the Public Works Digest.

Warfighter Engineering Support. The Army Vision calls for transforming the current “Legacy Forces” as rapidly as possible, while maintaining the war-fighting readiness of its operational units. The USACE mission is to support Army transformation through professional, cost-effective and timely engineer support across the full spectrum of operations.

Interagency and International Support. The Corps of Engineers provides engineering support to 60 non-DoD Federal agencies, States, and local governments under the Interagency and International Support program, including toxic waste cleanup for the Environmental Protection Agency’s “Superfund” program, construction support for the Nation’s space program, and facilities for the Drug Enforcement Agency and the Immigration and Naturalization Service. The Corps also provides support to other nations, for example, water resource advice and training in South America, bridges in Bulgaria, joint earthquake research with Japan, and channel surveys for Bangladesh.

M.1.3 Real Estate

Real Estate manages the full range of real estate services (appraisal, planning and control, acquisition, management, and disposal of land) for the military and civil works activities of the Army and Air Force, and for other Federal agencies as requested.

Direct Real Estate Activities. The Corps has the necessary expertise to prepare comprehensive plans for meeting the real estate requirements of any Federal or Federally funded program or project. Our team of realty specialists, cadastral staff, appraisers, attorneys, and other Corps experts work with customers to identify the

real property interests required; evaluate alternatives and finalize site selection; prepare mapping, surveys, and legal descriptions; perform appraisals and environmental due diligence assessments; develop cost estimates and schedules; and comply with the complex legal and regulatory requirements pertaining to historic preservation, endangered species, wetlands, and a myriad of other considerations.

Perform DoD Executive Agent Duties. The Real Estate Community of Practice executes three programs for the DoD: lease all the recruiting stations for the Army, Navy, Air Force, and Marine Corps; run the Homeowners Assistance Program, which helps military and civilian Government employees whose homes lose value from a DoD base closure or realignment announcement; and assist DoD employee homeowners when they are forced to relocate.

Provide Real Estate Services for Military Contingencies. The Corps provides trained and ready real estate team members to support deployed forces and contingency operations.

Provide Real Estate Services for Natural Disaster Relief. The Corps provides trained and ready real estate team members to assist in natural disaster emergencies.

M.1.4 Research and Development

The Directorate of Research and Development (CERD), as a HQUSACE Directorate, supports the research and development efforts of the Corps of Engineers by providing strategic planning, strategic direction, and oversight; developing and maintaining national relationships; developing policy and doctrine; developing national program integration; advising the Chief of Engineers on science and technology issues; and creating conditions for USACE corporate success.

Warfighter Support. The R&D Program creates and shapes policy and performs strategic planning, direction, and oversight for research and development for the warfighters in the general areas of Battlespace Environment and Military Engineering.

Civil Works. The R&D Program provides high-quality, responsive engineering and environmental research and development support to the Nation. This Program develops innovative science and technology solutions that support navigation, flood control and storm damage reduction, infrastructure, emergency management, and environmental sustainability and management.

Installation Support and Environmental Restoration. The R&D Program provides high-quality, responsive engineering and environmental research and development support to the DoD. This Program develops innovative science and technology solutions that support facility acquisition and revitalization, installation operations, and installation environmental issues.

M.2 Support Delivery of Services

Support Functional Areas, or Support Delivery of Services, refers to the functions that provide the critical policy, programmatic and managerial underpinnings that facilitate USACE delivery of services to citizens.

M.2.1 Legal Services and Internal Review

The Legal Services System is an integrated network of Counsel offices that spans the globe. The System plays a critical role in the planning and execution of Corps projects to facilitate smooth and effective execution. Its mission is to represent Corps legal position and rights as an organization in such areas as contract law, environmental law, fiscal law, torts and admiralty claims, personnel law and EEO, just to name a few.

Internal Review. Internal Review provides reviews related to procurement, safeguarding assets, financial accounting, management controls, managing resources, compliance with laws and policies, and achieving program results.

- **Conduct Review and Analysis.** The Legal Services System counsels decision-makers and plays a critical role in the planning and execution of Corps projects by participating in the planning and design phases of Corps projects to facilitate smooth and effective execution.
- **Provide Staff Review, Internal Control and Approval.** The internal review program is developed and executed, prioritizing needs for enhancing management controls and known or suspected problems.
- **Direct Audit, Internal Review.** The primary purposes of these reviews will be to evaluate the adequacy of program direction, supervision, and staffing; review compliance with Government Auditing Standards and prescribed policies and procedures; and furnish advice and assistance in connection with any auditing, administrative or internal problems.
- **Investigation and Inspection.** Assess activities inside USACE.
- **Direct/Manage Efficiency Programs.** Chief Counsel's Task Force on the Delivery of USACE Legal Services will provide recommendations to the Chief Counsel on ways of improving the effectiveness and efficiency of the delivery of legal services throughout USACE.

Legal Services and Internal Review. The Legal Services System is an integrated network of Counsel offices that spans the globe. The System plays a critical role in the planning and execution of Corps projects to facilitate smooth and effective execution. Its mission is to represent Corps legal position and rights as an organization in such areas as contract law, environmental law, fiscal law, torts and admiralty claims, personnel law and EEO, just to name a few.

- **Conduct Review and Analysis.** The Legal Services system counsels decision makers and plays a critical role in the planning and execution of Corps projects

by participating in the planning and design phases of Corps projects to facilitate smooth and effective execution.

- **Direct and Manage Efficiency Programs.** Chief Counsel’s Task Force on the Delivery of USACE Legal Services will provide recommendations to the Chief Counsel on ways of improving the effectiveness and efficiency of the delivery of legal services throughout USACE. The Office of Internal Review serves commanders, business line managers, and support office managers with professional advice on audit, risk management, business processes, and management control issues. They perform reviews and analyses requested by management and those required by regulation or law. The internal review program is developed and executed, prioritizing needs for enhancing management controls and known or suspected problems.
- **Reviews.** These efforts involve an objective examination of evidence for the purpose of providing an independent assessment on risk management, control, or governance process for the organization.
- **Provide Policy Advice.** The Office of the Chief Counsel, Corps of Engineers Headquarters in Washington, DC, is primarily responsible for overseeing the delivery of Corps legal services worldwide through policy development, execution and guidance.
- **Liaison.** On behalf of the commander, Internal Review facilitates audits performed by external audit organizations. They may expedite the external audit process by coordinating meetings and conferences, assisting external auditors in getting to the proper officials, facilitating and staffing command replies to audit findings and recommendations, mediating disagreements between external auditors and command, and validating projected monetary savings claimed by external auditors.
- **Follow-up.** Internal Review provides the commander with reasonable assurance that corrective actions have been accomplished, that they have been taken in a timely manner, and that the actions have minimized known risks.
- **Risk Management.** Internal Review assists commanders in the assessment of risks, design and implementation of mitigating controls, and testing of control compliance.
- **Consulting and Advisory Services.** Provides advisory and related client service activities that are intended to add value and improve an organization’s operations.

M.2.2 Resource Management

The Directorate of Resource Management, a major staff component of the U.S. Army Corps of Engineers, provides valuable budget, business practices, finance and accounting, and manpower advice to commanders, staff, and customers.

Budget Preparation. The Budget and Programs Division establishes USACE budgetary policies and procedures and provides implementing guidance to staff and operating officials. The Division consolidates and submits civil works and military budgets to Office of Management and Budget and Headquarters.

Budget Execution. During execution, USACE manages and accounts for funds and manpower to carry out approved programs; monitors how well Corps activities use allocated resources to carry out approved programs; and adjusts resource requirements based on execution feedback.

Manage Resources. Budget execution applies appropriated funds to carry out approved programs. This entails apportioning, allocating and allotting funds; obligating and disbursing them; and associated reporting and review. It also involves financing unbudgeted requirements caused by changed conditions unforeseen when submitting the budget and having higher priority than the requirements from which funds have been diverted.

Budget Process Training. The Human Resource Development Steering Committee focuses on resources applied to Corps-wide training and executive development.

Budget and Resource Analysis. All programs are analyzed to include execution data, midyear review, year-end close out, and new starts; perform what-if drills to propose options for SRG review; and conduct independent horizontal and vertical analysis of program execution and accomplishment.

M.2.3 Other

These are cross-cutting business functions that support the major business areas.

Safety and Health. The Safety and Occupational Health Office provides policy, programs, technical services, and oversight related to safety and occupational health matters in support of worldwide USACE missions.

- **Policy and Programs Management.** The policy, programs, processes and approaches will be standardized through USACE to gain efficiencies and effectiveness at all level of the organization from HQ, Major Shared Commands, Centers, Districts and Field Operating Activities. Focus will be performance based versus prescriptive and simple versus complex and detailed.
- **Safety Engineering and Technical Criteria.** This factor involves the programs, processes, and approaches that integrate systems safety processes into project management to ensure the identification, ranking and assessment of hazards, identification of procedures for the elimination or control of hazards, procedures for residual risk acceptance and the collection of lessons learned throughout the life-cycle of USACE projects (planning, design, construction, operation and close-out).
- **Construction, Operations, Training and Career Program.** This program involves the programs, processes and approaches that incorporate risk

management to eliminate or reduce hazards to an acceptable level in response and military contingency operations. It determines training needs and requirements and manages the Safety and Occupational Health career program specific to interns and career progression.

- **Industrial Hygiene.** This factor involves the programs, processes and approaches for the conduct of health hazard assessments specific to the recognition, evaluation, and control of chemical, biological, and physical agent hazards that impact USACE and contractor workforces and USACE mission activities.
- **Occupational Health.** This program medically determines and documents baseline health and periodically (annual, biennial, etc.) conducts medical surveillance of designated USACE employees to determine health status specific to work-related health hazard exposures.
- **Civil Resource Conservation Program.** This program involves programs, processes, and approach to curb USACE human capital losses from accident and occupational illnesses, Government property damage losses associated with the improper application of Safety and Occupational Health procedures, and monetary losses associated with the payment of workers' compensation.
- **Environmental Restoration.** This factor involves programs, processes, and approaches that focus on the Safety and Occupational Health aspects of Hazardous, Toxic and Radioactive Waste and Ordnance and Explosives Environmental Restoration mission work including EPA Superfund, Defense Environmental Restoration Program, Formerly Used Sites Remedial Action Program (FUSRAP) and Support for Others.
- **Civil Disaster and Military Contingency.** This factor involves the processes and approaches to ensure the safety and health of USACE employees and mission activities associated with USACE Civil Disaster Response Activities and Military Contingency Operations. Focus for Civil Disaster Response is floods, fire, earthquake, hurricanes and WMD. Focus for Military Contingency Operations is Iraq and Afghanistan.

Public Affairs. The Public Affairs Office provides advice to the Commander and senior staff members on matters involving the Corps communications with the public and the media. Through its three teams - Civil Works, Military, and Command Information – it provides policy and programs information to the media, public, and members of the Corps.

Command History. The mission of the Office of History is to collect, document, interpret, and preserve the history and heritage of the U.S. Army Corps of Engineers.

- **Provide History Advice.** The mission of the Office of History is to collect, document, interpret, and preserve the history and heritage of the U.S. Army Corps of Engineers.

- **Direct Museum Activities.** The Corps does not possess a museum; however, its Office of History maintains a collection of more than ten thousand historic artifacts that document the history of the organization.
- **Provide History of USACE Projects.** The Office of History maintains histories of Corps projects on their Web site.
- **Direct, Plan and Develop USACE Historical Center.** The planning, development, and operation of the USACE historical center and museum are under HQUSACE.

Security and Law Enforcement. The purpose of this program is to strive for a safe and secure workplace, while maintaining a commitment to accomplishing the District's ongoing mission.

Commander Staff. Responsibilities include the planning and operation of the Corps.

- **Oversight.** Responsible for day-to-day operations of the Corps.
- **Strategic Initiatives.** Activities that support the out-year planning of future directions of the Corps.

M.2.4 Science and Engineering

The Directorate of Civil Works Engineering and Construction plans, directs, and manages the engineering and construction technical missions of the organization. It is the primary corporate leader in the areas of science, engineering, technology and environmental protection.

Planning. This organization serves as the authority in corporate-level engineering decision-making activities such as corporate goal setting, establishing engineering technical policy and standards and managing technical corporate programs.

Design. This organization establishes and analyzes performance goals and indicators of USACE-wide performance for the technical aspects of USACE missions. It establishes quality assurance and technical policies and guidance for construction management and acquisition of design and construction.

Engineering. This organization serves as the authority in corporate-level engineering decision-making activities such as corporate goal setting, establishing engineering technical policy and standards and managing technical corporate programs. Has principal responsibility for implementing the technical aspects of the corporate strategic plan and is responsible for the execution, policy and guidance of the technical aspects of the worldwide mission.

Construction. This organization develops engineering and construction management technical policies and guidance for new construction, facility operations, maintenance and repair. Provides USACE-wide oversight of construction and quality management responsibilities and monitors construction execution issues.

M.3 Management of Government Resources

Internal Support Functional Areas, or Management of Government Resources, encompass the activities that must be performed for USACE to operate effectively.

M.3.1 Acquisition Management

The Office of the Principal Assistant Responsible for Contracting (PARC) at Headquarters ensures that the contracting interests of the Head of Contracting Activity (HCA) and USACE are safeguarded.

Direct Procurement SADBUs Programs. The purpose of the Office of Small and Disadvantaged Business Utilization is to sustain the Corps of Engineers as a premier organization in developing small businesses and maximizing their opportunities to participate in our procurements, thereby ensuring a broad base of capable suppliers to support the Corps of Engineers mission and strengthen our Nation's economic development.

Oversee Contracting Performance. The Office of the PARC at Headquarters provides guidance, assistance, contracting automation support, training and information on acquisition-related subjects to Corps contracting offices, including the following:

- **Develop, Implement, and Monitor USACE Procurement Policies and Procedures.** They also serve Corps contracting by providing guidance, assistance, contracting automation support, training and information on acquisition related subjects to Corps contracting offices.
- **Evaluate Operations and Management of Civil and Military Contracts.** They also serve Corps contracting by providing guidance, assistance, contracting automation support, training and information on acquisition related subjects to Corps contracting offices.

M.3.2 Asset (Logistics) Management

Provide full spectrum of support from peacetime to contingency planning and response, mobilization, wartime, humanitarian operations, and disaster relief.

Develop Logistics Policy and Guidance. Provide direction, coordination and technical guidance through value-added worldwide logistics policy, plans, and programs for all command logistics functions and business processes.

Manage Logistics Inspections. Maintain control and accountability over Corps inventory assets and manage them effectively.

Develop and Manage Logistic Budget. Programming, budgeting, allocating funds, utilization, calculation of costs and reporting requirements for the Revolving Fund,

Plant Replacement Improvement Program (PRIP), project specific, and Operations and Maintenance, Other Procurement, Army (O&M, OPA).

Evaluate Operations and Management of Civil and Military Logistics Activities. Helps the Corps manage its assets and provide centralized asset visibility.

M.3.3 Human Resource Management

Establish, direct, and maintain USACE programs in labor and employee relations, human resources development, and human resources program planning and evaluation.

Manage Military Personnel. Provide policy guidance on individual and organizational development for military personnel.

Manage Civilian Personnel and Training. Provide policy guidance on individual and organizational development for civilian personnel.

Direct EEO Program. Responsible for planning, organizing, and directing the EEO and related programs.

M.3.4 Information Technology Management

Provide the vision, policy, guidance and leadership for managing information resources and information technology within the U.S. Army Corps of Engineers.

Automation Services and Systems Support. Ensure that all Information Systems (IS) programmatic decisions are based on the best value and on the total anticipated benefits that will be derived over the life of the IS or IS modernization.

Communications Services and Systems Support. Functionality and capability are provided 24/365 in a manner that remains robust, viable, and meets customer performance expectations while maintaining a secure and cost-conscious culture.

Information Assurance Program, Services and Support. Implementing procedural and materiel protective measures, developing plans and policies, and validating requirements to protect the Corps communications, computers and data.

Records Management Services. The USACE Records Management Program ensures that staffs, at all levels, have needed information in usable form, and that official business is documented.

Printing and Publications Services. Provides publishing and technology transfer services in hardcopy and electronic publication of documents.

Visual Information Services. Use of electronic desktop publishing technology to create documents for Web publishing and preparation of camera-ready copy for traditional printing; and capability of videography, graphics, and presentations.

Library Services. Retrieving and disseminating information, as well as providing access to information and resources and service.

IM/IT Administration/Management. Standard business processes for creating, storing and retrieving corporate knowledge across the enterprise in a secure manner.

Appendix N – Performance Reference Model



This is a blank appendix. It is a placeholder.

Appendix O – Service Reference Model



Service Reference Model

The SRM is a business and performance-driven, functional framework that classifies Service Components with respect to how they support business and/or performance objectives.

O.1 Back Office Services

The Back Office Services defines the set of capabilities that support the management of enterprise planning and transactional-based functions.

O.1.1 Data Management

Defines the set of capabilities that support the usage, processing and general administration of unstructured information.

Data Classification. Defines the set of capabilities that allow for the classification of data.

Data Cleansing. Defines the set of capabilities that support the removal of incorrect or unnecessary characters and data from a data source.

Data Exchange. Defines the set of capabilities that support the interchange of information between multiple systems or applications.

Data Mart. Defines the set of capabilities that support a subset of a data warehouse for a single department or function within an organization.

Data Recovery. Defines the set of capabilities that support the restoration and stabilization of data sets to a consistent, desired state.

Data Warehouse. Defines the set of capabilities that support the archiving and storage of large volumes of data.

Extraction and Transformation. Defines the set of capabilities that support the manipulation and change of data.

Loading and Archiving. Defines the set of capabilities that support the population of a data source with external data.

Meta Data Management. Defines the set of capabilities that support the maintenance and administration of data that describes data.

- **Web Service Registry.** Interface defines the capabilities of communicating, transporting, and exchanging information through a common dialogue or method.

Delivery channels provide the information to reach the intended destination, whereas interfaces allow the interaction to occur based on a predetermined framework. Access to the registry is available through the CDF Web site <https://cdf.usace.army.mil>.

o **Service Discovery**

– **Universal Description Discovery and Integration (UDDI) Version 2.0.**

Universal Description Discovery and Integration (UDDI) provides a searchable registry of XML Web Services and their associated URLs and WSDL (Web Services Description Language) pages. <http://www.uddi.org/about.html>
Service discovery defines the method in which applications, systems, or Web services are registered and discovered. A Registry of Web Services is one of the primary components of Common Delivery Framework (CDF). The CDF Service Registry, based on the UDDI specification, is a searchable registry of all services contained within the CDF. It provides the mechanism by which product line developers find available services. The Registry contains all of the information necessary to describe a service, how it is used, and where it is located.

o **Service Description/Interface**

– **Web Service Description Language (WSDL) Version 1.1.** Web Services Description Language (WSDL) is an XML based Interface Description Language for describing XML Web services and how to use them.

<http://www.w3.org/TR/wsdl>.

Service description or interface defines the method for publishing the way in which Web services or applications can be used. Web Services Description Language (WSDL) is a World Wide Web Consortium (W3C) standard specification for describing Web services based on XML. A WSDL file contains all of the information needed to interact with a Simple Object Access Protocol (SOAP) service, such as input parameters, type, and number for method input, as well as the output parameters, type, and number for method output. It also contains the URL address of the SOAP service and the SOAP encoding scheme that is used. All CDF services require a WSDL file. The WSDL also serves as a contract between the client and a service provider. If a service provider publishes a WSDL file for use with a particular service, and the WSDL is not valid for use with the said service, then the provider is not meeting the obligations of the contract. WSDL files are available for all services in the CDF Service Registry.

O.1.2 Human Resources

Defines the set of capabilities that support the recruitment and management of personnel.

O.1.3 Financial Management

Defines the set of capabilities that support the accounting practices and procedures that allow for the handling of revenues, funding and expenditures.

O.1.4 Assets/Materials Management

Defines the set of capabilities that support the acquisition, oversight and tracking of an organization's assets.

O.1.5 Development and Integration

Defines the set of capabilities that support the communication between hardware/software applications and the activities associated with deployment of software applications.

O.1.6 Human Capital/Workforce Management

Defines the set of capabilities that support the planning and supervision of an organization's personnel.

O.2 Support Services

The Support Services defines the set of cross-functional capabilities that can be leveraged independent of mission area.

O.2.1 Continuity of Operations

Many of the enterprise services are critical to the day-to-day operations of USACE. Virtually all vital information is processed in some form by computers. Hence, a key aspect in USACE must be the ability to respond to unplanned, adverse situations that may destroy, damage, degrade, or compromise information system data or computing processing capabilities so that essential operations may continue. Ensuring that this ability exists, is indeed viable, and meets business requirements is the major function of continuity of operations planning.

OMB Circular A-130 requires continuity of operations planning for every information system. This includes both contingency planning (short-term) and continuity planning (long-term) in order to rapidly and effectively deal with the potential distribution of critical mission and business functions. To avert these disruptions, or minimize their damage, developers and sponsoring organizations must take steps to develop a Continuity of Operation Plan (COOP). As part of USACE, the Corps of Engineers Enterprise Infrastructure Services (CEEIS) has documented the set of COOP services for USACE critical applications and servers. This document (CEEIS COOP plan) should be referred to by application and infrastructure developers to determine what business contingency actions are taken by CEEIS. These developers need to review the CEEIS COOP plan to determine also what CEEIS does not currently do for application COOP. Developers also need to take into account any relationships and interfaces between other applications when determining COOP needs.

Contingency Services. Contingency-oriented services provide the following operational recovery capabilities:

- Redundancy in infrastructure components such as firewalls, routers, etc.

- Circuit redundancy from separate frame carriers.
- Rerouting capabilities in the case of Internet circuit failures.
- Clustering in support of hardware failure.
- Storage Area Network (SAN) / Redundant Array Intelligent/Inexpensive Disk (RAID) devices provide redundancy and high availability in data storage.
- Backups – data are located offsite from the centers.
- 24x7x365 system administrative support.
- Alternate site (can provide for long- or short-term recovery)

Generators are capable of sustaining alternate power until normal power can be restored. Additional enterprise level details can be found in the CEEIS COOP plan.

Continuity Services. Continuity-oriented services address operational recovery issues dealing with long-term or disaster scenarios. Specifically, continuity services are as follows:

- Cold site - Coordinate with other Government agencies to leverage an operational standby facility. In the event of a disaster situation, the affected office(s) in conjunction with the software vendors reinitiate the systems within an acceptable downtime.
- Hot site — Coordinate with other Government agencies to leverage capabilities whereby systems are preloaded with the applications and supporting data.
- Redundant site — A redundant site within USACE is equipped and configured exactly like the primary site.
- Reciprocal agreement — A formal agreement is made between two organizations to back each other up.

O.2.2 Web Hosting

The Web Farm is designed to be a comprehensive Web hosting service supporting the needs of USACE and its customers. The goal of the Web Farm is to offer a centralized, consolidated Web development and Web hosting solution that is cost-shared among its supporting projects. The Web Farm can satisfy the client organizations' requirements for reliable Web hosting and Web application, Web database, and Web site development as well as a high level of server availability via the networks on which it resides. Use of the Web Farm gives clients access to high-bandwidth networks, cutting-edge technologies and experienced, well-trained Web application and database developers, while costs are reduced for local expertise (and maintenance of local expertise) as well as for the costs of purchasing, operating, and maintaining hardware, operating systems, and software.

Software Architecture

- **Windows Server 2003.** Windows 2003 Server provides server processing for applications that rely on Windows. It includes Sharepoint.
- **Windows 2000 Server.** Windows 2000 Server and Windows 2000 Advanced Server are used to provide server processing for applications that rely on Windows.

Software environments supported by the Web Farm.

Network Connectivity. Network architecture refers to the organization of Information Technology Laboratory (ITL) Web Farm network segments, the routers that direct traffic to portions of the network, the gateways that provide access to the network, the means for limiting access to and from portions of the network, the protocols allowed, and the means for monitoring network activity. Access to network resources is controlled by a PIX firewall and its rules, and an Army proxy server. The network architecture is an important element in the security of the Web Farm.

The Web Farm uses two gateways. One is to the CEEIS frame relay network; the other is to the high-speed Defense Research and Engineering Network (DREN).

The Web Farm has two tiers of network access: public and Corps-only. Each is served by specific network segments. Firewall rules control whether a network segment is public or Corps-only. Firewall rules prevent computers on the CEEIS public or Internet accessible subnet (IAS) from initiating outgoing requests.

Internet machines and applications on the IAS allow unrestricted outgoing access to the entire public. **Extranet** machines and applications on the IAS provide public access but apply their own rules to limit access by user-id and password or by domain. **Intranet** machines are on segments accessible within the Corps and may have rules that limit access within the Corps.

The CEEIS network is further protected by Corps-wide security measures. For Internet Web servers using the DREN gateway an Army-controlled proxy provides protection. A PIX server and other firewalls control access to and from the network, as well as protocols used by all Web Farm machines and network segments.

Web sites developed as products of U.S. Army Engineer Research and Development Center (ERDC) research that support customers outside of the Corps of Engineers use the DREN gateway. Web servers which support applications for internal ERDC audiences are placed on the ITL network and pass traffic between the ERDC locations via the DREN network.

- **Intranet.** Internally accessible restricted Web sites, Intranet Web sites, also make use of production systems and in some cases development systems. Development systems are used in cases where there is ongoing development of an information system application that does significant server-side processing.

Once an Intranet Web site that consists of simple HTML is in production operation, it is possible for pagemasters to modify and maintain that HTML directly on the production systems.

- **Internet.** Publicly accessible Web sites supported by the Web Farm are implemented with production systems, development systems, and Web proxy servers that operate as described in the following paragraphs.

Web (or “reverse”) Proxy Servers are set up so that they support the DNS name of a given Web site. Incoming HTTP requests first pass through the Web proxy server. When the HTTP request arrives, the proxy server responds to the request either from its locally available cached pages or by first issuing a request and receiving a response from a production server. Web proxy servers are configured to periodically check the production servers for newer versions of Web pages. The Web proxy servers use sophisticated algorithms and experience to learn how frequently page contents change on the production servers and therefore how frequently they need to check for updates. The Web proxy servers are configured as “appliances,” running stripped down operating systems with only the software and services necessary to perform the proxy function. Their primary purpose is to enhance the security of the production servers by being resistant to penetration by hackers. The Web proxy servers are located on network segments that are outside the firewalls.

Production systems contain the complete Web site being hosted. Because of the configuration of the Web proxy servers, the production systems only answer requests from the Web proxy servers. These production systems are located on network segments that are outside the firewalls.

Development systems are set up so that they contain the original copy of a Web site. It is on the development systems that content providers can write HTML pages and Web applications and run them in a test mode. When content providers are satisfied with the look and feel of their material and the functioning of their applications, they execute a process that “publishes” their information by moving a copy of their information from the development systems to the corresponding production systems. Development systems are located on network segments inside the firewalls. They push data to be published through the firewalls to the production servers.

- **Extranet.** Extranet Web sites use a system architecture similar to the Internet Web sites. The important difference is that data are often changed by users through interaction with the production systems. Extranet systems can be collaborative in nature, requiring users to update production data, whereas on Internet systems only internal pagemasters update production data. The primary purpose of the Extranet is to provide the ability to interoperate with our business partners and customers. At a minimum, applications and data served through the Extranet must be password protected and communicate through encrypted messages via an SSL connection.

Server Architecture. Server architecture refers to the organization of the physical computers on which the various types of Web systems, database servers, and applications operate. Services offered by a machine are limited to the main purpose of the machine; all nonessential services are turned off. Except for the sizing of machines based on workload, the server architecture is the same for Internet, Extranet and Intranet systems. The Web Farm potentially will support several different server architectures that will be appropriate for different customers and applications. These server architectures are described in the following paragraphs.

- **Web servers** use either HTTP or the secure HTTPS (encrypted) protocol which generally use port 80 or 443, respectively. Although it is possible to respond to both HTTP and HTTPS requests, Web Farm Web servers generally support only one of them. A single physical Web server can support multiple separate Web sites, each with its own unique name and underlying IP address. When more than one site resides on a single server, those sites are said to be running on “virtual servers.” This is invisible to Web site visitors and provides an economy of scale for the Web Farm customers. When a computer is serving virtual hosts, the directory structure is arranged to isolate files that belong to the individual customers but provide access to a single copy of shared services. Large amounts of disk space are typically provided and that disk is configured for fast access by the system. Web servers are configured with high-speed, often redundant, network interfaces.
- **Application Servers** run applications that are accessed by users through a Web interface or an application program interface (API). The application software may run on the Web server, making that computer a combination Web and application server, or the application server may run on a second, separate computer making it a dedicated application server. The application software can range from simple scripts run by the operating system to do a simple task like incrementing a hit counter, through more complicated software that varies the data sent to a user based on input provided, up to extremely complex analysis or modeling. Application servers are typically larger, more powerful computers than the Web servers, in response to the requirement for the additional processing required by the applications. Application servers are typically configured with more memory and more/faster CPUs than Web servers. Application servers may not require as much disk space as pure Web servers or database servers (described below) because their function is I/O and computation, not storage.
- **Database Servers.** Database servers are computers that typically run relational database management software. The database servers receive queries from application servers, execute those queries, and return the results to the application servers. A database server may support multiple databases and multiple application servers and is configured with multiple CPUs, large memory, and large fast-access disk storage.
- **Streaming Servers** provide output to be processed by the client as it is being sent. For example, video can be displayed and audio can be heard as soon as the transmission starts and continue while the transmission is taking place. Video

and audio files can be quite large and this “instant-on” characteristic means the customer does not need to wait for a potentially lengthy download to complete before presenting the information.

Services. General services provided through the Web Farm.

- **Monitoring Servers and Sites.** Software to monitor individual sites on the internal networks is used by the Web Farm. Web Farm Web servers are monitored 24 hours a day, 7 days a week, 365 days a year by automated systems that alert system human monitors when a system is down. These site monitors alert system administrators based on the most recently revised Web Farm-CEEIS Operators Standard Operating Procedure (SOP). System administrators will respond to these alerts within 2 hours or as described in the specific Web Farm Agreement developed with the affected customer. The person named as Web site Point of Contact (POC) or backup POC at the initialization of the Web site hosting on the Web Farm is contacted if a Web site problem occurs. These details are arranged before a Web site is loaded on the Web Farm.
- **Backups.** It is standard Web Farm procedure to back up new or updated content on each Web site daily and to back up all files each week. Database backup includes daily complete backup. Other backup scenarios are provided for sites requiring higher levels of security.
- **DNS Registration.** USACE Web sites will have domain names ending with *.usace.army.mil*. ERDC sites will have domain names ending with *.erdc.usace.army.mil*. Web sites created for non-Corps entities can have domain names as required by the funding agency and agreed to by domain name owners. Currently we run sites for the Assistant Secretary of the Army with the domain name *pmw.army.mil*. Web Farm personnel will work with Web site managers and their local DNS administrators to set up DNS registrations.
- **System Administration.** The Web Farm employs the services of highly qualified, Army-certified system administrators. The Web Farm team includes experienced specialists who are trained in their areas of specialty and maintain knowledge of the latest technologies. This enables Web Farm customers to create Web sites and Web applications without the costs associated with maintaining a high-tech staff. The Web Farm takes the responsibility for the following administrations:
 - UNIX system
 - Windows system
 - Web software
 - Oracle database
- **Usage Reporting.** The Web Farm currently makes the raw log files available for customer analysis of Web site usage. When resources permit development of this feature, the Web Farm will offer each customer a monthly report on usage

statistics for their Web sites available through a Web browser interface. The Web Farm will operate log servers where usage logs from all Web servers are stored. The log server will provide user analysis tools to produce a suite of utilization reports for each Web site hosted by the Web Farm. The specific statistics to be published will be chosen by the customer from a menu of options at the initialization of their Web site. Statistics collected on users and usage will be in accordance with DoD privacy and security restrictions.

- **Help Desk.** The Web Farm works within the ERDC Help Desk system to provide support for Webmasters. Technical operation of a Web site requires close cooperation between the developers and the systems support crew. The Web Farm Help Desk is the link that helps to keep the communications flowing between them.

Security

- **AR 25-2.** Army regulation for Information Assurance that outlines best practices to facilitate the Army's ability to adapt to changing technology or implementation guidance.

Web applications that reside on networks run by USACE, including those of the Web Farm, are expected to comply with all DoD, Army, and USACE requirements for security. Any application hosted by the Web Farm must be accredited through the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) process, by the proponent organization's designated accreditation authority (DAA), or should be covered under an interim authority to operate (IATO) while the final accreditation is being completed. A completed accreditation document is expected as soon as possible. For the purposes of Web hosting, an application is defined as any set of Web pages that employs any software technology other than standard HTML. The Web Farm staff can provide templates and assistance in producing accreditation documentation or an IATO.

- **Password Protection.** All Extranets are set up as SSL sites on servers reserved for use by Extranets (SSL previously described). Since Extranets are Web sites that restrict access to a set of users, developers of Extranet applications residing on the Web Farm will determine the method of user login required for that application. Available options include USACE U-PASS logins, CDF Authentication Service, and Remote Authentication Dial-in User System (RADIUS). All passwords used on Web Farm servers will conform with the AR 25-2/U-PASS standards.
- **Network Security.** Web Farm networks are monitored and protected by an array of firewalls, filtering routers, and intrusion detection systems. These devices provide a high degree of protection for Web Farm systems. These devices are operated by and maintained by the appropriate Information Assurance (IA) entity.

- **System Security Incidents.** Web Farm security incidents are reported to the appropriate Information Assurance Security Point of Contact as listed on the system contact list. Incidents are generally reported from the associated Computer Emergency Response Team (CERT) to the Network Security Manager for the associated network.
- **Scanning.** The IA Team and the appropriate Network Operations Security Center (NOSC) in which the system network resides regularly scan all Web Farm servers for IA vulnerabilities. Any vulnerabilities detected are promptly corrected.

O.2.3 Collaboration

Defines the set of capabilities that allow for the concurrent, simultaneous communication and sharing of content, schedules, messages and ideas within an organization.

E-mail

- **MS Exchange 2003.** E-mail server for all USACE e-mail delivery and retrieval. All sites are migrating to this version.
- **Outlook 2003.** Standard client for workstations for delivery and retrieval of e-mail, calendaring, tasking and other office functions.
- **Windows Server 2003.** Windows 2003 Server provides server processing for applications that rely on Windows. It includes Sharepoint.
- **Active Directory 2003.** Active Directory is an essential and inseparable part of the Windows network architecture that improves on the domain architecture to provide a directory service designed for distributed networking environments. Active Directory lets organizations efficiently share and manage information about network resources and users. In addition, Active Directory acts as the central authority for network security, letting the operating system readily verify a user's identity and control his or her access to network resources. Equally important, Active Directory acts as an integration point for bringing systems together and consolidating management tasks. Information concerning deployment is available on the Web site <https://www.ceeis.usace.army.mil/activedirectory.htm>.
- **Microsoft Exchange 5.5.** Microsoft Exchange 5.5 e-mail is the exchange of computer-generated and stored messages by telecommunication. An e-mail can be created manually via messaging applications or dynamically programmatically such as automated response systems. USACE is migrating off this version of e-mail server.

Defines the set of capabilities that support the transmission of memos and messages over a network.

Document Library. Defines the set of capabilities that support the grouping and archiving of files and records on a server.

Web Conferencing

- **Live Meeting 2003.** Web conferencing service from Microsoft. This product is being evaluated by various groups within USACE.

Capabilities that host meetings via the Web.

Video Conferencing. Defines the set of capabilities that support video communications sessions among people that are geographically dispersed.

Computer/Telephone Integration. Several ongoing VOIP efforts across USACE.

Shared Calendaring

- **Groove.** Application software that allows teams of people to work together over a network as if they were in the same location. More details are available on <http://www.groove.net>. The architecture that supports Groove is shown in Figure O.1.

Defines the set of capabilities that allow an entire team as well as individuals to view, add and modify each other's schedules, meetings and activities.

Task Management

- **Groove.** Described previously.

Primavera Project Manager 3.5.1. Project management application.

- **Primavera Project Manager 4.1.** Project management application.

Defines the set of capabilities that support a specific undertaking or function assigned to an employee.

Threaded Discussions

- **Groove.** Described previously.

Defines the set of capabilities that support the running log of remarks and opinions about topic or subject.

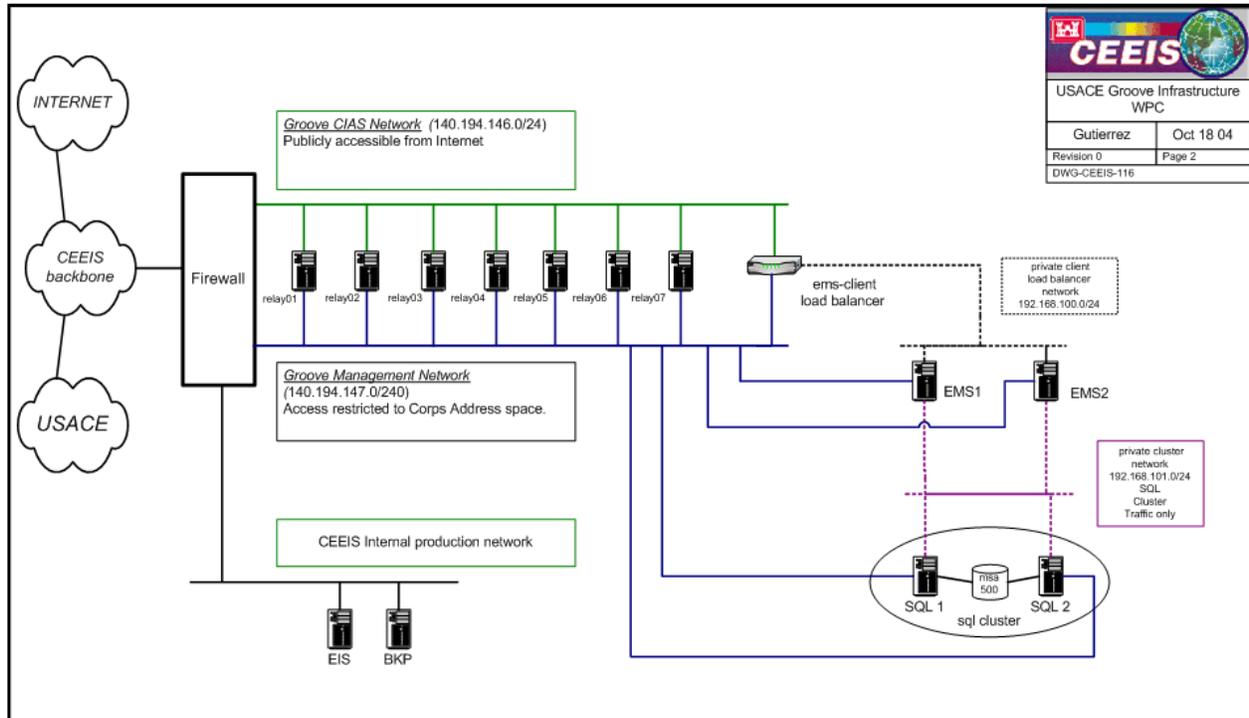


Figure O.1. Architecture that supports Groove

Search

- Autonomy.** Autonomy is used to automatically process and organize large amounts of unstructured information into project-relevant content. Autonomy calculates the probabilistic relationship between multiple variables and determines the extent to which one variable impacts another. This makes it feasible to calculate the relationships between many variables, allowing software to reveal the context of a piece of unstructured information. Once the meaning is understood, Autonomy then relies on Shannon's theory, which states that the less frequently a unit of communication (for example a word or phrase) occurs, the more information it conveys. Thus ideas, which are more rare within the context of communication, tend to be more indicative of its meaning. This approach is independent of the language of the text and allows the main concepts to be identified and prioritized.

Figure O.2 outlines the current configuration of Autonomy. The main components of Autonomy reside on two separate servers. One server is configured as the machine to crawl the targeted sites while a second server houses the active databases. Note that Autonomy is designed to manage multiple databases. This allows each application (Web site, desktop client, portal, etc.) that requires search capabilities to have Autonomy build and manage a database unique to its needs. As a result, the Autonomy administrator is responsible for managing all the links that support each application.

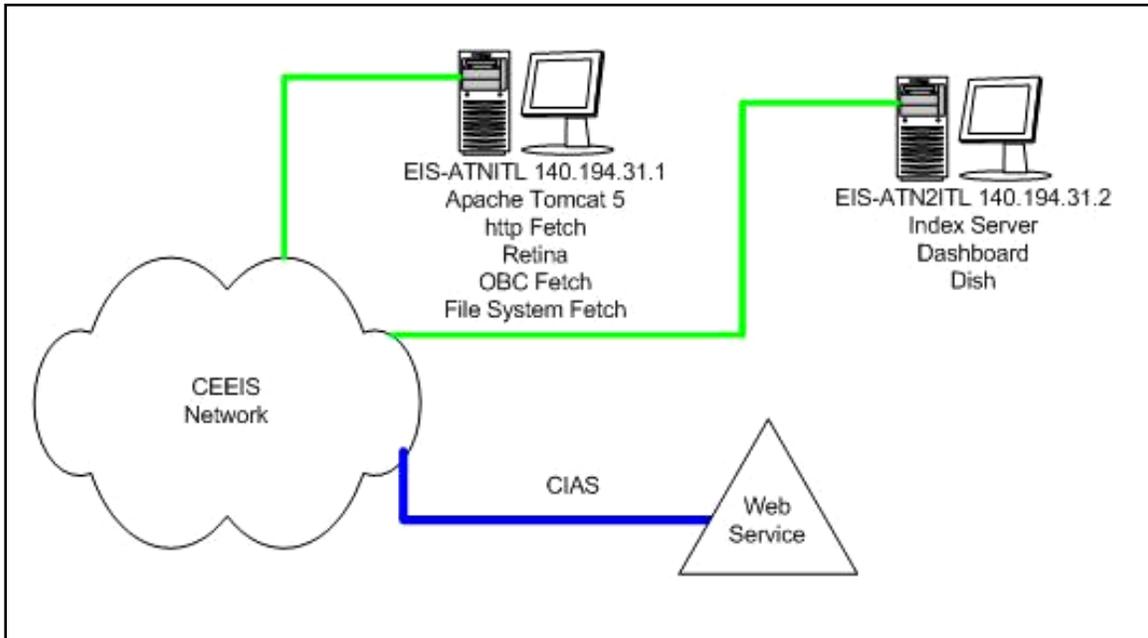


Figure O.2. Current configuration of Autonomy

Applications interface with the Autonomy databases through a Web service. The implementation of the Web service is based on the standards presented in the Web Services section in the Technical Reference Model (TRM) (see Appendix P). The connectivity of the Web service to the backend Autonomy database follows the guidelines described in the Enterprise Application Integration section of the TRM. The Web service interface works by taking an Autonomy command (see Autonomy documentation) and sending it to the database using an HTTP GET command. The request is processed and returned to the waiting application in XML through the Web service.

O.2.4 Communications

Defines the set of capabilities that support the transmission of data, messages and information in multiple formats and protocols.

Audio Conferencing. Defines the set of capabilities that support audio communications sessions among people who are geographically dispersed.

Community Management

- **Groove.** Described previously.

Defines the set of capabilities that support the administration of online groups that share common interest.

Computer/Telephony Integration. Defines the set of capabilities that support the connectivity between server hardware, software and telecommunications equipment into a single logical system.

Event/News Management. Defines the set of capabilities that monitor servers, workstations and network devices for routine and no routine events.

Instant Messaging. Defines the set of capabilities that support keyboard conferencing over a Local Area Network or the Internet between two or more people.

Real Time/Chat. Defines the set of capabilities that support the conferencing capability between two or more users on a Local Area Network or Internet.

Video Conferencing. Defines the set of capabilities that support video communications sessions among people who are geographically dispersed.

O.2.5 Security Management

AR 25-2. Army regulation for IA that outlines best practices to facilitate the Army's ability to adapt to changing technology or implementation guidance.

Defines the set of capabilities that support the protection of an organization's hardware/software and related assets.

O.3 Customer Service

The Services for Citizens Business Area describes the mission and purpose of the United States Government in terms of the services it provides both to and on behalf of the American citizen. It includes the delivery of citizen-focused, public, and collective goods and/or benefits as a service and/or obligation of the Federal Government to the benefit and protection of the Nation's general population.

O.4 Process Automation Services

The Process Automation Services Domain defines the set of capabilities that support the automation of processes and management activities that assist in effectively managing the business. The Process Automation Services Domain represents those services and capabilities that serve to automate and facilitate the process associated with tracking, monitoring, and maintaining liaison throughout the business cycle of an organization.

O.5 Business Management Services

The Business Management Services Domain defines the set of capabilities that support the management of business functions and organizational activities that maintain continuity across business and value-chain participants. The Business Management

Services Domain represents those capabilities and services that are necessary for projects, programs and planning within a business operation to successfully be managed.

O.6 Digital Asset Services

The Digital Asset Services Domain defines the set of capabilities that support the generation, management and distribution of intellectual capital and electronic media across the business and extended enterprise.

Knowledge Management

- **Groove.** Described previously.
- **Autonomy. Autonomy.** Autonomy is used to automatically process and organize large amounts of unstructured information into project-relevant content. Autonomy calculates the probabilistic relationship between multiple variables and determines the extent to which one variable impacts another. This makes it feasible to calculate the relationships between many variables, allowing software to reveal the context of a piece of unstructured information. Once the meaning is understood, Autonomy then relies on Shannon's theory, which states that the less frequently a unit of communication (for example a word or phrase) occurs, the more information it conveys. Thus ideas, which are more rare within the context of communication, tend to be more indicative of its meaning. This approach is independent of the language of the text and allows the main concepts to be identified and prioritized.

Figure O.2 outlines the current configuration of Autonomy. The main components of Autonomy reside on two separate servers. One server is configured as the machine to crawl the targeted sites while a second server houses the active databases. Note that Autonomy is designed to manage multiple databases. This allows each application (Web site, desktop client, portal, etc.) that requires search capabilities to have Autonomy build and manage a database unique to its needs. As a result, the Autonomy administrator is responsible for managing all the links that support each application.

Applications interface with the Autonomy databases through a Web service. The implementation of the Web service is based on the standards presented in the Web Services section in the Technical Reference Model (TRM) (see Appendix P). The connectivity of the Web service to the backend Autonomy database follows the guidelines described in the Enterprise Application Integration section of the TRM. The Web service interface works by taking an Autonomy command (see Autonomy documentation) and sending it to the database using an HTTP GET command. The request is processed and returned to the waiting application in XML through the Web service.

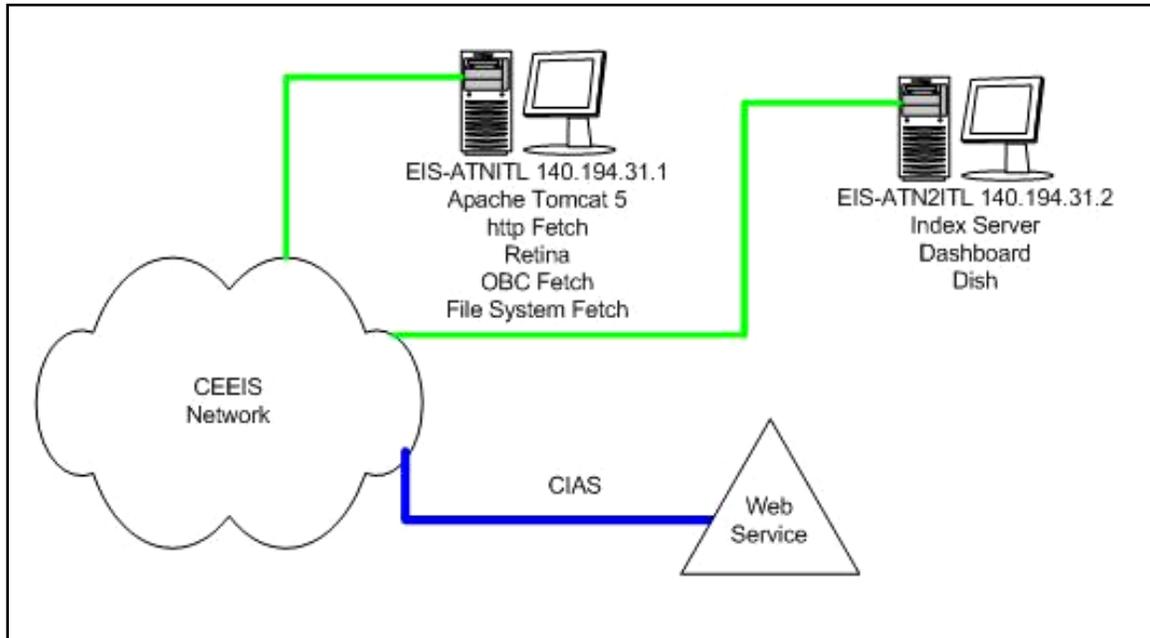


Figure O.2. Current configuration of Autonomy

- Oracle Portal 3.0.9.** Oracle Portal provides a complete and integrated framework for developing, deploying, and managing enterprise portals. It enables secure information access, self-service publishing, online collaboration, and process automation.

Defines the set of capabilities that support the identification, gathering and transformation of documents, reports and other sources into meaningful information.

O.7 Business Analytical Services

The Business Analysis Services Domain defines the set of capabilities supporting the extraction, aggregation and presentation of information to facilitate decision analysis and business evaluation.

Windows Server 2003. Windows 2003 Server provides server processing for applications that rely on Windows. It includes Sharepoint.

Windows 2000 Server. Windows 2000 Server and Windows 2000 Advanced Server are used to provide server processing for applications that rely on Windows.

Web Service Description Language (WSDL) Version 1.1. Web Services Description Language (WSDL) is an XML based Interface Description Language for describing XML Web services and how to use them. <http://www.w3.org/TR/wSDL>

Universal Description Discovery and Integration (UDDI) Version 2.0. Universal Description Discovery and Integration (UDDI) provides a searchable registry of XML Web Services and their associated URLs and WSDL (Web Services Description Language) pages. <http://www.uddi.org/about.html>

Appendix P – Technical Reference Model



The TRM provides the technical perspective of how technology is assembled to support the U.S. Army Corps of Engineers (USACE). As such, it has two mutually supporting objectives. The first and foremost objective is to provide the foundation for a seamless flow of information and interoperability among all USACE systems that produce, use, or exchange information electronically. The second objective is to define standards and guidelines for system development and acquisition that will dramatically reduce cost, development time, and fielding time for improved systems.

The TRM is the minimal set of design principles, technologies, standards, preferred products, and configurations that govern the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. More specifically, the TRM provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are built, and products are developed. This includes a collection of the technical standards, conventions, rules, and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular system architecture views and that relate to particular operational views.

The technical direction within this document represents the evolving implementation of the Office of Management and Budget's (OMB's) e-Government recommendations to develop a strong, enforceable technical architecture with a heavy emphasis on commercial standards and profiles. The intent is to achieve interoperability while reducing cost by leveraging the large investment that industry has made in developing and implementing standards-based technologies that are in widespread use. Every effort has been made to avoid closed commercial or military-unique standards. The standards contained herein are based primarily on commercial "open systems" technologies (open systems approach) that are being commonly used throughout the DoD and industry. Military standards are used only where absolutely necessary. Overarching standards comply with those set by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). A hierarchy of standards by family was developed to guide selection of specific standards for incorporation into this version of the TRM. The general order of preference, subject to modifications due to specific operational interoperability requirements and acceptance in the commercial marketplace (market acceptance), was standards specified by neutral standard groups such as the Institute of Electrical and Electronics Engineers (IEEE) or International Organization for Standardization (ISO), followed by industry consortiums such as the World Wide Web Consortium (W3C), then vendor standards that are so widely supported as to be de facto industry standards, and finally government standards such as Federal Information Processing Standards (FIPS) and Military Standards

(MIL-STDs). Several activities both inside and outside the USACE contribute to the evolution of the TRM.

P.1 Service Access and Delivery

Service Access and Delivery - refers to the collection of standards and specifications to support external access, exchange, and delivery of Service Components or capabilities. This area also includes the Legislative and Regulatory requirements governing the access and usage of the specific Service Component.

P.1.1 Access Channels

Access Channels define the interface between an application and its users.

P.1.1.1 Common Operating Environment

The Common Operating Environment (COE) defines the desktop environment for USACE. It involves the specification and process of continually evolving a stable baseline-operating environment to take advantage of new technologies as they mature and to introduce new capabilities. Changes are effected incrementally so that USACE Information Technology (IT) users (internal and external) always have a stable baseline environment in which to work while changes between successive releases are perceived as slight. The end result is a strategy for fielding systems with increased interoperability, reduced development time, increased operational capability, minimized technical obsolescence, minimal training requirements, and minimized life-cycle costs.

a. Desktop Operating System

Desktop applications are most commonly executed at the user level to perform work and run under the mandated operating system. At the base of this group of applications is the Office Automation Suite. The suite must be compatible with the files used in word processing, spreadsheet, graphic representation, and e-mail communications that are shared across USACE agencies.

(1) Windows 2000

Windows 2000 is a multipurpose network operating system that is scalable from the desktop to the data center. It is the Corps of Engineers' mandated desktop/office automation operating system and the Department of the Army mandated e-mail platform. Centralized management utilities, troubleshooting tools, and support for self-healing applications all make it simpler for administrators and users to deploy and manage Windows 2000 computers.

(2) Windows XP Professional

Microsoft Windows XP Professional (SP2) is a multipurpose network operating system that is scalable from the desktop to the data center. It is the Corps of Engineers' mandated desktop/office automation operating system and the Department of the Army mandated e-mail platform. Centralized management

utilities, troubleshooting tools, and support for self-healing applications all make it simpler for administrators and users to deploy and manage Windows XP computers. Windows Operating system software must be acquired off the Army Enterprise license agreement. Some configuration parameters that are default within the SP2 version of XP need to be modified in order to interact with some USACE applications.

Operating systems perform basic tasks, such as recognizing input from the keyboard or mouse, sending output to the display device, managing files and directories, controlling peripheral devices, and managing access to the system. They provide the software platform within which application programs run. Therefore, the choice of operating systems determines the applications that can be run. The operating system provides access to local computing resources and platform services. In addition, the operating system provides access to distributed platform services such as network file systems, printer resources, and data applications. Network access protocols are provided by the operating system to facilitate connection to the network. The operating system mediates access to computing processes between applications, network hardware, and the end user. Furthermore, the operating system provides services for distributed as well as centralized computing.

The predominant operating systems in USACE are general purpose, commercially available, and capable of simultaneously supporting multiple users and tasks, and they adhere to the following principles as established in the preceding standards and rules:

- Manageability - The Corps will utilize the minimum number of operating systems and system utilities necessary to support USACE's IT mission.
- Security - Security of the USACE sensitive platforms is vital. USACE must have operating systems that provide a level of security appropriate to the information and systems they manage.

(1) Microsoft Office 2000

Microsoft Office 2000 - Provides office automation products approved as the standard for USACE. This suite covers word processing, spreadsheet, slide presentation software, and the e-mail client. Microsoft Office products have become de facto standards at least at the level of document interchange.

(2) Microsoft Office 2003

Microsoft Office 2003 - Provides office automation products approved as the standard for USACE. This suite covers word processing, spreadsheet, slide presentation software, and the e-mail client. Microsoft Office products have become de facto standards at least at the level of document interchange. These products must be acquired off the Army Enterprise License Agreement.

(3) IE Web Browser

Microsoft - IE V6 (SP1) - Web browser; interconnection to Internet display text, graphics, images, and sounds. The desired configuration for client operations

with an application is through the use of Web browsers on the client and Web servers/services on the application side. This reduces deployment and management impacts on the client.

(4) **WSFTP**

WSFTP - WSFTP32 - File transfer utility.

(5) **WinZip**

WinZIP Version 9 - A desktop application that provides compression and decompression tools.

(6) **Adobe Acrobat Reader v6.0**

Adobe Acrobat Reader v6.0 - Utilizes the Portable Document Format (PDF) to read documents as a faithful representation of the original document in display mode.

(7) **Window Media Player**

Windows Media Player V8 - Audio and video player

(8) **Bentley - Microstation Version 8**

The scope of this section specifically addresses the acquisition and/or creation of data from Computer-Aided Design and Drafting (CADD) computer systems. CADD technology has become the preferred method for the preparation, distribution, storage, and maintenance of architectural and engineering drawings. Types of products produced from these systems include the following (Note: many of these drawing types are also applicable to Geographic Information System (GIS) and facility management technologies):

- Engineering drawings for vertical (building) construction.
- Facility management drawings/maps.
- Master planning drawings/maps.
- Environmental compliance drawings/maps.
- Hydrographic surveying of rivers, ports, open ocean, bays, channels, and lakes.
- Topographic mapping.
- Drawing/map conversion, raster scanning/vector conversion.
- High-order geodetic control (horizontal and vertical) surveys using differential Global Positioning System (GPS) and conventional survey techniques, for control, and property/ boundary surveys.
- Controlled and noncontrolled aerial photography and photo processing.
- Photogrammetric mapping including aerotriangulation.

- Finish map (color and black-and-white) publishing or production from GIS data sets and software applications.
- Digital-orthophotography image file and map production.
- Remote sensing, radar, and satellite imagery.
- Large-format map and/or aerial imagery document production.

The Corps currently requires the use of the most current version of the CADD/GIS Technology Center's Architectural/Engineering/Construction (A/E/C) CADD Standard for the development of most two-dimensional (2-D) and three-dimensional (3-D) CADD drawings. Although some CADD applications have the capability to use attached (or internal) databases, these capabilities are not widely used within the Corps. It should be noted that the A/E/C CADD Standard is compliant with the U.S. National CAD Standard distributed by the National Institute of Building Sciences. The A/E/C CADD Standard expands the U.S. National CAD Standard by adding DoD-specific requirements. The A/E/C CADD Standard is distributed via CD-ROM and the Internet at <http://tsc.wes.army.mil>.

(9) **Symantec AntiVirus**

Symantec AntiVirus Corporate Edition v9.0

(10) **McAfee VirusScan**

McAfee VirusScan Enterprise 7.1.0 (SP1)

(11) **Microsoft Visio Viewer 2003**

Microsoft Visio Viewer 2003

P.1.1.2 Government Partners

Connectivity with business partners outside the USACE Wide-Area Network (WAN) occurs through the Extranet channel.

P.1.1.3 Industry Partners

Connectivity with business partners outside the USACE WAN occurs through the Extranet channel.

P.1.1.4 Public

Public access to unrestricted information via the Internet channel.

P.1.2 Delivery Channels

Delivery Channels define the level of access to applications and systems based upon the type of network used to deliver them.

P.1.2.1 Secure

Secure communication is facilitated by SIPRNET. Communication is provided by either dedicated circuit or secure in-dial modems. The volume of secure traffic has been historically light but is significantly increasing with the advent of global terrorism and growing military conflicts.

P.1.2.2 Internet

The Internet is a worldwide system of computer networks in which users at any one computer can, if they have permission, get information from any other.

P.1.2.3 Intranet

An Intranet is a private network that is contained within USACE. The principal Intranet for USACE is the local area network (LAN) at each USACE location and the WAN circuits that interconnect them. This corporate network provides each Corps employee with access to all corporate resources.

P.1.2.4 Extranet

An Extranet is a private network that uses the Internet protocol and the public telecommunication system to securely share with business partners. One of the growing areas of delivery centers on how USACE interoperates with partners and customers outside the WAN. Due to the security restrictions, it is believed that the Web provides the most dependable approach to delivery.

P.1.2.5 Virtual Private Network (VPN)

Ideally, USACE would be able to cut off all externally initiated traffic to all production assets. In the real world, this is not feasible. There are a large number of customers outside the Corps network who critically need access to production systems. In order to support this requirement, the Corps is deploying VPN technology. As needed, the firewalls will be configured to allow outside initiated traffic to production systems as long as the external client is using encrypted VPNs and augmented with validated keys. VPNs will be used not only to encrypt the session but also to authenticate and control access. Automated Information Systems (AIS) developers need to be aware of the location of their customer base. If customers of the AIS are located outside the enterprise WAN, they should discuss the VPN support requirements with the Corps of Engineers Enterprise Infrastructure Services (CEEIS).

The USACE security configuration creates LANs at each site that are typically not accessible from outside USACE. Exceptions to this are cases where someone outside of the WAN needs access to production systems. Where this type of access is required, USACE punches holes in the firewalls to allow access. The VPN deployment is designed to close off these holes and provide access in a more secure manner.

Placing a VPN client on the external system allows the traffic between the client and the USACE internal network to be encrypted. This also allows USACE, through the use of Public Key Infrastructure (PKI) to ensure that the traffic is coming from a user that has

been granted access to USACE production systems. Complemented by the use of personal firewall and personal IDS software, risk to the client, while connected to the Internet is reduced. This prevents the client from being used to “ricochet” traffic through the client’s system and into the WAN.

P.1.3 Service Requirements

Service Requirements defines the necessary aspects of an application, system or service to include legislative, performance and hosting.

P.1.3.1 Legislative/Compliance

Legislative/Compliance defines the prerequisites that an application, system, or service must have mandated by Congress or governing bodies.

Section 508

Section 508 requires that Federal agencies’ electronic and information technology is accessible to people with disabilities, including employees and members of the public.

P.1.3.2 Authentication

Authentication refers to a method that provides users with the ability to login and get access to all application, services, and data.

- a. **U-PASS Authentication.** At the Corps of Engineers enterprise level, an internally developed application known as U-PASS is used to provide password management and authentication services for all users of UNIX and Windows/Active directory based enterprise and local resources. Applications and systems must be deployed with interfaces to U-PASS.
- b. **AKO Authentication.** Army Knowledge Online (AKO) supports authentication via LDAP services. Note that a Web service interface is available through CDF. Check the UDDI registry for more details.

P.1.4 Service Transport

Service Transport defines the end-to-end management of the communications session to include the access and delivery protocols.

P.1.4.1 Transport Control Protocol (TCP)

TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the destination.

P.1.4.2 Internet Protocol (IP)

IP is the protocol of the Internet and has become the global standard for communications. IP accepts packets from TCP, adds its own header and delivers a “datagram” to the data link layer protocol. IP addresses at the enterprise level are assigned by the CEEIS office whereas IP addresses at the regional level are assigned

by the regional IM office. IP addresses for reserved address spaces (10.0.0.0) are assigned by CEEIS.

P.1.4.3 HyperText Transfer Protocol (HTTP)

HTTP is the communication protocol used to connect the servers on the World Wide Web (WWW). The primary functions of HTTP are to establish a connection with a Web server and transmit HTML pages to the client browser.

P.1.4.4 File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after HTML pages for a Web site are developed on a local machine, they are typically uploaded to the Web server using FTP. This version of FTP should be used only where absolutely necessary or when used in transferring information using anonymous FTP. Since this protocol is plain-text, it is insecure and passwords can easily be captured.

P.2 Service Platform and Infrastructure

Service Platform and Infrastructure - refers to the collection of delivery and support platforms, infrastructure capabilities and hardware requirements to support the construction, maintenance, and availability of a Service Component or capabilities.

P.2.1 Infrastructure

USACE has a top-level, enterprise-managed network infrastructure that interconnects all Corps sites at the Field Operating Activity (FOA) level. This includes approximately 70 major sites worldwide. In addition to these sites, many Corps sites also have connections to local project offices. In some cases, sites have as many as 50 project offices, field offices, construction offices, dams and locks that are interconnected. This backbone network is composed of T-1 frame relay connections into the Sprint and MCI FTS2001 frame clouds. In order to handle the traffic load of those applications that are centralized, there are 45-Mbps connections to each processing center from both Sprint and MCI. This network provides for the passing of traffic between Corps sites in support of engineering, financial, e-mail, real-time data collection and other USACE business functions. In addition, USACE has a very high number of external customers, both military and nonmilitary. These customers access USACE systems via Internet gateways at the centers.

Primary external connections - In order to provide USACE staff access to non-Corps systems and to provide access by external customers to USACE systems, there are two external gateways located in Portland, OR, and Vicksburg, MS (Figure P.1). These gateways provide 45-Mbps connections at each gateway site

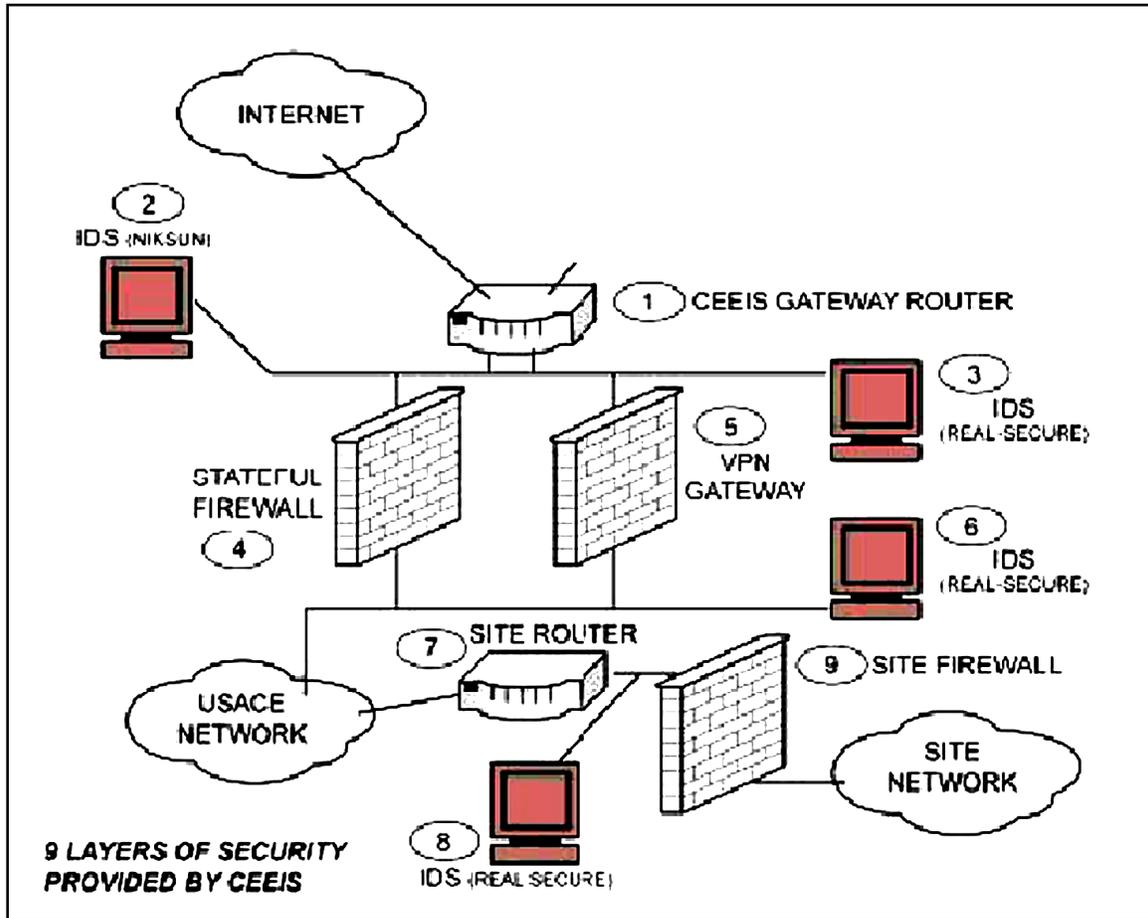


Figure P.1. External connections with USACE systems

Other external connections - At a few Corps sites there are also external connections to other agency networks in support of the Corps mission. These include Environmental Protection Agency, U.S. Fish and Wildlife Service, U.S. Bureau of Reclamation, National Oceanic and Atmospheric Administration, and other Federal, State and local entities.

P.2.1.1 Enterprise WAN-baseline

a. WAN Security Model

The WAN benefits from a nine-layer security model that protects all components of the enterprise infrastructure.

- (1) Gateway router - These routers connect the USACE network to outside networks. They initially provide security functions through the use of Access Control Lists (ACLs). These are configured to block out traffic that is not needed within USACE and also to block particular hosts or networks that have been observed to exhibit improper security behaviors.

- (2) IDS - Nixsun - These devices log all inbound/outbound traffic to/from the USACE network and retain these logs for a number of days. They also provide traffic analysis both real-time and historic that can be used to analyze security events.
- (3) IDS - real-secure (Gateway) - These devices monitor inbound/outbound traffic to/ from the USACE network and are configured to look for particular security events through the use of signatures. These events are reported back to a centralized console at the processing centers. The primary intent of these devices is real-time analysis of the USACE security infrastructure.
- (4) Stateful firewall - These devices inspect all inbound/outbound traffic to/from the USACE network and allow or deny it based on a variety of parameters. This device is configured to allow particular traffic in and deny all other traffic.
- (5) VPN gateway - These devices are used to authenticate and encrypt VPN traffic from external VPN clients. These clients are typically teleworkers, USACE's staff located on other networks etc.
- (6) IDS - real-secure (Inside USACE) - These devices monitor inbound/outbound traffic to/from each USACE site after this traffic has been processed by the gateway firewall and the VPN gateway. These are configured to look for particular security events through the use of signatures. These events are reported back to a centralized console at the processing centers. The primary intent of these devices is real-time analysis of the USACE security infrastructure as it relates to the site.
- (7) Site router - These routers connect each USACE site to the CEEIS network. They provide initial security functions through the use of ACLs. These are configured to ensure that traffic to/from the site cannot be spoofed. This is done by making sure that all traffic leaving the site contains addresses that belong to that site.
- (8) IDS- real-secure (Site) - These devices monitor inbound/outbound traffic to/from each USACE site and are configured to look for particular security events through the use of signatures. These events are reported back to a centralized console at the processing centers. The primary intent of these devices is real-time analysis of the USACE security infrastructure as it relates to the site.
- (9) Firewall (Site) - These devices inspect all inbound/outbound traffic to/from each USACE site and allow or deny it based on a variety of parameters. This device is configured to allow particular traffic in and deny all other traffic. In addition, these devices hide internal site addresses from networks outside of USACE.

b. Production Segment

With the exception of systems located on IAS or CIAS segments described previously, all other systems at Corps sites are located on production segments.

This includes workstations, servers, e-mail systems, and all other components of the site's IT infrastructure. Systems on production segments are allowed to connect to other systems within USACE and systems outside of USACE. There are restrictions on which ports and protocols are allowed in/out of a site. Restrictions are contained in a separate "ports and protocols" document. Systems on production segments can initiate connections to systems outside USACE. However, external systems are not allowed to initiate connections to production segments. Exceptions of external access to production systems are facilitated by approval of a firewall change request and creation of specialized firewall configurations access. The use of VPN configuration can also provide this type of access. Systems that are designed and deployed within USACE must take these security configurations into account.

c. Controlled Internet Accessible Segment/Network

Controlled Internet Accessible Segment/Network (CIAS) segments are similar to IAS segments. They have additional restrictions to provide increased security. Systems on these segments are allowed to initiate connections to the Internet, to other IAS segments, and to other CIAS segments. These systems are not allowed to initiate connections to the production segments in the default configuration. Segments are limited to the services they are allowed to use. These segments are used to create small "island" networks that allow interconnection between Corps sites. As application developers discuss their requirements with CEEIS staff, there could be instances where it is appropriate to place applications on CIAS segments either at a site or at the processing centers. Systems that are deployed such that external access is required must take these deployment configurations into account.

d. Internet Accessible Segment/Network

The Internet Accessible Segment/Network (IAS) is a special LAN segment attached to the firewall and configured to allow access from anywhere (Internet, Corps production, etc.). The limitation on the IAS, however, is that systems on the IAS cannot initiate traffic outside the segment. This configuration prevents someone from gaining unauthorized access to systems on the IAS and then using this as a launching point to attack Corps production systems. This configuration also requires that any information to be contained on systems that are located on the IAS must be pushed to this segment. A large amount of data are collected on systems that are on the production segments and are then transferred (in real-time or on a schedule) to the system(s) on the IAS. For this reason, the IAS is typically located at the same site as the production system that is gathering the information. This ensures that the bandwidth between these two segments is high and cost-effective (typically 100 Mbps LAN connections). This scheme essentially creates a demilitarized zone (DMZ) at Corps sites as needed for location of IASs. This DMZ, unlike a typical DMZ that is located in front of the firewall, is configured such that additional security can be applied to a system located on this segment. The access to the IAS is limited to the proxies that have

been configured for the segment. In most firewall installations, the only permissible network applications are HTTP to port 80 and FTP. There are instances where other ports are allowed for hypertext markup language secure (HTTPS) and other services such as telnet and secure shell. Since these systems cannot be used to attack USACE internal devices, a violation of security on them is not critical to overall USACE security. However, they need to be protected. In cases where access is required through applications like FTP and telnet, sites should consider using secure forms of these protocols. There are currently limited cases where the IAS is allowed to make connections to production segments. In these cases, they are heavily restricted by port and machine. This is most often used where systems on the IAS need to make requests of production systems to back up the IAS server or to query a production database. Application developers must work closely with the CEEIS team to ensure the proper location of the applications within the security infrastructure. Proper location is driven by the level of external (non-USACE) access to be provided to the application.

The USACE WAN (operated by CEEIS) provides and maintains an open-system, standard-based infrastructure that provides managed interconnectivity down to the Division/District/laboratory level. This WAN is the mandatory enterprise method of interconnected Corps sites at the FOA level. The WAN is based on a high-speed network of dedicated and frame-relay circuits and intelligent switching and routing devices. This WAN encompasses approximately 100 major sites worldwide. This baseline backbone network is composed of dual T-1 Frame relay connections into the FTS2001 Sprint and MCI frame relay networks with 45-Mbps connections into each frame network at the two processing centers (Portland, OR, and Vicksburg, MS). All CONUS sites are provided with a baseline connectivity of 2 each frame connections for added bandwidth and redundancy. There are a few sites that connect to a center using dedicated T-1 (nonframe) circuits.

This network provides traffic exchange between Corps sites in support of engineering, financial, e-mail, real-time data collection, and other USACE business functions. USACE has a very high number of external customers both military and nonmilitary. The WAN consists of the following types of circuits:

- Dedicated circuits – provide dedicated bandwidth between two sites (typically between a site and a processing center). This type of direct site-to-site connectivity does not have the same level of redundancy as the frame services described in the next bullet.
- Frame relay – frame connectivity from sites into a frame cloud that fosters point virtual connections (PVCs). These connections can operate at up to the connected speed but are provided with a confirmed information rate (CIR) guaranteeing a particular level of service. These connections can have virtual connections to both centers for redundancy.

- Integrated Services Digital Network (ISDN) – used for low-speed connection of support staff to the infrastructure. Used primarily to interconnect video teleconferencing systems
- Dial up – used to provide corporate level in-dial services to the Corps.
- Digital Service Loop (DSL) – used to interconnect some remote systems to the Internet where traffic can then flow to USACE systems with the Internet gateway.
- Cable modems – similar to DSL, used to interconnect some remote systems to the Internet where traffic can then flow to USACE systems with the Internet gateway. In order to provide USACE staff access to non-Corps systems and to provide access by external customers to USACE systems, gateways are located in Portland, OR, and/or Vicksburg, MS.

CONUS site baseline: The CONUS baseline services (Figure P.2) include:

- One each T-1 MCI Frame circuit to each site with 64K CIR PVC between site and both centers (Western Processing Center (WPC) and Central Processing Center (CPC))
- One each T-1 Sprint Frame circuit to each site with 64K CIR PVC between site and both centers (WPC and CPC)

Functionality: This baseline service provides for:

- 3-Mbps load-balanced traffic between site and centers
- Direct paths (1 hop) to each Center
- 2-hop paths to every other primary Corps site
- Continued operation in case of single T-1 failure
- Continued operation in case of a center link failure
- Continued access to other center in case of complete center failure

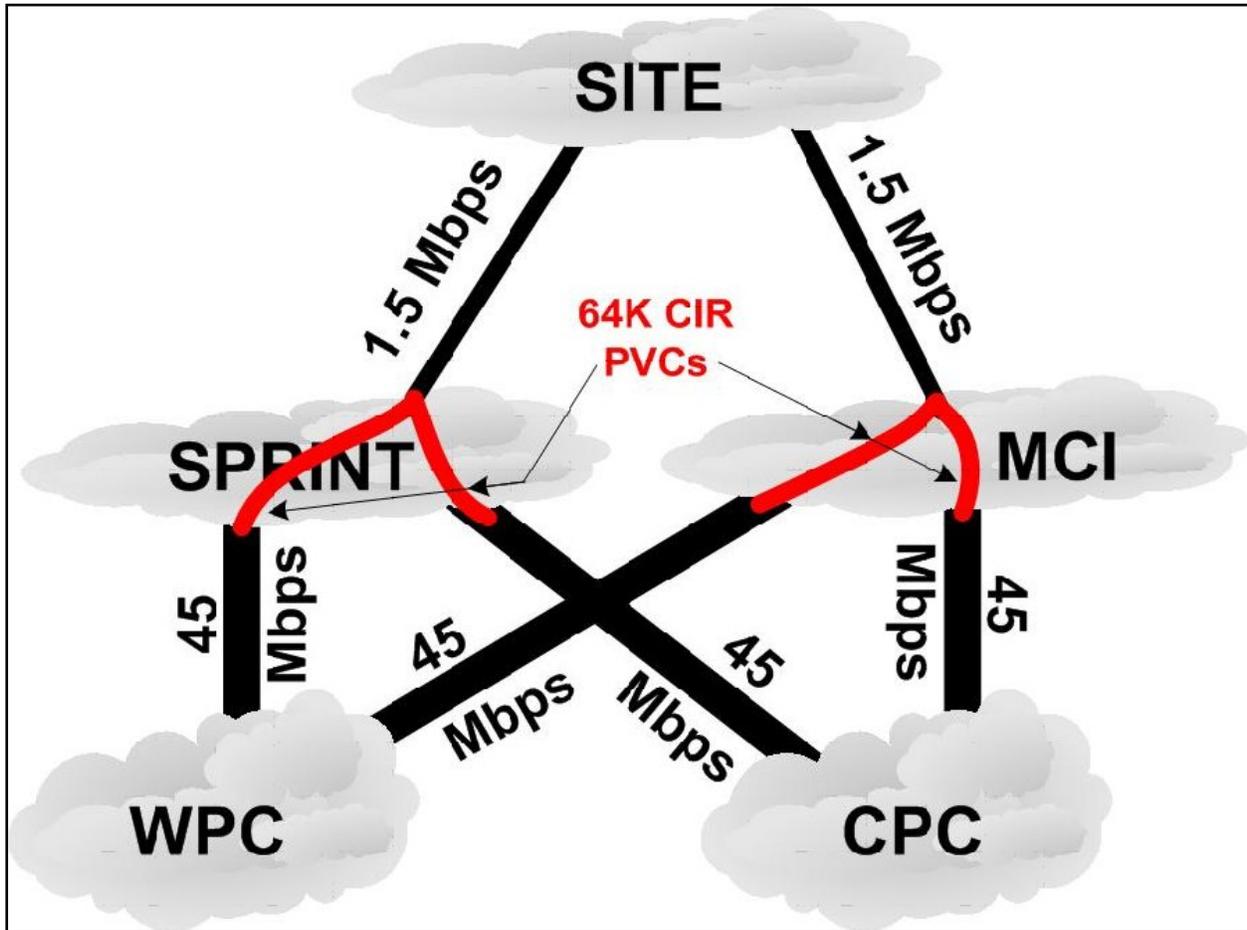


Figure P.2. MCI and SPRINT Frame circuits

OCONUS: These sites are handled on a case-by-case basis depending on the various international tariffs and connection options. Due to cost these sites do not currently have dual circuit connectivity, although potential failover options via Army have been discussed for each with the Army.

e. Processing Center Connectivity

- (1) Cisco Routers. Cisco router used in the enterprise level for all routing functions including local routing within processing centers and WAN connections at remote CEEIS managed sites.
- (2) FTS2001 Network Service. FTS2001 contract for long haul services. These services are mandatory for consideration but not mandatory for use

Routers determine the optimal path along which network traffic should be forwarded and provide the physical interfaces between LAN and WAN segments. The forwarding decisions are based on information stored within routing tables. The WAN is based on Open Shortest Path First (OSPF) routing internally with Border Gateway Protocol (BGP) on the external connections. There are some cases where

Interior Border Gateway Protocol (IBGP) is required within the WAN to transport routing information to internal routers. Much of the routing to external systems is done using the default route. This is possibly due to the fact that most external connections are located at the centers. Details concerning the routing tables are considered outside the scope of this document.

f. Site to WAN Routing

The firewalls located at the sites have static routes configured in them. Propagation of routing information from a site into the WAN is statically defined. Any routing configuration errors on the part of a Corps site cannot “infect” the corporate infrastructure routing tables. “Rogue” segments cannot be installed at sites since CEEIS staff must statically add routes for new segments into the firewalls. The firewalls do not send routing information to the internal site. Sites need to ensure that their internal network devices have a static default route that points to the firewall. Since the routing is static, sites need to work closely with the CEEIS networking staff if they are trying to design site redundancy to CEEIS.

g. Gateway Firewalls

Cisco Firewall

Cisco Firewall - PIX, latest version, used at the entrance points to the USACE infrastructure

The gateway firewall provides the initial filtering in order to block certain protocols and block access to production sites, etc. These gateway firewalls are Cisco PIX stateful packet filtering firewalls. The major entry points into the Corps are protected by Cisco PIX firewalls.

h. Center Firewalls

The center firewalls provide an additional level of protection to production systems that are located at the centers. These devices also create Internet Accessible Segment/Network (IAS) and Controlled Internet Accessible Segment/Network (CIAS) segments for use in providing corporate-level external access to information. These proxy firewalls are built on Sun platforms running Solaris, but are currently being replaced by Checkpoint software running on Nokia appliances. These firewalls are load balanced using Foundry switches and are redundant.

P.2.1.2 DREN

The Corps contains a series of laboratories that focus principally on engineering and environmental issues and topics. These laboratories have connectivity to the Defense Research and Engineering Network (DREN). The U.S. Army Engineer Research and Development Center (ERDC) in Mississippi hosts the DoD Major Shared Resource Center, which operates and maintains a series of supercomputers. Massive amounts of data are transmitted to and from these high performance systems, fostering some of the highest bandwidth requirements in the Corps.

P.2.1.3 SIPRNET

The Corps of Engineers maintains a small quantity of gateway circuits to the DoD Secure Internet Protocol Router Network (SIPRNET). These circuits are used to pass classified electronic mail, FTP, and HTTP traffic. A gateway circuit exists at each processing center to support remote access to the SIPRNET. While some sites have dedicated connections to SIPRNET, there are also sites that access this network only via dial-up. In addition, the number of workstations/staff that have access to SIPRNET attached resources is very low in most cases. Applications that are developed based around SIPRNET access need to take into account the low number of workstations that would be able to access the application.

P.2.1.4 LAN

a. Production Segment

With the exception of systems located on IAS or CIAS segments described previously, all other systems at Corps sites are located on production segments. This includes workstations, servers, e-mail systems, and all other components of the site's IT infrastructure. Systems on production segments are allowed to connect to other systems within USACE and systems outside of USACE. There are restrictions on which ports and protocols are allowed in/out of a site. Restrictions are contained in a separate "ports and protocols" document. Systems on production segments can initiate connections to systems outside USACE. However, external systems are not allowed to initiate connections to production segments. Exceptions of external access to production systems are facilitated by approval of a firewall change request and creation of specialized firewall configurations access. The use of VPN configuration can also provide this type of access. Systems that are designed and deployed within USACE must take these security configurations into account.

b. Controlled Internet Accessible Segment/Network

Controlled Internet Accessible Segment/Network (CIAS) segments are similar to IAS segments. They have additional restrictions to provide increased security. Systems on these segments are allowed to initiate connections to the Internet, to other IAS segments, and to other CIAS segments. These systems are not allowed to initiate connections to the production segments in the default configuration. Segments are limited to the services they are allowed to use. These segments are used to create small "island" networks that allow interconnection between Corps sites. As application developers discuss their requirements with CEEIS staff, there could be instances where it is appropriate to place applications on CIAS segments either at a site or at the processing centers. Systems that are deployed such that external access is required must take these deployment configurations into account.

c. Internet Accessible Segment/Network

The Internet Accessible Segment/Network (IAS) is a special LAN segment attached to the firewall and configured to allow access from anywhere (Internet, Corps production, etc.). The limitation on the IAS, however, is that systems on the IAS

cannot initiate traffic outside the segment. This configuration prevents someone from gaining unauthorized access to systems on the IAS and then using this as a launching point to attack Corps production systems. This configuration also requires that any information to be contained on systems that are located on the IAS must be pushed to this segment. A large amount of data are collected on systems that are on the production segments and are then transferred (in real time or on a schedule) to the system(s) on the IAS. For this reason, the IAS is typically located at the same site as the production system that is gathering the information. This ensures that the bandwidth between these two segments is high and cost-effective (typically 100-Mbps LAN connections). This scheme essentially creates a demilitarized zone (DMZ) at Corps sites as needed for location of Internet-accessible systems. This DMZ, unlike a typical DMZ that is located in front of the firewall, is configured such that additional security can be applied to a system located on this segment. The access to the IAS is limited to the proxies that have been configured for the segment. In most firewall installations, the only permissible network applications are HTTP to port 80 and FTP. There are instances where other ports are allowed for HTTPS and other services such as telnet and secure shell. Since these systems cannot be used to attack USACE internal devices, a violation of security on them is not critical to overall USACE security. However, they need to be protected. In cases where access is required through applications like FTP and telnet, sites should consider using secure forms of these protocols. There are currently limited cases where the IAS is allowed to make connections to production segments. In these cases, they are heavily restricted by port and machine. This is most often used where systems on the IAS need to make requests of production systems to back up the IAS server or to query a production database. Application developers must work closely with the CEEIS team to ensure the proper location of the applications within the security infrastructure. Proper location is driven by the level of external (non-USACE) access to be provided to the application.

d. Enterprise IAS

There are corporately available segments located at the two processing centers (WPC in Portland, OR, and CPC in Vicksburg, MS) where applications should be placed. The advantage of placing applications/servers at the centers is the reduction in traffic through the network for external access, the 24x7 staffing of the systems, continuity of operations provided and corporate management of the assets. This can also reduce life-cycle TCO.

Each USACE site is responsible for all LAN connectivity behind the firewall interfaces. These LANs are typically a mixture of shared 10-Mbps all the way up to switched Gigabit services and are widely varied based on site requirements.

P.2.1.5 Site WAN

Many USACE sites manage a WAN infrastructure that is local to their site. This WAN infrastructure typically connects to remote project offices, dams, locks, construction offices, and resident offices. There is a wide variety of WAN connectivity to these sites ranging from 56K up to T-1 connections. Application developers need to be very aware

of their business model and the need for remote offices to interface with the application. Applications that require heavy traffic transfer can cause implementation problems at some Corps sites. In most cases, application developers can assume that there is free and open access between these remote sites and the District site with respect to the security model. Interconnectivity of the Districts and laboratories with field entities is critical to the USACE with the implementation of more network-centric enterprise applications. Many Corps sites have established network connectivity to as many as 50 project offices, field offices, construction offices, dams, locks, etc. This connectivity is accomplished through the use of a variety of methods. The type of connection is usually determined by the most cost-effective method for delivering the bandwidth. Most Corps offices have established site WANs using frame relay circuits to connect their major remote sites to the site LANs. Smaller sites and mobile workers traditionally used dial-up (telephone) connections to remote access servers using Remote Access Dial-In User Service (RADIUS) authentication. Currently, in order to meet the higher bandwidth requirements of enterprise and local shared applications, remote, mobile, and teleworkers have begun to request and use newer broadband technologies (i.e., cable modems, DSL, satellite DSL, etc.). Unlike the processing centers, most Corps sites are not funded to provide onsite 24x7 LAN/ WAN support. The majority of sites provide some level of off-hours support, but this is typically supported by on-call arrangements. This can result in widely varying response times. Application developers need to keep this in mind when placing or assessing assets at Corps sites and entering into support service level agreements (SLAs). It directly relates to repair response time.

a. Site Firewalls

Checkpoint Firewall

Checkpoint Firewall running on Nokia appliances. These firewalls are deployed in a dual configuration at each CEEIS managed site and are managed by CEEIS.

The site firewalls provide an additional layer of protection-to-production systems located at each Corps site. The devices create IAS and CIAS segments for site use in providing external access to information. These are CEEIS managed Checkpoint firewalls running on Nokia appliances. Each Corps site is protected by a firewall of this type.

b. Bandwidth Management

Sitara QOS8000

Sitara - Rate shaping and bandwidth management – Sitara

QOS8000- function is being migrated to Cisco routers

Each Corps site has a device installed that performs the functions of TCP rate-shaping, bandwidth management/allocation, and optional Web caching. The function of these devices is being migrated to the CEEIS managed routers. Application developers need to be aware of the capability of these devices in case tuning of network performance is needed.

c. **Site routing**

If sites have no redundant connections into CEEIS (examples of a redundant connection would be a Continuity of Operations (COOP) site), these sites can perform internal routing using whatever method is most effective. If sites have multiple connections to CEEIS, the internal site network must run a dynamic routing protocol like OSPF.

d. **Site-to-Site VPNs**

Some sites choose to connect remote field sites using site-to-site encrypted VPN tunnels from the field site, through the Internet and into USACE through one of the two Internet gateways. These configurations are coordinated with the CEEIS office and must be configured with static IP addresses at the remote end. Cisco PIX units are used to perform the remote site encryption.

P.2.1.6 Wireless

Wireless Configuration

The following items are used to create a site's wireless configuration (Figure P.3):

- Wireless Access Point (WAP) - Any vendor's WAP can be used
- Cisco PIX 501- Connects to each WAP or network of WAPs
- Cisco VPN Concentrator- Used to terminate VPNs- installed in Corps Network Security Stack (CNSS)
- RADIUS Server- To authenticate VPN sessions managed by U-PASS

Software developers planning to deploy applications dependent on wireless technology need to adhere to all wireless policies.

The USACE wireless design creates a wireless configuration that is easy to deploy, flexible, secure and vendor neutral. This configuration can be deployed without modification to the site's Defense Information Technology Security Certification and Accreditation Process (DITSCAP) security boundary.

In order to use the site wireless network, customers must use a VPN client. The PIX 501 units have simple rules which ensure that wireless users are connected using VPNs. The VPN traffic must be either destined to the site's Cisco VPN concentrator or leaving the site entirely. If the traffic is destined for the site's concentrator, the customer will be validated via U-PASS and allowed to connect. If the VPN traffic is leaving the site it does not pose a risk to the site. This outbound traffic may either be going to another Corps site's VPN concentrator or may be leaving USACE altogether.

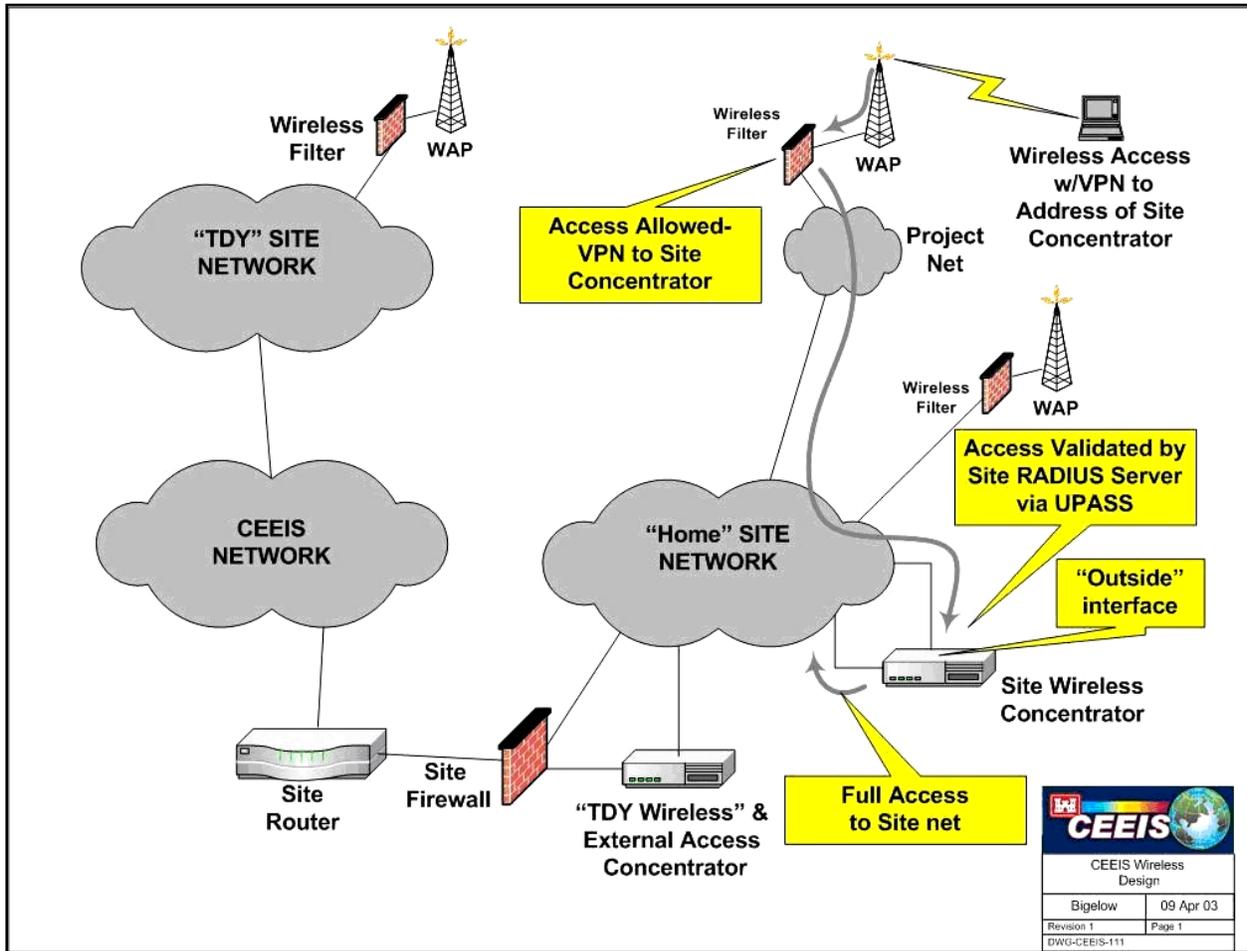


Figure P.3. Wireless network configuration

P.2.1.7 Enterprise WAN- nonbaseline1

- a. **Non-baseline to site:** There are a number of scenarios where connectivity to a site is considered to be outside of the CEEIS-provided baseline services:
 - **More than 2 circuits** - In these cases, CEEIS orders, configures, secures, and manages the circuits. However, CEEIS bills the site for the additional circuit(s).
 - **Higher than 64K PVCs** - As above, CEEIS provides and manages these PVCs. However, CEEIS bills the site for the cost difference between 64K and the requested CIR.
 - **More than 2 PVCs per circuit** - As above, CEEIS provides and manages these additional PVCs. However, CEEIS bills the site for additional PVC.
- b. **Non-baseline sites:** In order to recover from catastrophic site failures, some sites are choosing to deploy CEEIS connectivity to a field site. These types of connections allow for failover (continued access if site or field site circuits fail). These configurations require some CEEIS-managed equipment be located at the

field site including router(s), firewall(s), and Intrusion Detection System (IDS). For these connections, CEEIS provides and manages the circuit and bills the site for the cost of the circuit and a maintenance/management/ infrastructure impact fee that was approved by the CEEIS Configuration Control Board (CCB). This fee is currently set at \$950/month for FY04.

P.2.1.8 Internet

Internet access is provided for USACE through two Internet gateways, one at each center. Other Internet connections to Corps sites are not allowed with the exception of using DSL connections and site-to-site VPNs for small field offices.

P.2.1.9 Active Directory

USACE has a robust and well designed Active Directory (AD) configuration for Microsoft networking and directory services. Microsoft applications must be integrated with this directory and conform to various USACE standards and the MACOM AD Schema.

P.2.1.10 IP addressing

IP addressing within USACE is assigned either by CEEIS (for enterprise applications) or by regions (which assign addresses within their region). All major IP changes (added subnets, etc.) need to be coordinated with CEEIS so that they can be routed appropriately within the infrastructure. Also, CEEIS has allocated reserved addresses in the 10.0.0.0 address space for each Corps site. Application and infrastructure developers need to be aware of any addressing impacts of their deployments along with any issues related to the use of Network Address Translation (NAT) and the impact on their application.

P.2.1.11 VOIP

Various USACE sites are deploying Voice Over IP (VOIP) within their infrastructure boundary. At this time, there are no enterprise standards or plans for VOIP. Interoperation between sites is based solely on whether a site has deployed systems based on the same standards. This is an emerging technology for standards development within USACE.

P.2.1.12 CNSS

A key portion of the site enterprise infrastructure is the CEEIS CNSS. This rack contains routing, security, switching and remote management components needed to fully manage site connectivity and security. As this rack is within the CEEIS DITSCAP boundary, any changes or any access to this rack must be coordinated with CEEIS.

P.2.1.13 Emergency infrastructure

In addition to the infrastructure in place for use during normal scenarios, there is also an infrastructure in place for use during disasters. This includes USACE connectivity to satellite vendors, Readiness Response Vehicles (RRVs) and other disaster support infrastructure for communications and computing.

P.2.1.14 Ports and protocols

Application developers need to pay close attention to the USACE security model. There are a large number of ports and protocols that are not and will not be allowed into or out of the USACE infrastructure. This includes the Microsoft networking ports. In developing applications, these restrictions must be taken into account.

P.2.2 Servers

This section defines the middle to upper range of computers that cover both local and enterprise servers. In open system architecture, a multitude of standards and manufacturers exist that allow the server to easily connect to the network, manage the necessary network resources, and execute programs that provide the communication service. The communication service is predicated on conforming to transmission protocols and standards that ensure proper receipt. The protocol is dependent on the network design and bandwidth. The majority of servers are dedicated devices that perform the designated task. In a multiprocessing operating system environment, the server is just an application that manages the necessary network resources. The typical examples of servers are for print, file, database, end-user applications, mail, news, proxy, and Web services.

The physical server hardware devices used by USACE are based on Sun and Intel platforms. These servers are commercially available and use prevailing industry manufacturing standards for compatibility between manufacturers and availability from more than one manufacturer. As a network device, a server has a physical communication connection to support high bandwidth, a high capacity, intelligent physical storage capability, and various interfaces, monitors, and controls to ensure the communication service is correctly performed.

P.2.2.1 Operating Systems

a. Windows Server 2003

Windows 2003 Server provides server processing for applications that rely on Windows. It includes Sharepoint.

b. Windows 2000 Server

Windows 2000 Server and Windows 2000 Advanced Server are used to provide server processing for applications that rely on Windows.

c. Solaris 8

Solaris 8 is a Unix operating system based on Open Systems standards. It is backwards compatible with former versions and is in wide use inside the Corps of Engineers. Solaris 8 runs on SPARC (32- and 64-bit) or Intel Architecture (32-bit) platforms. Solaris 8 is acceptable for use on existing applications in order to migrate to Solaris 9.

d. Solaris 9

Solaris 9 is a Unix operating system based on Open Systems standards. It is backwards compatible with former versions and is in wide use inside the Corps of Engineers. Solaris 9 runs on SPARC (32- and 64-bit) or Intel Architecture (32-bit) platforms. Solaris 9 is the default UNIX-based operating system that applications should be developed under.

Various server operating systems are used at both the enterprise level of the infrastructure and at the locally managed level. The preferred server operating system at the enterprise is Sun Solaris at the most recent version with all Information Assurance Vulnerability Alert (IAVA) and other security patches applied. In some selected cases, primarily due to application operating system availability, enterprise operating systems are based on Windows 2000 or 2003. Applications that are proposed for use at the enterprise level should be evaluated in coordination with the CEEIS office for which operating system would be most appropriate. There are cases where the Linux operating system is used at the enterprise level.

P.2.2.2 Database Servers

USACE uses database servers to perform many functions including financial processing, project management and other data collection and querying applications. At the enterprise level, the Oracle database system is used. There are some applications where the use of Microsoft SQL is required. Some local applications are developed in Microsoft Access. In addition, there are externally developed applications outside of USACE control that may use databases outside of these listed. One example of this is the use of Sybase for the DoD-mandated SPS system.

a. Oracle 7.2.3

Oracle 7.2.3

b. Oracle 7.3.3

Oracle 7.3.3

c. Oracle 8.1.7

Oracle 8.1.7

d. Oracle 9.0.1

Oracle 9.0.1 - applications should be developed for Oracle 9.0.1 or later.

e. Oracle 9.2.0 (9i)

Oracle 9.2.0- applications should be developed for this version of Oracle or later

f. Oracle 10.1.0 (10g)

g. MySQL 4.0

MySQL version 4 open source Relation Database Management System (RDBMS). This database is used in isolated situations within USACE and is typically not used for enterprise applications. If developers design or intend to deploy in this environment, issues relates to support and enterprise capabilities (clustering, backups, etc.) need to be evaluated.

h. Microsoft Access 2000

Microsoft Access 2000 desktop RDBMS for small applications. Existing applications can be maintained in the environment; however, new applications should be developed in 2003

P.2.2.3 Web Servers

Web servers use either HTTP or the secure HTTPS (encrypted) protocol, which generally use port 80 or 443, respectively. Although it is possible to respond to both HTTP and HTTPS requests, Web Farm Web servers generally support only one of them. A single physical Web server can support multiple separate Web sites, each with its own unique name and underlying IP address. When more than one site resides on a single server, those sites are said to be running on “virtual servers.” This is invisible to Web site visitors and provides an economy of scale for the Web Farm customers. When a computer is serving virtual hosts, the directory structure is arranged to isolate files that belong to the individual customers but provide access to a single copy of shared services. Large amounts of disk space are typically provided and that disk is configured for fast access by the system. Web servers are configured with high-speed, often redundant, network interfaces.

a. Apache 1.3x

Apache - An enterprise WWW server that runs on Microsoft and UNIX based servers. See <http://www.apache.org> for more details.

b. Microsoft IIS Version 4

A WWW server built into Windows NT operating system.

c. Microsoft IIS Version 5

A WWW server built into Windows 2000 operating system.

d. Microsoft IIS Version 6

A WWW server built into Windows XP operating system.

P.2.2.4 Geographic Information System Servers

a. ESRI ArcGIS 8.2

ESRI - ArcGIS 8.2 - Scalable system of software for geographic data creation, management, integration, analysis, and dissemination for every organization, from an individual to a distributed.

b. ESRI ArcGIS 9.0

ESRI - ArcGIS 9.0 - Scalable system of software for geographic data creation, management, integration, analysis, and dissemination for every organization, from an individual to a distributed.

c. Oracle Spatial 8i

Oracle 8i

d. Oracle Spatial 9i

Oracle 9i

GIS is defined as an integrated geospatial technology infrastructure delivering spatial information products, services and standard data sets to all business elements and processes of the organization. The GIS architecture defines how geospatial technology within USACE is managed and deployed. Guiding principles for the development of the eGIS architecture include (a) shared spatial data infrastructure, (b) distributed architecture, (c) integration with non-GIS applications, (d) maximized performance and internal functionality, (e) maximized external interoperability, (f) maximized use of COTS products, (g) use of commercial providers or A&E services as applicable, (h) adherence to industry IT and communication standards, and (i) accommodation of desktop, client-server, and Web-based applications. The USACE GIS architecture incorporates these principles. The technical configuration is described in Figure P.4.

GIS is intended to provide a standard enterprise approach for geospatial data storage and accessibility while preserving some flexibility at the regional and local levels. This architecture is built upon the assumptions that ESRI is the preferred GIS product for USACE and Oracle is the preferred relational database product. The architecture is intended to maximize the use of COTS relational database technology and ArcSDE geodatabase (<http://tsc.wes.army.mil>) organizational techniques. An important feature of this architecture is its scalability and repeatability across corporate, regional, District, and field office levels. Scalable refers to its ability to accommodate a range in volumes of data and users. Repeatable means that this configuration can be replicated at corporate, regional, District, and field levels.

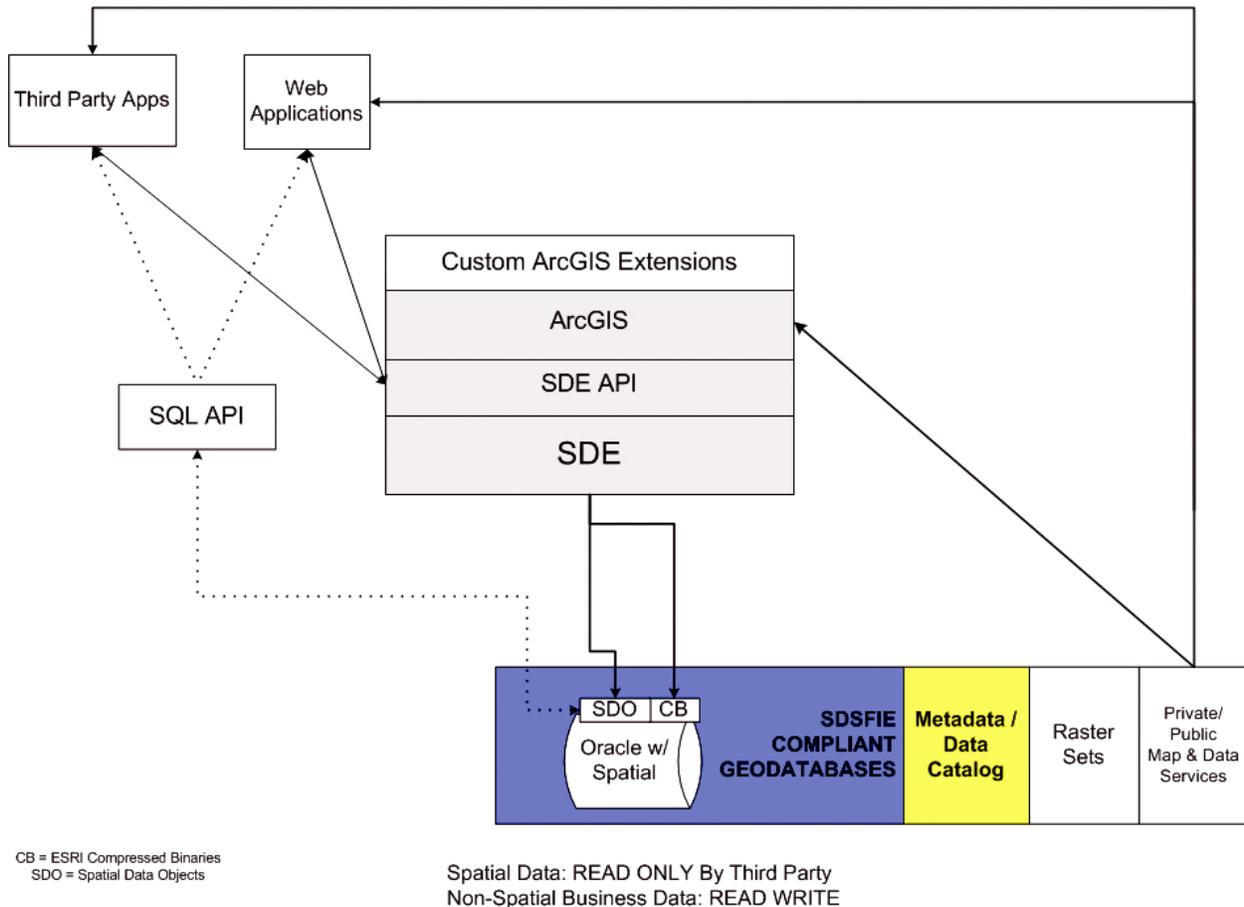


Figure P.4. Technical configuration of GIS architecture

Key points of the architecture include the following:

- The essential components of the GIS architecture are (1) ArcSDE maintained (SDSFIE)-compliant geodatabase, (2) ArcGIS software suite, (3) ArcSDE, (4) Federal Geographic Data Committee (FGDC)-compliant metadata, and (5) a spatial data catalog. Other components are flexible.
- Ideally, all enterprise base map geospatial data will be stored and maintained as an ArcSDE geodatabase using the Spatial Data Object (SDO) geometry type in Oracle 9i. Corporate data are defined as basemap data themes or business area specific themes centrally maintained to support USACE Automated Information Systems and primarily housed at one of the USACE processing centers.
- All Geospatial data are stored in an SDSFIE-compliant geodatabase (<http://tsc.wes.army.mil/>). A geodatabase is defined as a physical store of geographic information inside a relational database management system. The spatial content of the geodatabases is controlled by ArcGIS and ArcSDE. All other softwares and applications have read-only access to the spatial content of

the geodatabase. Read-write access to the nonspatial (attribute) content of the geodatabase is permitted by third parties on a case-by-case basis.

- ArcSDE functions as the mediator between various applications and the geodatabase. It provides the common access and delivery architecture that eliminates the need for redundantly stored data for multiple applications. ArcSDE enables database tuning, data loading, raster tiling, indexing, pyramiding, shared topology, topology maintenance, object definitions, version controls, projection on the fly, spatial indexing, and direct connection to large organized geodatabases at remote locations.
- For non-ESRI clients, universal access to the spatial and nonspatial content of the geodatabase is provided by the SDE Application Programming Interface (API). For spatial content this access is read-only. The SDE API is the preferred method of access by third-party applications.
- Direct SQL API access is available to spatial content via Oracle Spatial.
- It is important to note that nonspatial content (attributes or business data) is accessible at all times by any standard SQL database applications.
- Map Services provide an effective option for accessing map data hosted and maintained by private and public organizations. These services can be consumed by both GIS software and third party applications.

Location

When applications are being designed and deployed, one of the most important configuration issues is server location. Server locations can impact the following areas:

- Network traffic from other Corps sites – the current USACE network architecture is very processing center-centric. Sites need to get most of their traffic to/from the center for access to corporate applications, access to external customers, Internet, e-mail, etc. For this reason, the network bandwidths are configured to favor delivery of traffic to/from a center. If a system is to be accessed by other Corps sites, it may be best to place this system at a center to take advantage of the high-speed connections to the centers and the network design.
- Network traffic from external customers – If a system is to have a large amount of access from external customers, it also may be best to place this system at one or both of the centers. This allows the external customers to access the system with only a single hop (Internet direct to system at center). If instead the system is deployed at a remote site, this traffic must compete with normal site traffic to/from the centers.
- Network traffic primarily internal – If a system is designed such that most of the access is limited to those located at the same physical site, it may be best to locate this system at the site to reduce external traffic flows.
- Staffing – Careful consideration needs to be given to the ability to monitor and support the system. If access to the system is to be 24x7 or if the system is

critical enough that extended downtime is not acceptable, it is recommended that the system be deployed where there is 24x7 staffing of IT management.

- Operational continuity – If continuity of operations/business contingency operations are important to the system, there are server location and network design issues that should be evaluated. Locating servers at both processing centers and replicating data between them can be an effective method to reduce the risk of outage in case of disasters.
- Server class – If the system being deployed is critical, it is recommended that the hardware used be enterprise class server hardware. These are typically rack mounted, have multiple redundant components (fans, processors, disks), can have components hot-swapped and provide for other features unique to enterprise class server hardware.

P.2.3 Software Engineering

P.2.3.1 Life-cycle Management of Information Systems (LCMIS)

LCMIS provides a disciplined, yet flexible, management approach for developing AISs. Specifics concerning LCMIS and its application within USACE are documented in ER 25-1-2 (<http://www.usace.army.mil/inet/usace-docs/eng-regs/er25-1-2/entire.pdf>).

Software engineering covers not only the technical aspects of building software systems, but also management issues, such as testing, modeling, and versioning.

P.2.3.2 Software Configuration Management

Software Configuration Management is applicable to all aspects of software development for design to delivery specifically focused on the control of all work products and artifacts generated during the development process. Although no specific guidance is provided, all development activities should have a plan and subsequent processes to address version management, defect tracking, change management, requirements management and traceability, and testing.

P.2.4 Infrastructure Configuration Management

There are various level of configuration management (CM) that need to be performed in order to provide for a stable and manageable computing environment within USACE. Configuration management is a key activity that must be performed at all levels.

P.2.4.1 CEEIS Configuration Control Board (CCB)

CEEIS manages a formal configuration control board for processing of proposed configuration changes to the enterprise infrastructure.

All changes are submitted as Engineering Change Proposals (ECPs) to an advisory board (Active Directory, Networking, Security and Systems) and either approved locally, forwarded to the CEEIS Project Manager for approval or forwarded to the CCB. The CCB makes recommendations to the Chief Information Officer for implementation of

major changes. Those proposing changes to the enterprise infrastructure must follow this configuration control process.

a. FARs

Changes to the security infrastructure at the enterprise level are requested using the Firewall Action Request (FAR) form. These are required for all inbound and outbound changes to all CEEIS-managed firewalls.

P.2.4.2 AIS CCBs

Each Application is to have a configuration control board. In addition, applications that interface or integrate with either the infrastructure or other applications should have a process to route changes through the various boards to ensure that changes do not negatively impact other portions of the infrastructure.

P.3 Component Framework

Component Framework refers to the underlying foundation, technologies, standards, and specifications by which service components are built, exchanged, and deployed across USACE.

P.3.1 Security

Security defines the methods of protecting information and information systems from unauthorized access, use, disclosure, modification, or destruction in order to provide integrity, confidentiality, and availability.

P.3.1.1 Certificates/Digital Signature

Software used by a certification authority (CA) to issue digital certificates and secure access to information.

a. VPN Client

The Corps base VPN deployment uses the Cisco VPN client software Version 4.0.3D in order to provide for externally initiated trusted sessions. This software is deployed in a preconfigured manner and by default is configured with no-split tunnel. All other inbound VPN solutions are denied.

b. VPN Server

The USACE VPN standard server platform to which the inbound VPN clients connect are Cisco 3000 series concentrators running version 4.0.1 release K9 software. These servers are managed by the CEEIS staff and use enterprise managed RADIUS servers to authenticate.

c. Secure Socket Layer (SSL)

Secure Sockets Layer (SSL) - An open, non-proprietary protocol for securing data communications across computer networks. SSL is sandwiched between the

application protocol (such as HTTP, Telnet, FTP, and NNTP (Network News Transport Protocol)) and the connection protocol (such as TCP/IP, UDP (User Datagram Protocol)). SSL provides server authentication, message integrity, data encryption, and optional client authentication for TCP/IP connections.

P.3.1.2 Security Services

Security Services consist of the different protocol and components to be used in addition to certificates and digital signatures.

a. U-PASS Authentication

At the Corps of Engineers enterprise level, an internally developed application known as U-PASS is used to provide password management and authentication services for all users of UNIX and Windows/Active Directory based enterprise and local resources. Applications and systems must be deployed with interfaces to U-PASS.

b. AKO Authentication

AKO supports authentication via LDAP services. Note that a Web service interface is available through CDF. Check the UDDI registry for more details.

c. Symantec AntiVirus

Symantec AntiVirus Corporate Edition v9.0

d. McAfee VirusScan

McAfee VirusScan Enterprise 7.1.0 (SP1)

P.3.1.3 Information Assurance Plan and Program

Describes a set of ongoing activities focused on technological awareness/capability enhancement, developing and protecting the workforce, and developing and/or implementing policies and procedures to accomplish the first two.

a. Plan

A set of ongoing activities focused on enabling and sustaining Information Assurance over the long run.

(1) Responsibilities

Under Department of Army Regulation AR 25-2, Information Assurance, which may be accessed through the Policy and Guidance Web page of the Defense Information Systems Agency, <http://iase.disa.mil/policy.html>, paragraph 2-7:

2-7. Commanders of MACOMs; Chief, Army Reserve (CAR); Chief, National Guard Bureau (NGB); program executive officers (PEOs); direct reporting program managers; NETCOM RCIOs; direct reporting units (DRUs); Installation

Management Agency (IMA); and the Administrative Assistant to the Secretary of the Army

Commanders of MACOMs; Chief, Army Reserve; Chief, National Guard Bureau; Program Executive Officers; direct reporting program managers (PMs not under the PEO structure); NETCOM RCIOs; direct reporting units; Installation Management Agency; and the Administrative Assistant to the Secretary of the Army (acting as the senior official for all HQDA administrative and management services), in addition to the responsibilities defined in [paragraph 2-2](#) [of this regulation], will —

- a. Develop and implement an IA program with the hardware, software, tools, personnel, and infrastructure necessary to fill the IA positions and execute the duties and responsibilities outlined in this regulation.
- b. Oversee the maintenance, documentation, and updating of the certification and accreditation (C&A) requirements required for the operation of all ISs as directed in this regulation.
- c. Implement and manage IT system configurations, including performing IAVM processes as directed by this regulation.
- d. Appoint IA and other personnel (for example, alternates) to perform the duties in chapter 3 of this regulation and provide IAPM POC information to the NETCOM RCIO, supporting Regional Computer Emergency Response Teams (RCERTs)/Theater Network Operations and Security Centers (TNOSCs), and the Army Computer Emergency Response Team (ACERT). MACOM IAPMs will report to the RCIO of the region in which the headquarters is physically located.
- e. Appoint or approve DAAs as required.
- f. Establish an oversight mechanism to validate the consistent implementation of IA security policy across their areas of responsibility.
- g. Oversee annual security education, training, and awareness programs to all users that address, at a minimum, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.
- h. Oversee the implementation of IA capabilities.
- i. Incorporate IA and security as an element of the system life-cycle process.
- j. Develop and implement an AUP for all users for privately owned equipment (for example, cell phones, personal digital assistants (PDAs), wireless devices) and ISs prohibited during training exercises, deployments, and tactical operations. Incorporate, as a minimum, the prohibition of utilizing such devices or the limitations of acceptable use, as well as the threat of operational exposure represented by these devices in garrison, pre-deployment staging, tactical, and operational areas.
- k. Develop procedures for immediate notification and recall of IA personnel as assigned.

l. Report security violations and incidents to the servicing RCERT in accordance with Section VIII , Incident and Intrusion Reporting.

m. Adhere to and implement the procedures of the networkiness certification process.

n. Program, execute, and report management decision packages (MDEPs) MS4X and MX5T resource requirements

Within the Corps of Engineers, the Chief of Engineers, as MACOM Commander, has delegated program management responsibilities for enterprise Information Assurance (IA) to the Chief Information Officer (CIO), who heads the Directorate of Information Management (DIM), within the Headquarters USACE. Within the DIM, IA responsibilities, including the position of Information Assurance Program Manager (IAPM) are resident with the Information Assurance Division (CECI-A), which was only instituted as a separate divisional element in 2002, subsequent to the 2001 Federal Information System Controls Audit Manual (FISCAM) audit. The Division mission is to *"Provide planning and management of the USACE Information Assurance (IA) Program to ensure the confidentiality, integrity, and availability of information processed by the USACE information-based systems."* This includes providing a measure of confidence that the security features, practices, procedures, and architecture of each information system accurately implements and enforces security policies.

In the post 9/11 world, the Corps, like other Federal agencies, finds itself coping with a world greatly changed. Where previously the command was concerned primarily with denial of service or fiscal/property impacts, today we must contend with threats of physical harm to American citizens caused by cyber intrusion directed against Corps operational assets. The change is neither trivial, nor simple to implement. The Corps is closely watching the Department of the Army's evolution of DA PAM 25-IA, Information Management Information Assurance Implementation Guide (DRAFT). It is clear that the Corps will have to issue similar implementation guidance via an Engineer Regulation (ER), although the timing of this is undetermined at this time.

(2) Technology

The Corps missions are continually evolving, as is the technology available to support them. The introduction of new technologies or the implementation of existing technologies in new ways to support existing missions, may result in the recognition or emergence of new threats to the operating environment. Among recent technological evolutions offering security risks or potential security enhancements are:

- "Wireless" technologies
- Portable Electronic Devices (PEDs)
- Software auditing tools

Various wireless technologies offer tempting capabilities to the managerial problem solver while posing considerable risks to the enterprise. Wireless technologies are generally based on some variation of the IEEE 802.11, which lacks secure cryptographic capability. While extremely flexible in their general mobility and utility, personal electronic devices such as Personal Digital Assistants (PDA's) lack any meaningful secure capability, and can, if improperly implemented, offer a window of vulnerability into the enterprise.

Software auditing tools offer the enterprise the opportunity to rapidly test for multiple vulnerabilities in a thorough and cost-effective manner. Tools such as **Internet Scanner**, and SafeSuite **Database Scanner** by Internet Security Systems, which have recently been ordered, will significantly improve the enterprise's ability to ascertain its security vulnerability status by performing automated probes of communication services and devices, operating systems, and applications including database systems implementations in support of corporate AIS.

Among existing technologies facing new scrutiny are the Corps Supervisory Control and Data Acquisition (SCADA) systems, which manage our power generation capabilities, with minimal supervision in many cases, as well as implementing a significant portion of our flood control operations. Occurrences such as the recent Northeast blackout, as well as ongoing efforts to protect against and mitigate any possible effects of cyber terrorism, have led to the formation of a Project Delivery Team (PDT) comprising headquarters security personnel and engineering personnel in the field operating agencies (FOAs) which is addressing improving the security of SCADA systems.

(3) **People**

People are the heart of any of any security program – they are the greatest enabler and the greatest vulnerability. In accordance with AR 25-2, Information Assurance, security awareness begins when the employee is brought onboard. New employees are first briefed by the Security Monitor for the Division, and anyone new to the DoD and/or the Department of the Army is acquainted with AR 25-2, which is the generally governing regulation.

After the initial personnel level, the security hierarchy within the enterprise follows the structures laid out in AR 25-2. At the fundamental level is the **Systems Administrator (SA)** – responsible for the security of a single AIS, in all its self-determined aspects. At the next level up is the **Information Assurance Security Officer (IASO)**. The IASO is typically responsible for security at the workgroup or LAN level. Above the IASO is the **Information Assurance Manager (IAM)** who is responsible for security at the Division or District level. At the head of the security “pyramid” is the **Information Assurance Program Manager (IAPM)** who is responsible for the security of the enterprise.

Security awareness must encompass not only vulnerabilities of/to computer systems, but also vulnerabilities of the individual for the enterprise involving various types of “social engineering” hacker exploits. Yearly Subversion and Espionage Directed Against the Army (SAEDA) briefings assist in maintaining awareness of these types of vulnerabilities and preventing corporate compromise. While most social engineering penetration efforts are not directly destructive, they can create hidden vulnerabilities, which can be difficult and costly to rectify. All personnel also receive Yearly Information Security briefings to keep them current with emergent and emerging information security threats.

(4) **Procedures**

Security procedures in the Corps are directive under a number of Army Regulations and DoD Directives and Instructions, including:

- AR 25-2 Information Assurance
- AR 380-53 Information Systems Security Monitoring
- AR 380-67 Personnel Security Program
- AR 530-01 Operations Security
- AR 25-1 Army Information Management, and
- DoD Directive 8000.1: Defense Information Management Program

among others. The Information Assurance Division (CECI-A) has summarized much of this directive information in operational form and placed it on the corporate intranet, available Corps-wide at <https://corpinfo.usace.army.mil/ci/ia>.

The ultimate security and survival guarantor is a robust COOP plan as required by AR 25-2. Each of the Corps CEEIS processing centers acts as a COOP site for the other. In the event of a COOP execution requirement, some degradation of service is inevitable, as is a requirement for 24/7 operations by AIS users. “Excess” capacity is insufficient to support anything *more* than degraded mode operations. Nonetheless continued operations in the face of significant loss of processing capacity is possible. COOP is executed by each processing center on a regular schedule, but also by the AIS systems administrators. As a further backup, COOP plans for Y2K failures would permit some AIS to operate for up to 90 days in a purely local environment.

b. Program

Support to Information Assurance activities.

(1) **Physical Security**

The Corps uses a “defense in depth” strategy for its information infrastructure, beginning with “firewalls” at every network entrance point.

After passing the gateway firewall, traffic encounters an additional CEEIS-managed **Real Secure** intrusion detection system (IDS). Incoming e-mail is initially filtered for hostile traffic at the mail servers in Portland and Vicksburg using **Antigen** anti-virus/anti-spam software; it is further filtered at the servers in the FOA using **Norton** anti-virus, and finally filtered at the desktop by either the **McAfee** or **Norton** anti-virus, which are also provided to those who access the system remotely. As a result of using defense in depth with multiple anti-virus engines, recent Internet worm/Trojan attacks, while unavoidable, have had minimum impact on enterprise operations. Remote system access, in accordance with DA policy, is permitted only to modem pools employing the RADIUS standard. Security at the desktop is further enhanced by the use of password-protected screen saver “timeouts” as well as the implementation of VPNs for teleworkers.

Operationally, the applications, network and the enterprise components to the FOA level, have been, or are being, subject to ongoing security accreditation and review under the DITSCAP. DITSCAP is an intensive standardized four-phase security certification process consisting of Definition, Verification, Validation, and Post Accreditation phases. DITSCAP is based upon the National Institute of Standards and Technology (NIST) guidelines as implemented in a DoD environment. The DITSCAP process provides vulnerability assessments for the system or subsystem under review, as well as detailed procedural documentation for determining, securing, and maintaining the security of a given program, FOA, or AIS. Security of the network is critical, because information, which travels the network, including Water Control data, inland waterways traffic usage data, and emergency operations support (ENGLink) data, is not only mission critical but also life critical.

In addition to responding to Information Assurance Vulnerability Alerts (IAVAs) as required by the DoD and the Department of the Army, the Corps regularly performs internal assessment testing to identify vulnerabilities. Assessment testing involves not only penetration testing for known vulnerabilities in network control systems and processing center operating systems, but also “war dialing” to identify violations of general security access and control policy via unauthorized modems.

Ideally, all Corps servers and sites would be scanned for vulnerabilities every 6 months and the results reported to the IAPM and the CIO. Current manpower restrictions inhibit this, but the acquisition of the **INTERNET SCANNER** software, currently underway, should significantly improve the Corps capabilities in this regard. Although we currently capture assessment results in a database, there is, at present, no feedback capability from the assessment subject, nor any automated upward reporting capability; this has been proposed as an automation initiative for 2003.

Incident response procedures follow the Computer Emergency Response Team (CERT) guidelines for detection checklists and report formats, and flow through

the chain of command in parallel, to the Information Assurance Manager/Officer (IAM/IAO), the IAPM and the CEEIS Security Operations Center (SOC). Incidents are promptly reported and worked with the appropriate levels within Army (ACERT/CID) and other agencies (FBI/CID).

To further enhance the Corps security posture, enterprise data has been partitioned into “publicly accessible” data sets and private or enterprise data sets. “Publicly accessible” data sets comprise data generally available for the public good, such as the data on the availability of space in recreation areas, data available for public safety, such as water control data; and data available for public planning, such as data on the progress of the South Everglades Restoration Project. Publicly accessible data sets are “quarantined” away from “production” enterprise data sets supporting daily mission operations using CIAS versus the Internet accessible segments allowed internal enterprise users.

Future enhancements to the Corps information security posture, either underway or in planning, include:

- Adoption of the DoD Common Access Card (CAC) as the single network access token, with eventual migration to its use as the single point of entry, for both physical network access and logical data access.
- Public Key Enabling of the network and selected information systems resident thereon to use the PKI certificates on the CAC as an enhanced authentication mechanism, as required by DA/DoD directives, if supported by a business case based upon sound risk assessments.

(2) Logical Security

The Corps’ logical information infrastructure consists of multiple information systems, which support major Corps mission areas, or business processes, which in turn support those business areas. These AIS either have, or are in the process of being, accredited with a DITSCAP review. To facilitate this, in 2001, the Corps invested \$1.6M in 100 copies of the XACTA tool by TELOS Corp, which automates and simplifies the DITSCAP process. Additionally training and support for 3 years was also acquired under the same acquisition.

All AIS on the CEEIS network are password access controlled, both at the network access, and again at the information system access level. The corporate information systems database management system standard is ORACLE, which has a robust security architecture. The Corps AIS are implemented in ORACLE and take advantage of these security features, including the use of:

- UserID’s/Passwords – independent passwords are issued for ORACLE access to selected databases

- Product user profile table – users are restricted to the *specific* tools within the ORACLE tool suite necessary to accomplish their *specific* tasks within the AIS framework
- Roles – roles are predefined object and system privileges which grant different classes of users the necessary capabilities to accomplish their tasks within the AIS framework
- Views - view are used to segregate data access, permitting users to access *only* the data necessary to accomplish their tasks
- Encryption of data in Web applications – depending on the specific applications requirement, Web enabled applications may encrypt the session between the browser and the server (encryption is native to the ORACLE suite and may or may not include the use of the Secure Sockets Layer (SSL) protocols
- Auditing – some applications make extensive use of how and when given SQL capabilities are executed, as well as how data definitions and data manipulation are executed

The Corps was a pioneer within DoD in reducing paperwork and adopting electronic signatures (e-sigs). The Corps of Engineers Financial Management System (CEFMS) has incorporated e-sigs as a keystone of secure financial operations since 1994. The Corps is presently migrating this current secure e-sig standard from the FIPS 140-1 to a more robust PKI enabled FIPS 140-2 e-sig, in a cooperative effort between the Corps, and the NIST, with oversight by the Government Accountability Office (GAO), who pioneered this process with us. At the same time, we will be cooperatively defining the requirements for a “secure Web enabled” application. This effort is being funded using Department of the Army RDT&E monies made available for this purpose as a result of CEFMS being a “legacy” electronic signatures (e-sig) system.

The Corps AIS are managed under an ongoing LCMIS process, with security reviews included as a normal part of the system architecture, design, and acceptance process. Under Army guidance, additional AIS will be considered for migration to PKI enablement based upon risk assessments and sound business case review.

(3) **Internal and External Reviews**

Activities to monitor Information Assurance efforts.

(a) **Health of Network Study**

As part of our efforts to maintain efficiency and enhance security, the Directorate of Information Management commissioned a Communications Architecture Assessment, which was completed in October of 2000. This

study addressed network performance, documented our bandwidth deficiencies and some of the causes thereof, and projected the expected trends that we would have to deal with in the coming years. As a result of this study, the Corps acquired and installed **Sitara** network traffic prioritizers, and installed caching servers at selected sites to improve throughput.

In addition, the Corps conducted an Enterprise Management Systems (EMS) Pilot in partnership with our South Atlantic Division, deploying the **CA Unicenter** EMS products recommended by DA, to test the ability of these products to enhance management's "span of control," improve scarce personnel utilization, and offer improved security opportunities. This successful pilot demonstrated the potential for considerable improvement in efficiencies of operation at the field level, given adequate standardization and sufficient infrastructure investment.

(b) **Financial Information Systems Audit Control Manual**

During 2002, GAO in combination with the Corps Inspector General (IG) and the Army Audit Agency (AAA) participated in extensive Financial Management (FISCAM) reviews of general and applications controls. Through the use of a private contractor (Price-Waterhouse Coopers), these audits have identified weaknesses in the areas of:

- access controls
- software
- segregation of duties

In response to this, access controls in the form of firewalls and intrusion detection systems are now monitored 24/7/365. New and stricter authentication procedures have been established at the INTERNET gateways and at each individual server. We have also implemented both random and "by request" inspection procedures to look for system vulnerabilities, and unauthorized access through modem dial-up (using war-dialing techniques, as referenced previously).

We continue to limit physical access to devices or computer rooms via keypad access control locks, and we limit the number of persons having access as much as possible. In areas where changes were not technically or fiscally possible, we have put in place other procedures to mitigate the security risks.

(c) **Army Audit Agency (AAA) Reviews**

The AAA completed a separate and in-depth review of the Corps GAO sanctioned CEFMS electronic signature (e-sig) process. This review identified some operational policy issues, some of which may be mitigated by the issuance of AR 25-2 combined with the PKI enabling of CEFMS, which will

require an additional 18-24 months to complete and implement. In the interim, the enterprise will re-emphasize the training of e-sig users in their responsibilities for sound fiscal management at the individual level. Technical policy issues will be addressed by additional procedural guidance issued through the CEFMS Project Office.

(d) DoD Inspector General Audit

In July 2003, in response to a request by the Under Secretary of Defense (Comptroller)/Chief Financial Officer, the DoD IG initiated an audit of the follow-up on the GAO and AAA audit efforts. The scope of this effort includes CEEIS, the Corps Finance Center in Millington, TN, the Systems Development and Maintenance Directorate in Huntsville, AL, and selected field sites. The Corps is cooperating fully, and has already successfully demonstrated our corrective responses to some of the issues identified in the previous audits.

A separate audit review of previously identified issues in CEEIS alone began in February 2003 and is ongoing.

P.3.2 Software Development

Defines the software, protocol or method in which applications are developed.

P.3.2.1 Integrated Development Environment (IDE)

Integrated Development Environment (IDE) consist of the hardware, software and supporting services that facilitate the development of software applications and systems.

a. Microsoft Visual Studio .NET 1.1

Visual Studio .NET 1.1 is a comprehensive tool set for building and integrating Web Services, desktop and Web applications. Recommended languages include C#, VB, and C++.

b. Java Netbeans 3.6

Integrated Java environment for programmers building Java, Web, and Web service applications. See <http://www.netbeans.org/products/ide/features>.

P.3.2.2 Web Programming Languages, Tools, and Standards

General tools, languages, and standards used to develop computer software that executes via the Web.

a. eXtensible Markup Language (XML)

XML provide a standard approach to data exchange via the Web. Additional information is found on <http://www.w3.org/XML>.

b. Java Server Pages (JSP)

JSP is part of the Java suite that is used to create graphical user interfaces with the ability to change while the program is running.

c. Active Server Pages

ASP is Web server technology from Microsoft that allows for the creation of dynamic, interactive sessions with the user.

d. Active Server Pages .NET (ASP.NET)

ASP.NET is a set of technologies in the Microsoft .NET framework for building Web applications and XML Web Services. ASP.NET pages execute on the server and generate markup such as HTML or XML.

e. Cascading Style Sheets (CSS)

A style sheet format for HTML documents endorsed by W3C.

P.4 Service Interface and Integration

Service Interface and Integration refers to the collection of technologies, methodologies, standards, and specifications that govern how USACE will interface (both internally and externally) with a Service Component. This area also defines the methods by which components will interface and integrate with back office/legacy assets.

P.4.1 Integration

Integration defines the software services enabling elements of distributed applications to interoperate. These elements can share function and content, and communicates across heterogeneous computing environments.

P.4.1.1 Middleware

Middleware increases the flexibility, interoperability, and portability of existing infrastructure by linking or “gluing” two otherwise separate applications.

a. Web Services

Web services are the underlying technical standard that supports interoperability across USACE. They consist of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. This includes, but is not limited to, modules that are designed to interoperate with each other at runtime. Web services can be large or small, may be written by different programmers using different development environments, and may be platform independent.

(1) Simple Object Access Protocol (SOAP) Version 1.1

SOAP is a W3C standard protocol that allows remote procedure calls to be placed over the Internet using HTTP and XML. Clients make calls to SOAP “services.” SOAP services are basically code libraries/objects, which have exposed methods that are invoked remotely by a client.

<http://www.w3.org/tr/soap>.

(2) Web Service Description Language (WSDL) Version 1.1

Web Services Description Language (WSDL) is an XML based Interface Description Language for describing XML Web services and how to use them.

<http://www.w3.org/TR/wsdl>

(3) Universal Description Discovery and Integration (UDDI) Version 2.0

Universal Description Discovery and Integration (UDDI) provides a searchable registry of XML Web Services and their associated URLs and WSDL (Web Services Description Language) pages. <http://www.uddi.org/about.html>

b. Geographic Information Systems

(1) ESRI ArcObjects

ESRI - ArcObjects - Component object model (COM)-based collection of software components with GIS functionality and programmable interfaces. ArcObjects (Figure P.5) are platform-independent software components, written in C++, that provide services to support GIS applications, either on the desktop in the form of thick and thin clients or on a server for Web and traditional client/server deployments. Because this architecture supports a number of unique ArcGIS products with specialized requirements, all ArcObjects are designed and built to support a multi-use scenario.

http://www.esri.com/getting_started/developers/arcobjects.html

GIS is defined as an integrated geospatial technology infrastructure delivering spatial information products, services and standard data sets to all business elements and processes of the organization.

c. Relational Database Management System (RDBMS)

RDBMS manages a large set of structured data represented as mathematical relations and runs operation on the data requested by a user.

(1) Open Database Connectivity (ODBC)

ODBC is an implementation of a data access standard. The goal of ODBC is to make it possible to access any data from any application regardless of which database management systems (DBMS) is handling the data.

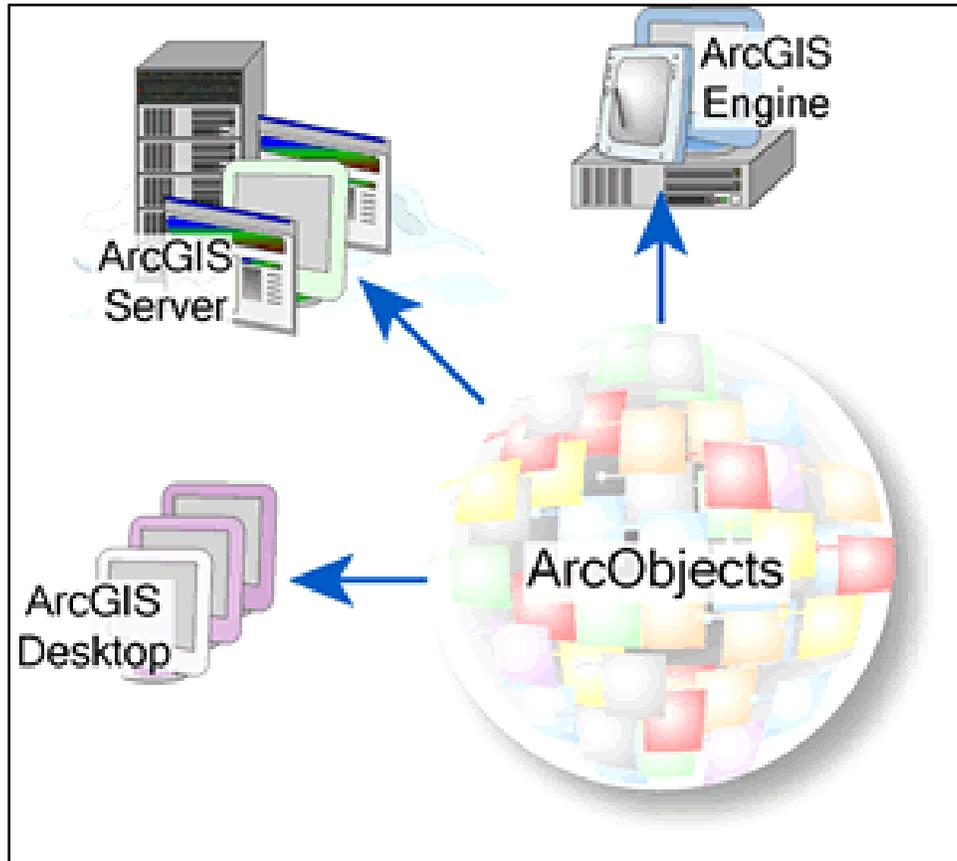


Figure P.5. ArcObjects

(2) Open ANSI SQL(92)

SQL is the information processing industry standard of relational database management systems (RDMS). ANSI X3.135-1992 (a.k.a., SQL-92 and ANSI SQL) is the industry standard for Database Language SQL.

P.4.1.2 Enterprise Application Integration (EAI)

Enterprise Application Integration (EAI) refers to the processes and tools specializing in updating and consolidating applications and data within USACE. EAI focuses on leveraging existing legacy applications and data sources so that enterprise can add and migrate to current technologies.

a. Data Exchange within WAN

Data exchange within the USACE WAN addresses the interface between the application platforms and the internal environments across which information is exchanged. It is defined primarily in support of system and application software interoperability. User and data portability are directly provided, but application software portability is also indirectly supported by references to common standard interfaces.

Figure P.6 declares that Web Services are used inside the production segment as a way to support integration among USACE AISs. Authentication and authorization of what the Web Service can see and access are controlled by the database security model. For example, access can be read only and limited to a certain set of tables. Note that the standard by which the Web Service interacts with the database is dependent on the type of database. In most cases this connectivity can be supported through ODBC. In the case of Oracle, connectivity can be supported directly through an Oracle-specific driver. Now AIS-2 gains access to AIS-1 Data via the AIS-1 WS. In short, sharing is funneled through a Web Service.

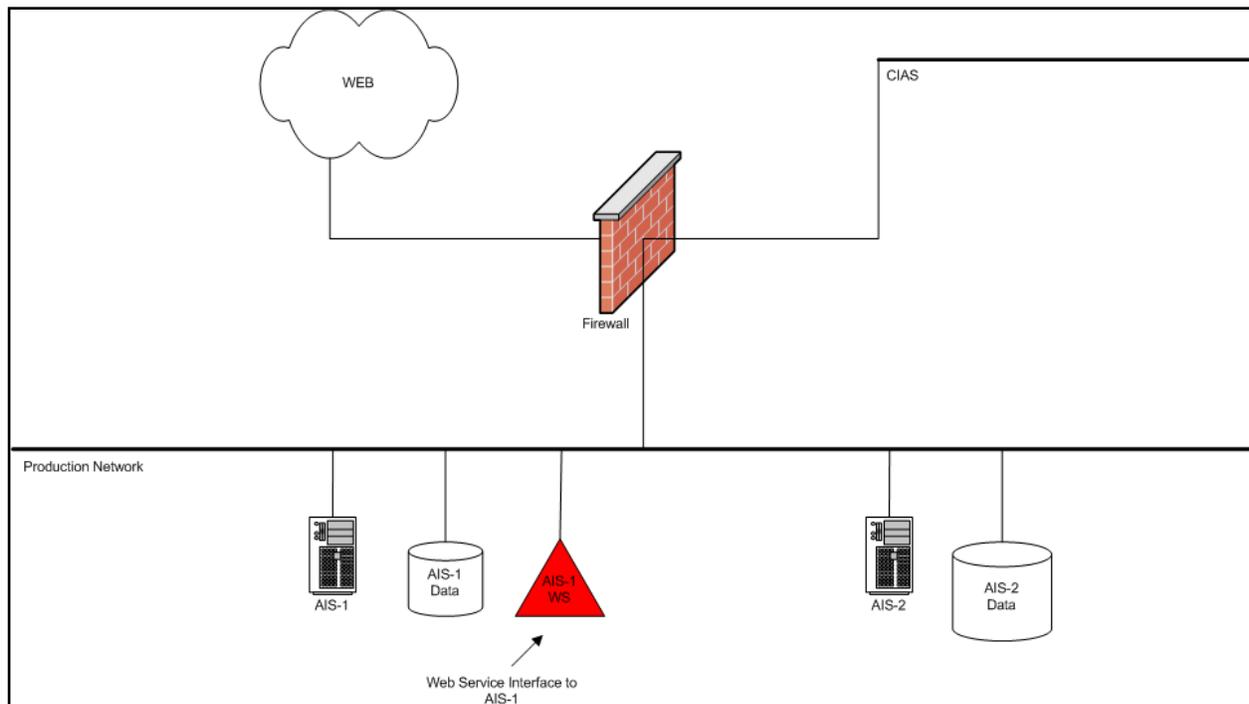


Figure P.6. Web Services support to integration among USACE AISs

b. Data Exchange from WAN to External Sources

Data exchange from WAN to external sources addresses the standards that describe how to interface USACE application platforms running in the production network with systems operating outside the production network. It is defined primarily in support of system and application software interoperability. User and data portability are directly provided, but application software portability is also indirectly supported by references to common standard interfaces.

Figure P.7 describes the approach. First a Web Service is placed on the CIAS. Web Services that reside in this area are accessible to **TRUSTED** systems via a Web connection (port 443). For this example, AIS-1 WS would access the AIS-1 Data and share the results with the external application via a Web connection. Note that the standard by which the Web Service interacts with the database is dependent on the type of database. In most cases this connectivity can be supported through ODBC. In the case of Oracle, connectivity can be supported directly through an Oracle-specific driver. Authentication and authorization between the Web Service and database is handled through the database security model. Access is always limited to read only.

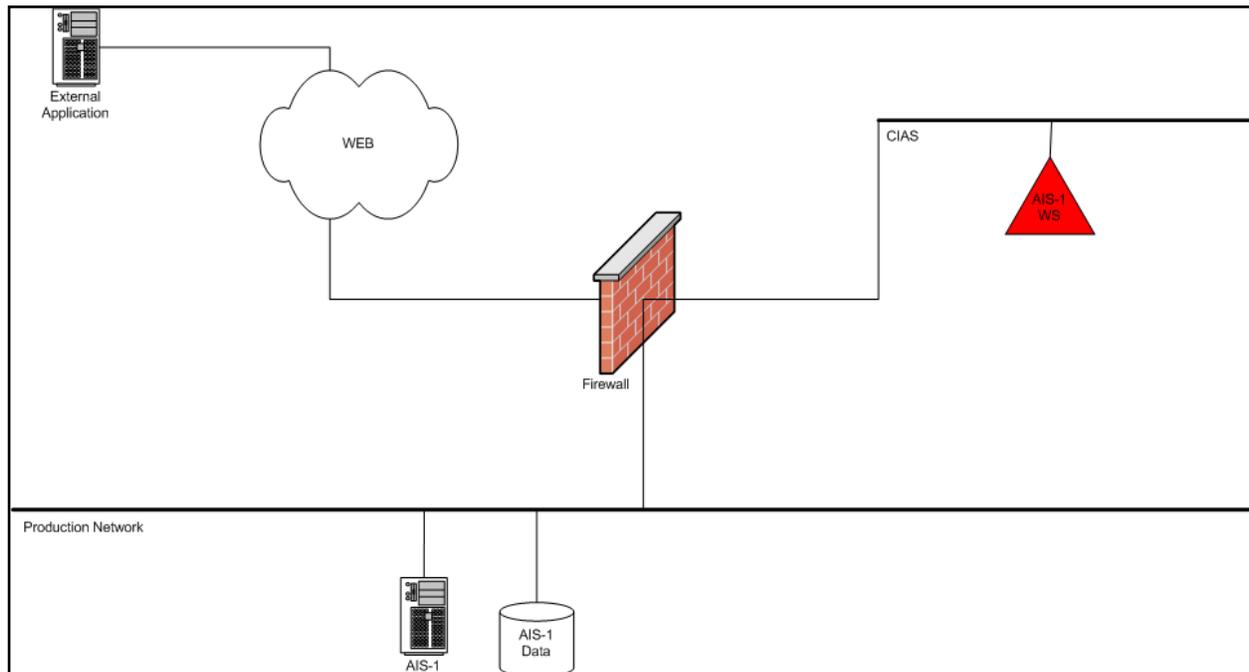


Figure P.7. Data exchange from WAN to external sources

P.4.2 Interoperability

Interoperability defines the capabilities of discovering and sharing data and services across disparate systems.

P.4.2.1 Data Format/Classification

This Section defines the structure of a file. There are hundreds of formats, and every application has many different variations (database, word processing, graphics, etc.). Each format defines its own layout of the data.

a. Extensible Model Data Format (XMDF)

XMDF is a generic data format for multidimensional models. The goal of this exercise is to develop, promote, and deploy a common modeling format that

facilitates data storage, exchange, access, analysis, and discovery of scientific and engineering data. The project encompasses one-, two-, and three-dimensional models including river cross-sections, scatter points, unstructured (finite element) grids, and structured grids. The objective of the project is to define a standard file format for all computational models developed in USACE. XMDF consists of a file format and an object code library (API). The API consists of a series of subroutines in both C/C++ and FORTRAN that can be used to read and write model geometry and data sets to the XMDF format. Model developers within USACE will be encouraged to adopt the format for all existing and future models. Numerous benefits will be derived from the standardized model format including highly compact and efficient file i/o. Using a common format makes it possible to easily share data between models, link models, and gain access to powerful visualization tools. More information is available on the XMDF Web site <http://emrl.byu.edu/xmdf/>.

b. eXtensible Markup Language (XML)

XML provides a standard approach to data exchange via the Web. Additional information is found on <http://www.w3.org/XML>.

P.4.2.2 Data Types/Validation

This Section refers to the specifications used in identifying and affirming common structures and processing rules.

a. XML Schema

XML Schemas define the structure, content, rules, and vocabulary of an XML document. XML Schemas are useful in automation through embedding processing rules.

P.4.2.3 Data Transformation

Data Transformation consists of the protocols and languages that change the presentation of the data within a graphical user interface or application.

a. eXtensible Stylesheet Language Transform (XSLT)

XSLT transforms XML documents from one schema into another. Used for data transformation between systems using different XML schema, or mapping XML to different output devices.

P.4.3 Interface

Interface defines the capabilities of communicating, transporting and exchanging information through a common dialog or method. Delivery Channels provide the information to reach the intended destination, whereas interface allows the interaction to occur based on a predetermined framework.

P.4.3.1 Service Discovery

Service Discovery defines the method in which applications, systems, or Web services are registered and discovered.

a. Universal Description Discovery and Integration (UDDI) Version 2.0

Universal Description Discovery and Integration (UDDI) provides a searchable registry of XML Web Services and their associated URLs and WSDL (Web Services Description Language) pages. <http://www.uddi.org/about.html>

P.4.3.2 Service Description

Service Description/Interface defines the method for publishing the way in which Web services or applications can be used.

a. Web Service Description Language (WSDL) Version 1.1

Web Services Description Language (WSDL) is an XML-based Interface Description Language for describing XML Web services and how to use them. <http://www.w3.org/TR/wsdl>

b. Windows Server 2003

Windows 2003 Server provides server processing for applications that rely on Windows. It includes Sharepoint.

c. Windows XP Professional

Microsoft Windows XP Professional (SP2) is a multipurpose network operating system that is scalable from the desktop to the data center. It is the Corps of Engineers' mandated desktop/office automation operating system and the Department of the Army mandated e-mail platform. Centralized management utilities, troubleshooting tools, and support for self-healing applications all make it simpler for administrators and users to deploy and manage Windows XP computers. Windows Operating system software must be acquired off the Army Enterprise license agreement. Some configuration parameters that are default within the SP2 version of XP need to be modified in order to interact with some USACE applications.

d. Windows 2000 Server

Windows 2000 Server and Windows 2000 Advanced Server are used to provide server processing for applications that rely on Windows.

e. Web Service Description Language (WSDL) Version 1.1

Web Services Description Language (WSDL) is an XML-based Interface Description Language for describing XML Web services and how to use them. <http://www.w3.org/TR/wsdl>

f. Universal Description Discovery and Integration (UDDI) Version 2.0

Universal Description Discovery and Integration (UDDI) provides a searchable registry of XML Web Services and their associated URLs and WSDL (Web Services Description Language) pages. <http://www.uddi.org/about.html>

Appendix Q – Automated Information Systems (AIS)



This section of the architecture documents USACE AISs and their relationships to the BRM, SRM, DRM, and TRM.

CEEMIS

CEEMIS

Functional Proponent: CERM

Title: COE ENTERPRISE MANAGEMENT INFORMATION SYSTEM

Acronym: CEEMIS

Project Manager: James Greene

PM Phone: 901-874-8405

Technical PM: Jeff Payne

Technical PM Phone: 901-874-8520

Operating System: Solaris

Database Language: Oracle

Programming Language: PL/SQL, SQL*Net, SQL*Forms, SQL*Plus, Pro*Cobol, Pro C, Structured Query Report, SQL*ReportWriter

Arch Type: Client Server, Web Based

Hosted by CEEIS:

Lines of Code:

Comm Req: CEEIS

Total Num of Users:

Concurrent Users:

Systems Interfaced: PRISM, CEFMS, ELECTRA (DFAS), PBAS (DFAS, GOALS (Treasury), PROMIS, IMD

DITSCAP: Yes

COOP: Yes

Run Time: 15 Hrs

Down Time: < 2 Wks

HPAMIS

HPAMIS

QMIS

QMIS

Functional Proponent: CERE

Title: Quarters Management Information System

Acronym: QMIS

Project Manager: Dwain McMullen

PM Phone: 202-761-5531

Technical PM:

Technical PM Phone:
Operating System: MS Windows 2000 Pro / XP
Database Language: Not Specified
Programming Language: Not Specified
Arch Type: Not Specified
Hosted by CEEIS:
Lines of Code: Not Specified
Comm Req: Not Specified
Total Num of Users: Not Specified
Concurrent Users: Not Specified
Systems Interfaced: Not Specified
DITSCAP: No
COOP: No
Run Time: Not Specified
Down Time: Not Specified
RECIS

RECIS

Functional Proponent: CERE-R-BI
Title: REAL ESTATE CORPORATE INFORMATION SYSTEM
Acronym: RECIS
Project Manager: Namejs Ercums
PM Phone: 202-761-7426
Technical PM: Ronda Johnson
Technical PM Phone: 251-694-3674
Operating System: Solaris
Database Language: Oracle
Programming Language: Java, Java Script, HTML, IQ, Oracle Designer, Forms 6i
Arch Type: Web Based
Hosted by CEEIS:
Lines of Code:
Comm Req: CEEIS
Total Num of Users: 30
Concurrent Users: 5
Systems Interfaced: REMIS, RFMIS, HAPMIS
DITSCAP: Yes
COOP: Yes
Run Time: 22 Hrs
Down Time: < 2 days
REMIS

REMIS

Functional Proponent: CERE-R-BI
Title: Real Estate Management Information System
Acronym: REMIS

Project Manager: Namejs Ercums
PM Phone: 202-761-7426
Technical PM: Ronda Johnson
Technical PM Phone: 251-694-3674
Operating System: Solaris
Database Language: Oracle
Programming Language: Java, Java Script, HTML, IQ, Oracle Designer, Forms 6i
Arch Type: Client Server /Web Based
Hosted by CEEIS:
Lines of Code:
Comm Req: CEEIS
Total Num of Users: 400
Concurrent Users: 34
Systems Interfaced: CEFMS, P2, FEM, RFMIS, HAPMIS, RECIS
DITSCAP: Yes
COOP: Yes
Run Time: 22 Hrs
Down Time: < 2 days
APPMS
APPMS

Functional Proponent: CELD
Title: Automated Personal Property Management System
Acronym: APPMS
Project Manager: Jimmie Smith
PM Phone: 202-761-0852
Technical PM: Ray Urena / Andy Gray
Technical PM Phone: 202-761-1618
Operating System: Solaris
Database Language: Oracle
Programming Language: Oracle Web, Java, C
Arch Type: Web Based
Hosted by CEEIS:
Lines of Code:
Comm Req:
Total Num of Users: 20000
Concurrent Users: Varies
Systems Interfaced: CEFMS, UPASS, VIMS
DITSCAP: Yes
COOP: Yes
Run Time: 5 Hrs
Down Time: < 2 Days

FEMS

FEMS

VIMS

VIMS

Functional Proponent: CELD-T

Title: Vehicles Information Management System

Acronym: VIMS

Project Manager: Jimmie Smith

PM Phone: 202-761-0852

Technical PM: Ray Urena / Andy Gray

Technical PM Phone: 202-761-1618

Operating System: Solaris

Database Language: Oracle

Programming Language: Oracle Forms

Arch Type: Client / Server and Web Based

Hosted by CEEIS:

Lines of Code:

Comm Req:

Total Num of Users: 2500

Concurrent Users: 200

Systems Interfaced: APPMS, UPASS

DITSCAP: No

COOP: No

Run Time: Varies

Down Time: Varies

DTOS

DTOS

Functional Proponent: CECS-O

Title: Deployable Tactical Operations System

Acronym: DTOS

Project Manager: Eugene Bentz

PM Phone: 251-690-2497

Technical PM:

Technical PM Phone:

Operating System: Open (COTS)

Database Language: Open (COTS)

Programming Language: Open (COTS)

Arch Type: Open

Hosted by CEEIS:

Lines of Code:

Comm Req: Open

Total Num of Users: Varies

Concurrent Users: Varies
Systems Interfaced: Open (COTS and GOTS)
DITSCAP: Yes
COOP: Yes
Run Time: Mission Driven
Down Time: Mission Driven
CEMRS
CEMRS

Functional Proponent: CERM-M
Title: Corps of Engineers Manpower Requirements System
Acronym: CEMRS
Project Manager: Peter C. Glycer
PM Phone: 202-761-1881
Technical PM:
Technical PM Phone:
Operating System: Replaced by P2
Database Language:
Programming Language:
Arch Type:
Hosted by CEEIS:
Lines of Code:
Comm Req:
Total Num of Users:
Concurrent Users:
Systems Interfaced:
DITSCAP:
COOP:
Run Time:
Down Time:
OMBIL PLUS
OMBIL PLUS

Functional Proponent: CECW-O
Title: Operations & Maintenance Business Info Link PLUS
Acronym: OMBIL PLUS
Project Manager: David Lichy
PM Phone: 703-428-9052
Technical PM:
Technical PM Phone:
Operating System: Solaris and Windows 2003
Database Language: Oracle
Programming Language: CGI, JAVA Scripts, Oracle Develop, others
Arch Type: Client Server Web Based
Hosted by CEEIS:

Lines of Code:

Comm Req: CEEIS

Total Num of Users: 5000

Concurrent Users: Varies

Systems Interfaced: NRRS, CEFMS, P2, PROMIS, CEEMIS, ABS, DPN, CORPSMAP

DITSCAP: No

COOP: No

Run Time: 24 Hrs

Down Time: 2 Days

PPDS

PPDS

Functional Proponent: CEMP-

Title: Programs and Projects Delivery System

Acronym: PPDS

Project Manager: Phil Pinol

PM Phone: 202-761-1321

Technical PM:

Technical PM Phone:

Operating System: MS Windows 2000/Pro / XP

Database Language: Oracle

Programming Language: OracleTools

Arch Type: Client Server

Hosted by CEEIS:

Lines of Code:

Comm Req: CEEIS

Total Num of Users: Varies

Concurrent Users: Varies

Systems Interfaced: CEFMS, P2, PROMIS

DITSCAP: No

COOP: No

Run Time: 20 Hrs

Down Time: 3 Days

SBIS

SBIS

Functional Proponent: CESB

Title: Small Business Information System

Acronym: SBIS

Project Manager: Karen Baker

PM Phone: 202-761-8790

Technical PM: Debbie Overstreet

Technical PM Phone: 202-761-0732

Operating System: Windows 2000 / XP

Database Language: Oracle

Programming Language: Dbase, Forpro for Windows

Arch Type:

Hosted by CEEIS:

Lines of Code:

Comm Req:

Total Num of Users:

Concurrent Users:

Systems Interfaced:

DITSCAP: No

COOP: No

Run Time:

Down Time:

ACASS/CCASS

ACASS/CCASS

Functional Proponent: CECW-CE-D

Title: Arch-Engr Contract/Constr Contract Appraisal System

Acronym: ACASS/CCASS

Project Manager: Harry Goradia

PM Phone: 202-761-4736

Technical PM: Marilyn Nedell

Technical PM Phone: 503-808-4590

Operating System: Solaris

Database Language: Oracle 7.33, Oracle Application Server (OAS) 4.08, Oracle RDBMScl 7.33 MS ACCESS (Support Staff) Sybase

Programming Language: Oracle version 7.2.3, Oracle Web server OAS 4.0.8, Bourne Shell, SQL Forms 3.0, SQL Script, XML, Java, COBOL

Arch Type: Client Server / Web Based

Hosted by CEEIS:

Lines of Code:

Comm Req: CEEIS

Total Num of Users: 2500

Concurrent Users: Unknown (varies)

Systems Interfaced: BPN, DD350 System DIOR,

DITSCAP: No

COOP: No

Run Time: 20 Hrs

Down Time: < 1 wk

EBS/ECS

EBS/ECS

SPS

SPS

Functional Proponent: CEPR
Title: Standard Procurement System (SPS)
Acronym: SPS
Project Manager: Dwight E. Dukes
PM Phone: 202-761-4236
Technical PM:
Technical PM Phone:
Operating System: Unix
Database Language: Sybase
Programming Language: Proprietary Software
Arch Type: Client Server and Web based
Hosted by CEEIS:
Lines of Code:
Comm Req: CEEIS
Total Num of Users: 1550
Concurrent Users: 25
Systems Interfaced: CEFMS
DITSCAP: No
COOP: No
Run Time: 20 Hrs
Down Time: 3 Days
BIS

BIS

Functional Proponent: CECW-EI
Title: Bridge Inventory System
Acronym: BIS
Project Manager: Paul Tan
PM Phone: 202-761-7584
Technical PM: Wayne Dahl
Technical PM Phone: 601-634-3511
Operating System: Windows 98, NT, XP
Database Language: dBase
Programming Language: Visual dBase
Arch Type: Client / Server
Hosted by CEEIS:
Lines of Code:
Comm Req: CEEIS
Total Num of Users: 300
Concurrent Users: 254
Systems Interfaced: N/A
DITSCAP: No
COOP: No
Run Time: 20 Hrs
Down Time:

AET

AET

CACES

CACES

Functional Proponent: CECW-E

Title: COMPUTER AIDED COST ENGINEERING SYSTEM

Acronym: CACES

Project Manager: Raymond L. Lynn

PM Phone: 202-761-5887

Technical PM: James Nichols

Technical PM Phone: 256-895-1842

Operating System: Windows 98, NT, XP

Database Language: Dbase, MS Access

Programming Language: Visual Studio .Net

Arch Type: Client Based

Hosted by CEEIS:

Lines of Code:

Comm Req: Local

Total Num of Users: 2000

Concurrent Users: N/A

Systems Interfaced: N/A

DITSCAP: Yes

COOP: Local

Run Time: Local

Down Time: Local

CASE

CASE

Functional Proponent: CECW

Title: Computer Aided Structural Engineering

Acronym: CASE

Project Manager: Anjana Chudgar

PM Phone: 202-761-7750

Technical PM:

Technical PM Phone:

Operating System: Windows 2000, XP

Database Language:

Programming Language: Fortran

Arch Type: Client

Hosted by CEEIS:

Lines of Code:

Comm Req: Local LAN

Total Num of Users: 500

Concurrent Users: N/A
Systems Interfaced: N/A
DITSCAP: No
COOP: No
Run Time: Varies
Down Time: 1 Wk
CORPSMAP
CORPSMAP

Functional Proponent: CEERD-RT
Title: CORPSMAP
Acronym: CORPSMAP
Project Manager: Joel Schlagel
PM Phone: 603-646-4387
Technical PM:
Technical PM Phone:
Operating System: Consolidated into EGIS
Database Language:
Programming Language:
Arch Type:
Hosted by CEEIS:
Lines of Code:
Comm Req:
Total Num of Users:
Concurrent Users:
Systems Interfaced:
DITSCAP:
COOP:
Run Time:
Down Time:
DPN
DPN

Functional Proponent:
Title:
Acronym: DPN
Project Manager:
PM Phone:
Technical PM:
Technical PM Phone:
Operating System: Consolidated into EGIS
Database Language:
Programming Language:
Arch Type:
Hosted by CEEIS:

Lines of Code:

Comm Req:

Total Num of Users:

Concurrent Users:

Systems Interfaced:

DITSCAP:

COOP:

Run Time:

Down Time:

DRCHECKS

DRCHECKS

Functional Proponent: CECW-EP

Title: Design Review and Checking System

Acronym: DRCHECKS

Project Manager: Gary House

PM Phone: 202-761-4598

Technical PM: Bill East

Technical PM Phone: 217-373-6710

Operating System: Windows 2000 / 2003

Database Language: Sql Server, other

Programming Language: JAVA, JAVA Script, HTML, Cikd Fusion, other

Arch Type: Client Server, Web Based

Hosted by CEEIS:

Lines of Code:

Comm Req: CEEIS, Local Networks

Total Num of Users: 10000

Concurrent Users: Varies

Systems Interfaced: N/A

DITSCAP: Yes

COOP: Yes

Run Time:

Down Time:

NID

NID

Functional Proponent: CECW-CE-R/SWD

Title: National Inventory of DAMS

Acronym: NID

Project Manager: Charles Pearre

PM Phone: 202-761-8994

Technical PM:

Technical PM Phone:

Operating System: MS Windows 2000/Pro / XP

Database Language: MS Access, MS Sql Server

Programming Language: HTML, Visual Basic, Visual InterDev

Arch Type: Web Based and/or Standalone

Hosted by CEEIS:

Lines of Code:

Comm Req: CEEIS, Local Network

Total Num of Users: Varies

Concurrent Users: Varies

Systems Interfaced: None

DITSCAP: No

COOP: No

Run Time: Not Specified

Down Time: Not Specified

KME

KME

Functional Proponent: CECI

Title: KME-Knowledge Management Environment

Acronym: KME

Project Manager: Brenda Ball

PM Phone: 202-761-4474

Technical PM:

Technical PM Phone:

Operating System: Open (COTS)

Database Language: Open (COTS)

Programming Language: Open (COTS)

Arch Type: Open

Hosted by CEEIS:

Lines of Code:

Comm Req: Open

Total Num of Users: Varies

Concurrent Users: Varies

Systems Interfaced: Open (COTS and GOTS)

DITSCAP: N/A

COOP: N/A
Run Time: Varies
Down Time: Varies
ECORPS

ECORPS

FUDMIS

FUDMIS

CLL

CLL

Functional Proponent: CECI
Title: Corps of Engineers Lessons Learned System
Acronym: CLL
Project Manager: Gary House
PM Phone: 202-761-4598
Technical PM: Bill East
Technical PM Phone: 217-373-6710
Operating System: Partially Rolled up into DRCHECKS
Database Language:
Programming Language:
Arch Type:
Hosted by CEEIS:
Lines of Code:
Comm Req:
Total Num of Users:
Concurrent Users:
Systems Interfaced:
DITSCAP:
COOP:
Run Time:
Down Time:
P2

P2

Functional Proponent: CECS
Title: PROMIS Phase II
Acronym: P2
Project Manager: Sean M. Wachutka
PM Phone: 202-761-7562
Technical PM: Chenita L. Bennett
Technical PM Phone: 601-634-4466
Operating System: Solaris and Windows 2003 / XP
Database Language: Oracle 8.1.7.4, Oracle 9.0.1 (OID),

Programming Language: Oracle Net8, Oracle Financial Analyzer, Oracle Internet Application, Oracle Portal, Oracle Project, Oracle Discover, Primavera, Primavision, OP3, Oracle Forms 6.0.8, Oracle Reports 6.0.8, Oracle Jinitiator 1.1.18, Oracle Internet Directory (OID)

Arch Type: Client / Server and Web Based

Hosted by CEEIS:

Lines of Code:

Comm Req: CEEIS (Citrix)

Total Num of Users: 30000

Concurrent Users: 5000-10000

Systems Interfaced: UPASS, CEFMS, RMS, FUDSMIS, CAPCES, ACES-PM, PPDS

DITSCAP: Yes

COOP: Yes

Run Time: 20 Hrs

Down Time: 3 Days

CEFMS

CEFMS

Functional Proponent: CERM

Title: COE FINANCIAL MANAGEMENT SYSTEM

Acronym: CEFMS

Project Manager: Linda Brooks

PM Phone: 256-864-1800

Technical PM: William Mordecai

Technical PM Phone: 256-864-1803

Operating System: Solaris

Database Language: Oracle 8.1, Oracle 9

Programming Language: PL/Sql, SQLNet, Oracle Dev Forms, Reports

Arch Type: Client Server / Web Based

Hosted by CEEIS:

Lines of Code:

Comm Req: CEEIS

Total Num of Users: 45,000

Concurrent Users: 12,600

Systems Interfaced: SPS, REMIS, P2, PROMIS, DCPS, IATS, RMS, VIMS, APPMS, FEMS, RFMIS

DITSCAP: Yes

COOP: Yes

Run Time: 16 Hrs

Down Time: < 5 Days

CWMS

CWMS

Functional Proponent: CECW

Title: Corps Water Management System

Acronym: CWMS
Project Manager: Gary House
PM Phone: 202-761-4598
Technical PM: Bill East
Technical PM Phone: 217-373-6710
Operating System: Solaris, Windows 2000, XP
Database Language: Oracle, HEC DSS, other
Programming Language: C, C++, Fortran, JAVA, JAVA Script, Visual Basic, Visual Basic Script, CGI, HTML, MS C
Arch Type: Client Server, Web Based
Hosted by CEEIS:
Lines of Code:
Comm Req: CEEIS, Local Networks
Total Num of Users: 10000
Concurrent Users: 1500
Systems Interfaced: WCDS, NWS, USGS, Power Systems, COES, BOR, SNOTEL, Regional, State, Local Water Agencies
DITSCAP: Yes
COOP: Yes
Run Time: Varies
Down Time: Varies
ENGLINK-I
ENGLINK-I
ENGLINK-S
ENGLINK-S
Functional Proponent: CECS
Title: ENGLink Secure
Acronym: ENGLINK-S
Project Manager: Eugene Bentz
PM Phone: 251-690-2497
Technical PM:
Technical PM Phone:
Operating System:
Database Language:
Programming Language:
Arch Type:
Hosted by CEEIS:
Lines of Code:
Comm Req:
Total Num of Users: Varies
Concurrent Users: Varies
Systems Interfaced: Unknown
DITSCAP: Yes

COOP: Yes
Run Time: Varies
Down Time: Varies
RMS

RMS

Functional Proponent: CECW-EE
Title: Resident Management System
Acronym: RMS
Project Manager: Haskell Barker
PM Phone: 760-247-0217
Technical PM:
Technical PM Phone:
Operating System: UNIX, Windows 2000 / XP
Database Language: Dbase, Xbase equivalent, Oracle
Programming Language: C, C++
Arch Type: Client Server, Standalone
Hosted by CEEIS:
Lines of Code:
Comm Req: CEEIS
Total Num of Users: 250
Concurrent Users: 1500
Systems Interfaced: CEFMS, PROMIS, P2
DITSCAP: Yes
COOP: Yes
Run Time: 20 Hrs
Down Time: 3 Days

Appendix R – Information Assurance in the U.S. Army Corps of Engineers



R.1 Background

The U.S. Army Corps of Engineers (Figure R.1) is the Nation's primary public engineering agency, with Civil Works, Military Programs, and Emergency Operations missions. Within the Civil Works Program, the Corps handles water control, rivers and harbors, environmental restoration, and power generation.

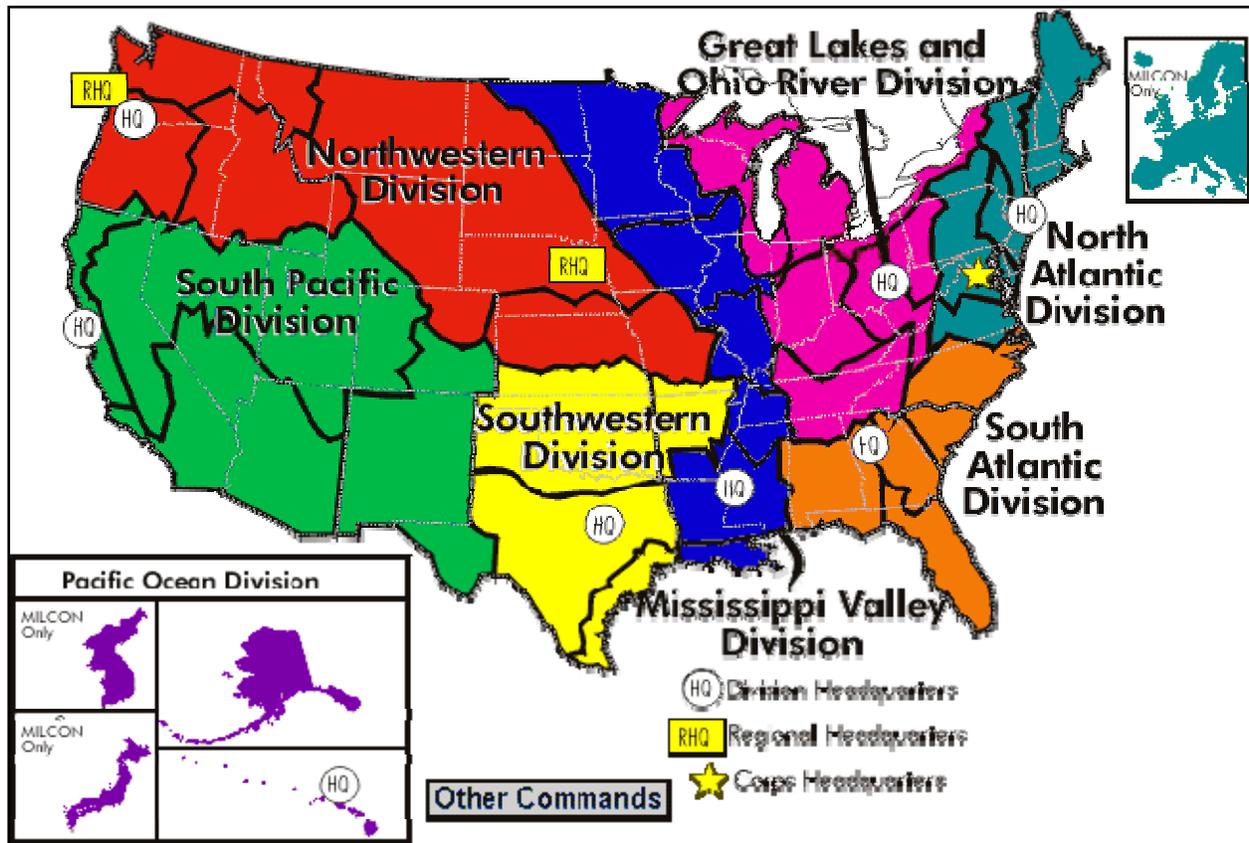


Figure R.1. Civil boundaries of the Corps

Within the Military Programs mission the Corps supplies support to the Army, the Air Force, and other Federal agencies for general construction, operations and maintenance, and direct military mission support (Figure R.2).

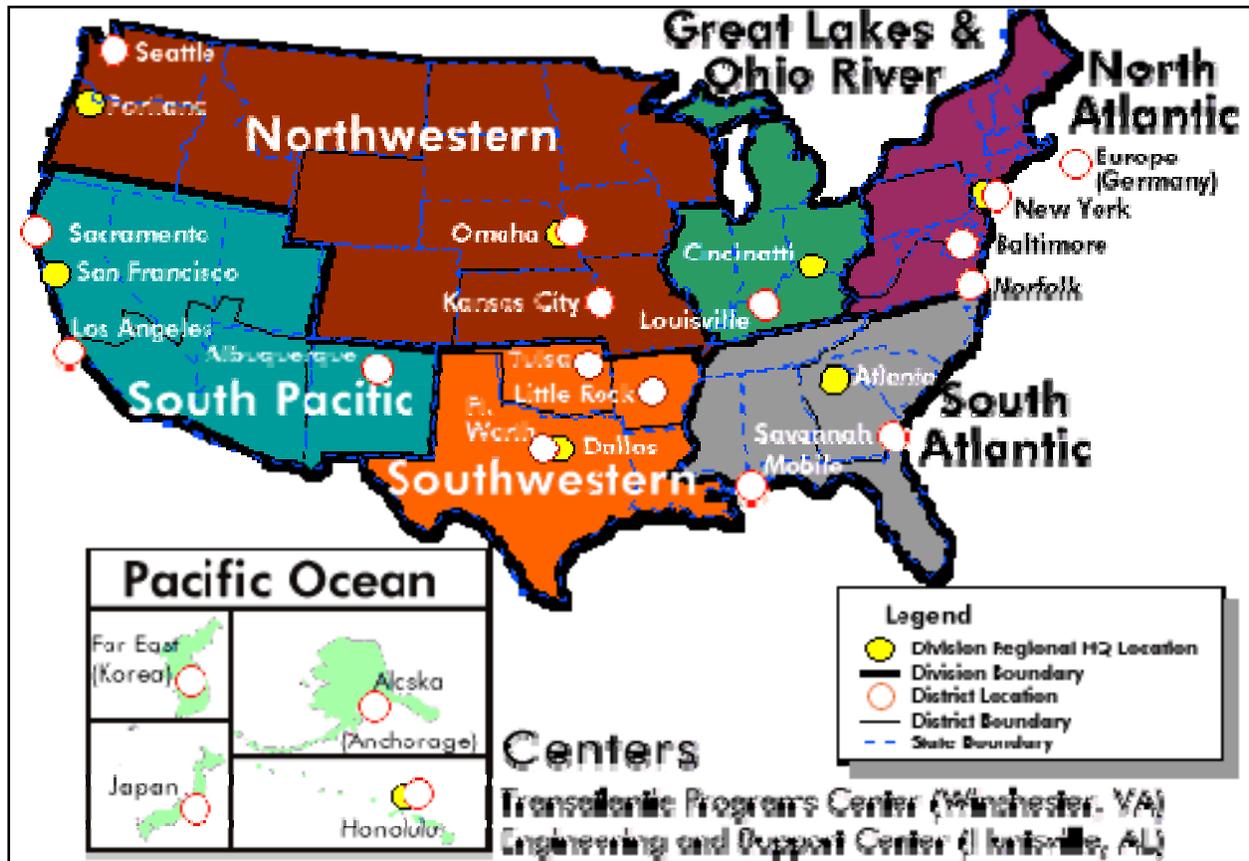


Figure R.2. Military boundaries of the Corps

Within our Emergency Operations Mission, we support the FEMA and various state and local Emergency Response Centers in dealing with earthquakes, hurricanes, floods, tornadoes and other natural disasters including terrorist attacks.

R.2 Corps of Engineers Computer Network

The information flow necessary to support these activities is supported through the Corps of Engineers Enterprise Information system (CEEIS) network, which provides backbone communications and data services, information processing for corporate information systems, and, through a corporate enterprise information architecture, data and information at the desktop, to Corps personnel and managers at all levels.

CEEIS is composed of two Internet gateways, two information processing centers at Vicksburg, MS, and Portland, OR, and T-1 connections into the FTS2001 network with 45-Mbps connections at the processing centers. This network provides for the passing of data and message traffic between Corps sites in support of engineering, financial, e-mail, water control and other USACE Business functions as well as providing connectivity to a high number of external customers and partners, both military and nonmilitary. These customers access USACE systems and data via the Internet

gateways at selected sites. CEEIS uses CISCO routers and Frame Relay to maximize the effective use of available bandwidth. CEEIS also provides connectivity to the DoD Secure Internet Protocol Router Network (SIPRNET) to support military missions and provide command and control capability for the Chief of Engineers. Riding the CEEIS network/processing center infrastructure in turn, and supporting the business processes which comprise our Civil Works, Military Programs, and Emergency Operations mission areas, is the Corps logical information architecture including all mission-essential AIS.

R.3 Information Infrastructure Protection Plan

The Directorate of Corporate Information's Information Infrastructure Protection Plan is a set of ongoing activities focused on enabling and sustaining the Information Infrastructure Protection Program over the long run. These ongoing sustainment activities focus on technological awareness/capability enhancement, developing and protecting the workforce, and developing and/or implementing policies and procedures to accomplish the first two.

R.3.1 Responsibilities

Under Department of Army Regulation AR 25-2, Information Assurance, which may be accessed through the Policy and Guidance Web page of the Defense Information Systems Agency, <http://iase.disa.mil/policy.html>, paragraph 2-7:

2-7. Commanders of MACOMs; Chief, Army Reserve (CAR); Chief, National Guard Bureau (NGB); program executive officers (PEOs); direct reporting program managers; NETCOM RCIOs; direct reporting units (DRUs); Installation Management Agency (IMA); and the Administrative Assistant to the Secretary of the Army

Commanders of MACOMs; Chief, Army Reserve; Chief, National Guard Bureau; Program Executive Officers; direct reporting program managers (PMs not under the PEO structure); NETCOM RCIOs; direct reporting units; Installation Management Agency; and the Administrative Assistant to the Secretary of the Army (acting as the senior official for all HQDA administrative and management services), in addition to the responsibilities defined in paragraph 2-2 [of this regulation], will —

- a. Develop and implement an IA program with the hardware, software, tools, personnel, and infrastructure necessary to fill the IA positions and execute the duties and responsibilities outlined in this regulation.
- b. Oversee the maintenance, documentation, and updating of the certification and accreditation (C&A) requirements required for the operation of all ISs as directed in this regulation.
- c. Implement and manage IT system configurations, including performing IAVM processes as directed by this regulation.

- d. Appoint IA and other personnel (for example, alternates) to perform the duties in chapter 3 of this regulation and provide IAPM POC information to the NETCOM RCIO, supporting Regional Computer Emergency Response Teams (RCERTs)/Theater Network Operations and Security Centers (TNOSCs), and the Army Computer Emergency Response Team (ACERT). MACOM IAPMs will report to the RCIO of the region in which the headquarters is physically located.
- e. Appoint or approve DAAs as required.
- f. Establish an oversight mechanism to validate the consistent implementation of IA security policy across their areas of responsibility.
- g. Oversee annual security education, training, and awareness programs to all users that address, at a minimum, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.
- h. Oversee the implementation of IA capabilities.
- i. Incorporate IA and security as an element of the system life-cycle process.
- j. Develop and implement an AUP for all users for privately owned equipment (for example, cell phones, personal digital assistants (PDAs), wireless devices) and ISs prohibited during training exercises, deployments, and tactical operations. Incorporate, as a minimum, the prohibition of utilizing such devices or the limitations of acceptable use, as well as the threat of operational exposure represented by these devices in garrison, pre-deployment staging, tactical, and operational areas.
- k. Develop procedures for immediate notification and recall of IA personnel as assigned.
- l. Report security violations and incidents to the servicing RCERT in accordance with Section VIII , Incident and Intrusion Reporting.
- m. Adhere to and implement the procedures of the networthiness certification process.
- n. Program, execute, and report management decision packages (MDEPs) MS4X and MX5T resource requirements

Within the Corps of Engineers, the Chief of Engineers, as MACOM Commander, has delegated program management responsibilities for enterprise Information Assurance (IA) to the Chief Information Officer (CIO), who heads the Directorate of Information Management (DIM), within the Headquarters USACE. Within the DIM, Information Assurance (IA) responsibilities, including the position of Information Assurance Program Manager (IAPM) are resident with the Information Assurance Division (CECI-A), which was instituted as a separate divisional element in 2002, subsequent to the 2001 Federal Information System Controls Audit Manual (FISCAM) audit. The Division's mission is to *"Provide planning and management of the USACE Information Assurance (IA) Program to ensure the confidentiality, integrity, and availability of information processed by the USACE information-based systems."* This includes providing a measure of confidence

that the security features, practices, procedures, and architecture of each information system accurately implements and enforces security policies.

In the post 9/11 world, the Corps, like other Federal agencies, finds itself coping with a world greatly changed. Where previously the Command was concerned primarily with denial of service or fiscal/property impacts, today we must contend with threats of physical harm to American citizens caused by cyber intrusion directed against Corps operational assets. The change is neither trivial, nor simple to implement. The Corps is closely watching the Department of the Army's evolution of DA PAM 25-IA Information Management Information Assurance Implementation Guide (DRAFT) it is clear that the Corps will have to issue similar implementation guidance via an Engineer Regulation, although the timing of this is undetermined at this time.

R.3.2 Technology

The Corps missions are continually evolving, as is the technology available to support them. The introduction of new technologies or the implementation of existing technologies in new ways to support existing missions may result in the recognition or emergence of new threats to the operating environment. Among recent technological evolutions offering security risks or potential security enhancements are:

- “Wireless” technologies
- Portable Electronic Devices (PEDs)
- Software auditing tools

Various wireless technologies offer tempting capabilities to the managerial problem solver while posing considerable risks to the enterprise. Wireless technologies are generally based on some variation of the IEEE 802.11, which lacks secure cryptographic capability. While extremely flexible in their general mobility and utility, personal electronic devices such as Personal Digital Assistants (PDA's) lack any meaningful secure capability, and can, if improperly implemented, offer a window of vulnerability into the enterprise.

Software auditing tools offer the enterprise the opportunity to rapidly test for multiple vulnerabilities in a thorough and cost-effective manner. Tools such as **Internet Scanner** and SafeSuite **Database Scanner** by Internet Security Systems, which have recently been ordered, will significantly improve the enterprise's ability to ascertain its security vulnerability status by performing automated probes of communication services and devices, operating systems, and applications including database systems implementations in support of corporate AIS.

Among existing technologies facing new scrutiny are the Corps Supervisory Control and Data Acquisition (SCADA) systems, which manage our power generation capabilities, with minimal supervision in many cases, as well as implementing a significant portion of our flood control operations. Occurrences such as the recent Northeast blackout, as well as ongoing efforts to protect against and mitigate any possible effects of cyber

terrorism, have led to the formation of a Project Delivery Team (PDT) comprising Headquarters security personnel and engineering personnel in the Field Operating Agencies (FOAs), which is addressing improving the security of SCADA systems.

R.3.3 People

People are the heart of any of any security program – they are the greatest enabler and the greatest vulnerability. In accordance with AR 25-2, Information Assurance, security awareness begins when the employee is brought onboard. New employees are first briefed by the Security Monitor for the Division, and anyone new to the DoD and/or the Department of the Army is acquainted with AR 25-2, which is the generally governing regulation.

After the initial personnel level, the security hierarchy within the enterprise follows the structures laid out in AR 25-2. At the fundamental level is the Systems Administrator (SA) – responsible for the security of a single AIS, in all its self-determined aspects. At the next level up is the Information Assurance Security Officer (IASO). The IASO is typically responsible for security at the workgroup or Local Area Network (LAN) level. Above the IASO is the Information Assurance Manager (IAM) who is responsible for security at the Division or District level. At the head of the security “pyramid” is the Information Assurance Program Manager (IAPM) who is responsible for the security of the enterprise.

Security awareness must encompass not only vulnerabilities of/to computer systems, but also vulnerabilities of the individual for the enterprise involving various types of “social engineering” hacker exploits. Yearly Subversion and Espionage Directed Against the Army (SAEDA) briefings assist in maintaining awareness of these types of vulnerabilities, and preventing corporate compromise. While most social engineering penetration efforts are not directly destructive, they can create hidden vulnerabilities, which can be difficult and costly to rectify. All personnel also receive Yearly Information Security briefings to keep them current with emergent and emerging information security threats.

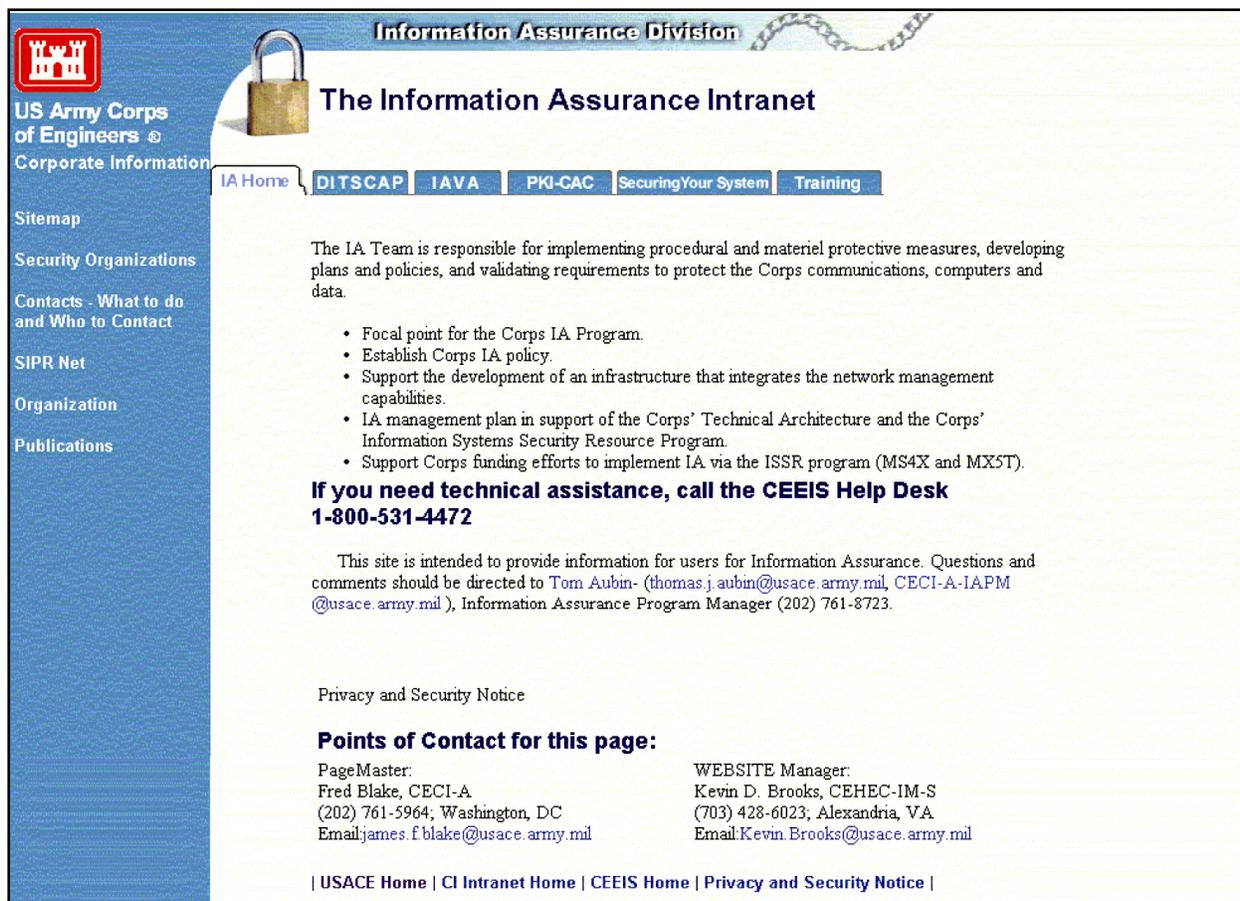
R.3.4 Procedures

Security procedures in the Corps are directive under a number of Army Regulations and DoD Directives and Instructions, including:

- AR 25-2 Information Assurance
- AR 380-53 Information Systems Security Monitoring
- AR 380-67 Personnel Security Program
- AR 530-01 Operations Security
- AR 25-1 Army Information Management
- DoD Directive 8000.1 Defense Information Management Program
- DoD Directive 8500.1 Information Assurance

- DoD Instruction (DoDIs) 8500.2 Information Assurance (IA) Implementation
- DoDI 5200.40 DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

among others. The Information Assurance Division (CECI-A) has summarized much of this directive information in operational form and placed it on the corporate intranet, available Corps-wide at <https://corpinfo.usace.army.mil/ci/ia>



The screenshot shows the 'Information Assurance Division' intranet page. The header includes the US Army Corps of Engineers logo and the title 'The Information Assurance Intranet'. A navigation menu contains links for 'IA Home', 'DITSCAP', 'IAVA', 'PKI-CAC', 'SecuringYour System', and 'Training'. The main content area describes the IA Team's responsibilities and lists key objectives:

- Focal point for the Corps IA Program.
- Establish Corps IA policy.
- Support the development of an infrastructure that integrates the network management capabilities.
- IA management plan in support of the Corps' Technical Architecture and the Corps' Information Systems Security Resource Program.
- Support Corps funding efforts to implement IA via the ISSR program (MS4X and MXST).

 A call to action states: 'If you need technical assistance, call the CEEIS Help Desk 1-800-531-4472'. Contact information for Tom Aubin and Kevin D. Brooks is provided. A footer contains links for 'USACE Home', 'CI Intranet Home', 'CEEIS Home', and 'Privacy and Security Notice'.

From the front page one can quickly go to information on any critical security function, such as incident reporting:



Information Assurance Division

Contacts - What to Do and Who to Contact

[IA Home](#) | [DITSCAP](#) | [IAVA](#) | [PKI-CAC](#) | [SecuringYour System](#) | [Training](#)

1. Immediately contact the CEEIS Help Desk at 1-800-531-4472. The Help Desk will notify Tom Aubin (thomas.j.aubin@usace.army.mil), Information Assurance Program Manager (202) 761-8723 or (202) 369-8281.
2. If you believe that you have a security issue that needs to be checked,
 - Make sure that you log everything you do and see. At a minimum document the following information:
 - the name and IP address of the machine,
 - the date,
 - source of the intrusion,
 - port numbers used,
 - strange or unusual files and programs found on the system.
 - Make backups of those logs onto another machine away from the machine you believe to be compromised.

[ACERT/RCERT Incident Submission Form](#)
[Virus Reporting Form](#)

This page is intended to provide System Security Information for users of the CEEIS network. All security questions and concerns should be directed to Tom Aubin- (thomas.j.aubin@usace.army.mil), Information System Security Program Manager (202) 761-8723.

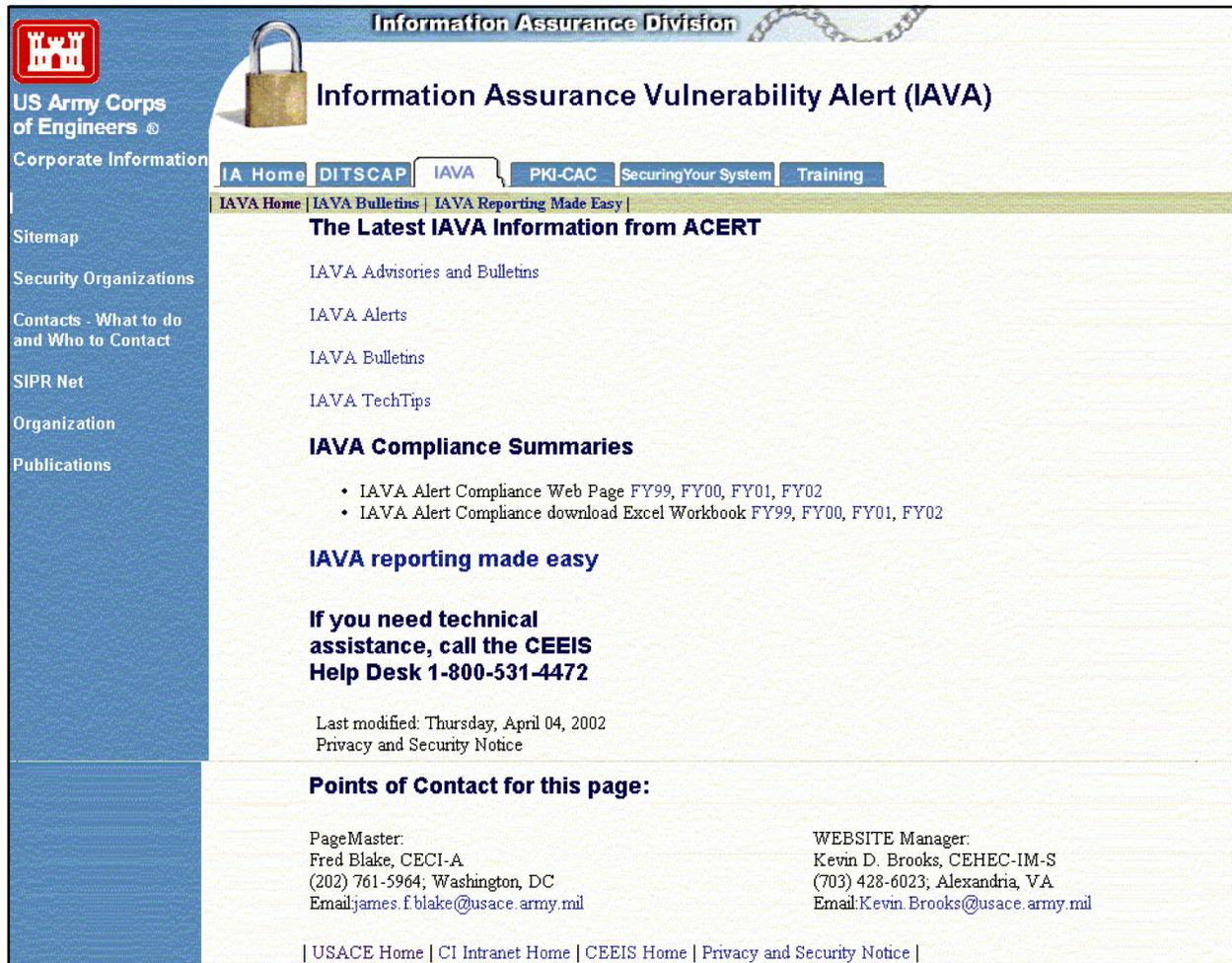
Last modified: Wednesday, April 10, 2002
[Privacy and Security Notice](#)

Points of Contact for this page:

PageMaster: Fred Blake, CECI-A (202) 761-5964; Washington, DC Email:james.f.blake@usace.army.mil	WEBSITE Manager: Kevin D. Brooks, CEHEC-IM-S (703) 428-6023; Alexandria, VA Email:Kevin.Brooks@usace.army.mil
---	--

| [USACE Home](#) | [CI Intranet Home](#) | [CEEIS Home](#) | [Privacy and Security Notice](#) |

or how to handle IAVAs from DA and/or DoD



Information Assurance Division

Information Assurance Vulnerability Alert (IAVA)

US Army Corps of Engineers ©

Corporate Information

IA Home | DITSCAP | IAVA | PKI-CAC | SecuringYour System | Training

IAVA Home | IAVA Bulletins | IAVA Reporting Made Easy |

The Latest IAVA Information from ACERT

IAVA Advisories and Bulletins

IAVA Alerts

IAVA Bulletins

IAVA TechTips

IAVA Compliance Summaries

- IAVA Alert Compliance Web Page FY99, FY00, FY01, FY02
- IAVA Alert Compliance download Excel Workbook FY99, FY00, FY01, FY02

IAVA reporting made easy

If you need technical assistance, call the CEEIS Help Desk 1-800-531-4472

Last modified: Thursday, April 04, 2002
Privacy and Security Notice

Points of Contact for this page:

<p>PageMaster: Fred Blake, CECI-A (202) 761-5964; Washington, DC Email:james.f.blake@usace.army.mil</p>	<p>WEBSITE Manager: Kevin D. Brooks, CEHEC-IM-S (703) 428-6023; Alexandria, VA Email:Kevin.Brooks@usace.army.mil</p>
---	--

| USACE Home | CI Intranet Home | CEEIS Home | Privacy and Security Notice |

or any of the other critical functions that the Information Assurance Division (CECI-A) is involved in.

The ultimate security and survival guarantor is a robust Continuity of Operations (COOP) plan as required by AR 25-2. Each of the Corps CEEIS processing centers acts as a COOP site for the other. In the event of a COOP execution requirement, some degradation of service is inevitable, as is a requirement for 24/7 operations by AIS users. "Excess" capacity is insufficient to support anything *more* than degraded mode operations. Nonetheless continued operations in the face of significant loss of processing capacity is possible. COOP is executed by each processing center on a regular schedule, but also by the AIS systems administrators.

R.4 Information Infrastructure Program

R.4.1 Physical Information Infrastructure

The Corps uses a “defense in depth” strategy for its information infrastructure (Figure R.3), beginning with “firewalls” at every network entrance point.

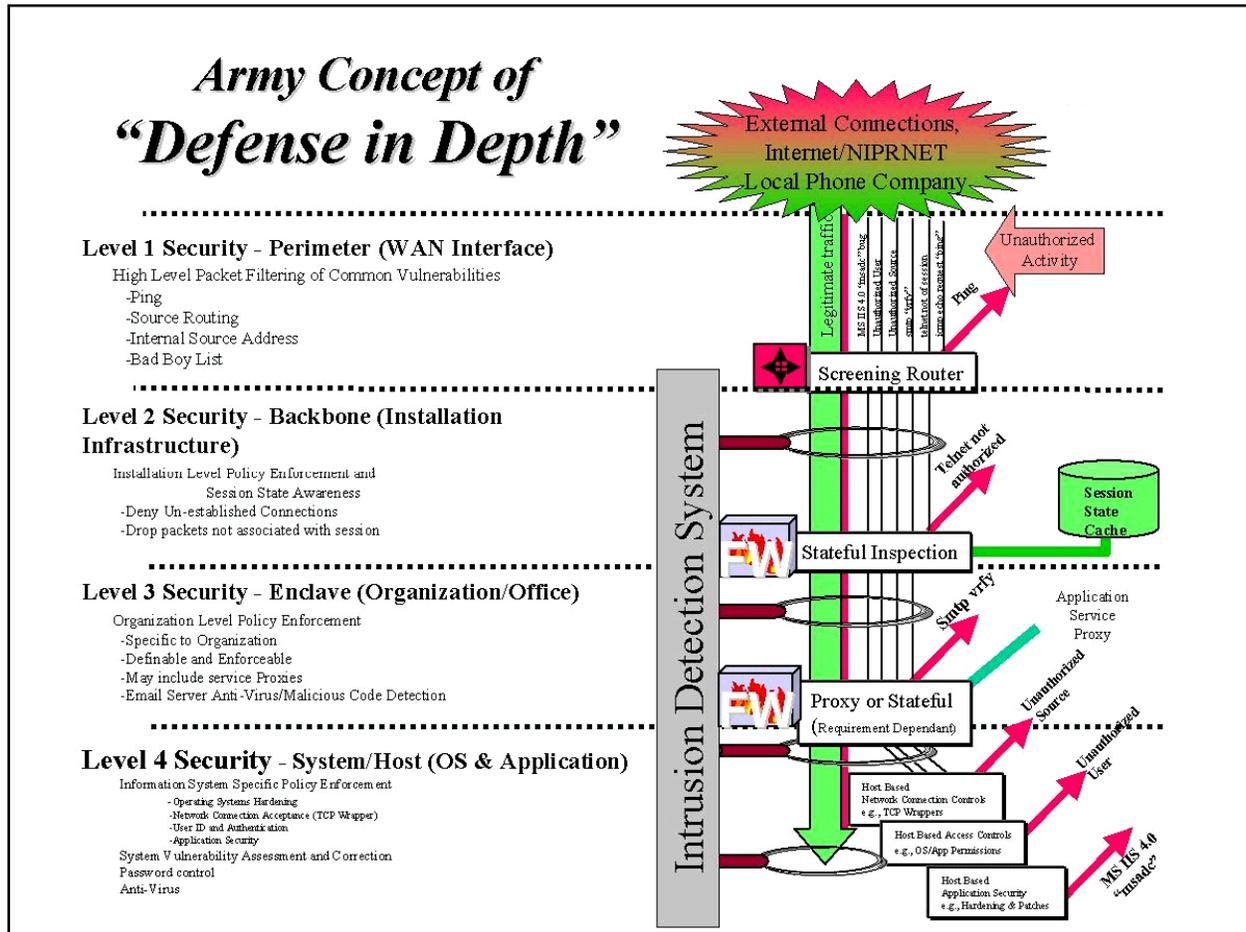


Figure R.3. The Corps “Defense in Depth” strategy

Information/data traffic entering the Corps first encounters an Army supplied router (ASR), and then a **Real Secure** intrusion detection system (IDS) managed by the Army’s Technical Network Operating Security Center (TNOSC) at Fort Huachuca. Subsequently the traffic encounters a Corps-operated gateway firewall. The Corps uses **Guantlet** firewalls supplied by NAI Corporation, and approved by the Department of the Army (DA). The Corps firewalls are centrally managed by the Network Operations Center (NOC) in Portland, OR, and Vicksburg, MS. The two sites provide continuous operational support (24/7/365). The CEEIS NOC is responsible for keeping the firewalls under constant observation and updating the “rules base” by which each firewall filters incoming traffic, based on Security Advisories from the Army Computer Emergency Response Team (ACERT).

After passing the gateway firewall, traffic encounters an additional CEEIS-managed **Real Secure** IDS (Figure R.4). Incoming e-mail is initially filtered for hostile traffic at the mail servers in Portland and Vicksburg using **Antigen** anti-virus/anti-spam software; it is further filtered at the servers in the Field Operating Activities (FOA) using **Norton** anti-virus, and finally filtered at the desktop by either the **McAfee** or **Norton** anti-virus, which are also provided to those who access the system remotely. As a result of using defense in depth with multiple anti-virus engines, recent internet worm/Trojan attacks, while unavoidable, have had minimum impact on enterprise operations. Remote system access, in accordance with DA policy, is permitted only to modem pools employing the remote authentication dial-in user system (RADIUS) standard. Security at the desktop is further enhanced by the use of password-protected screen saver “timeouts” as well as the implementation of virtual private networks (VPNs) for teleworkers.

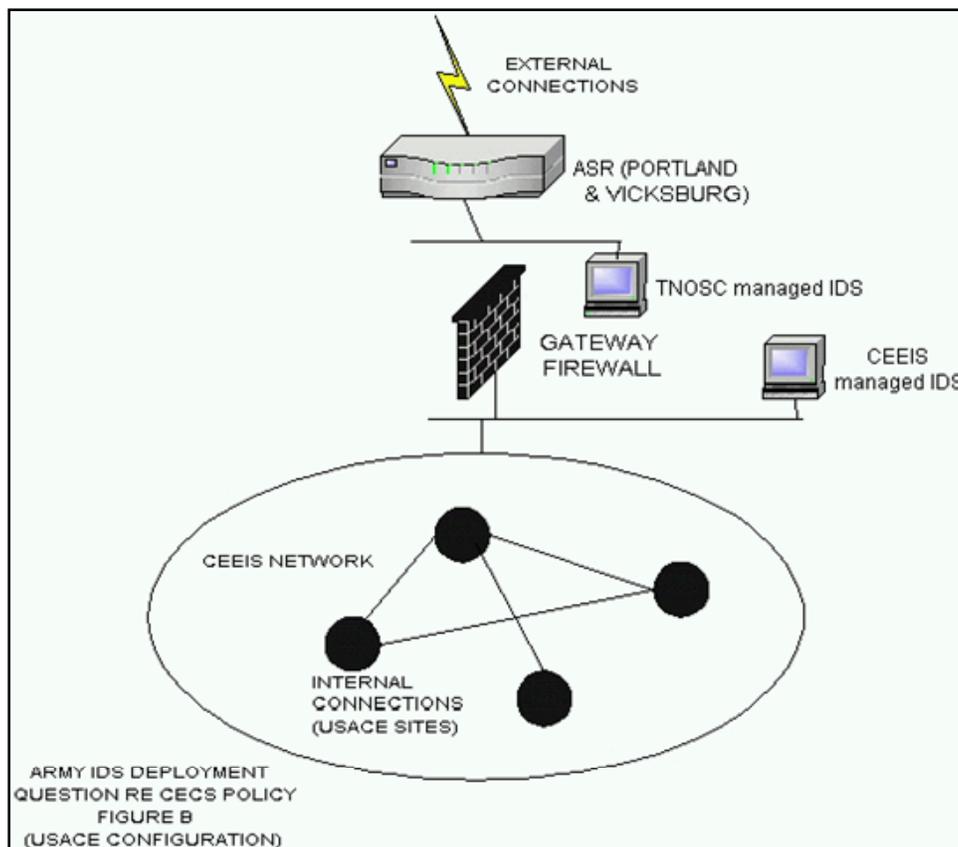


Figure R.4. Army IDS

Operationally, the applications, network and the enterprise components to the FOA level, have been, or are being, subject to ongoing security accreditation and review under the Defense Information Technology Security Certification and Accreditation Process (DITSCAP). DITSCAP is an intensive standardized four-phase security certification process consisting of Definition, Verification, Validation, and Post Accreditation phases. DITSCAP is based upon the National Institute of Standards and Technology (NIST) guidelines as implemented in a DoD environment. The DITSCAP

process provides vulnerability assessments for the system or subsystem under review, as well as detailed procedural documentation for determining, securing, and maintaining the security of a given program, FOA, or AIS. Security of the network is critical, because information, which travels the network, including Water Control data, inland waterways traffic usage data, and emergency operations support (ENGLink) data, is not only mission critical but also life critical.

In addition to responding to Information Assurance Vulnerability Alerts (IAVAs) as required by DoD and the Department of the Army, the Corps regularly performs internal assessment testing to identify vulnerabilities. Assessment testing involves not only penetration testing for known vulnerabilities in network control systems and processing center operating systems, but also “war dialing” to identify violations of general security access and control policy via unauthorized modems.

Ideally, all Corps servers and sites would be scanned for vulnerabilities every 6 months and the results reported to the IAPM and the CIO. Current manpower restrictions inhibit this, but the acquisition of the **INTERNET SCANNER** software, currently underway, should significantly improve the Corps capabilities in this regard. Although we currently capture assessment results in a database, there is, at present, no feedback capability from the assessment subject, nor any automated upward reporting capability; this was proposed as an automation initiative for 2003.

Incident response procedures follow the Computer Emergency Response Team (CERT) guidelines for detection checklists and report formats, and flow through the chain of command in parallel, to the Information Assurance Manager/Officer (IAM/IAO), the IAPM and the CEEIS Security Operations Center (SOC). Incidents are promptly reported and worked with the appropriate levels within Army (ACERT/CID) and other agencies (FBI/CID).

To further enhance the Corps security posture, enterprise data has been partitioned into “publicly accessible” data sets, and private or enterprise data sets. Publicly accessible data sets comprise data generally available for the public good, such as the data on the availability of space in recreation areas; data available for public safety, such as water control data; and data available for public planning, such as data on the progress of the South Everglades Restoration Project. Publicly accessible data sets are “quarantined” away from “production” enterprise data sets supporting daily mission operations using controlled Internet accessible segments (CIAS) versus the Internet-accessible segments allowed internal enterprise users (Figure R.5).

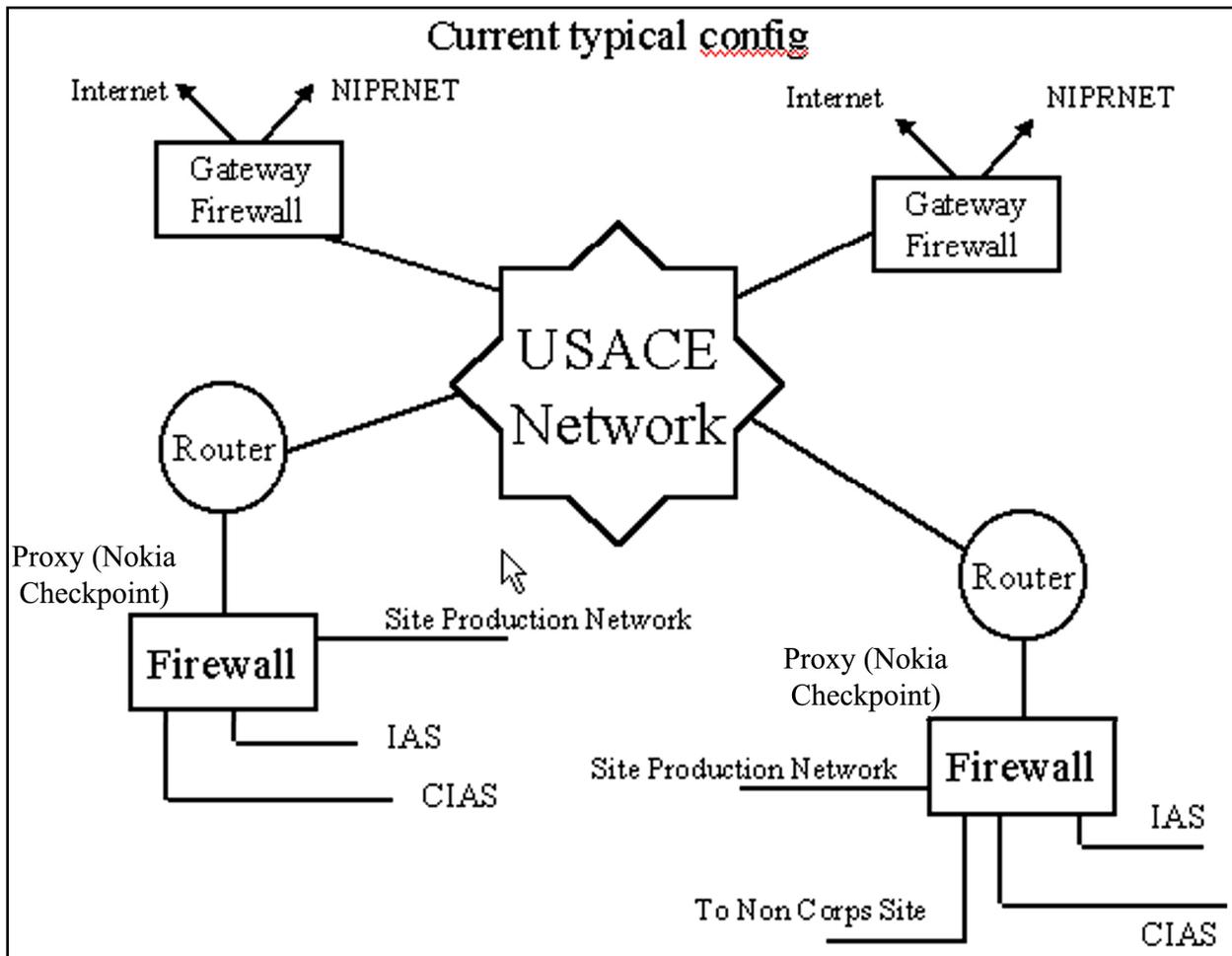


Figure R.5. Current typical configuration of USACE network

Future enhancements to the Corps information security posture, either underway or in planning, include:

- Adoption of the DoD Common Access Card (CAC) as the single network access token, with eventual migration to its use as the single point of entry, for both physical network access and logical data access.
- Public Key Enabling of the network, and selected information systems resident thereon to use the Public Key Infrastructure (PKI) certificates on the CAC as an enhanced authentication mechanism, as required by DA/DoD directives, if supported by a business case based upon sound risk assessments.

R.4.2 Logical Information Infrastructure

The Corps' logical information infrastructure consists multiple information systems, which support major Corps mission areas, or business processes, which in turn support those business areas. These AIS either have been, or are in the process of being

accredited with a DITSCAP review. To facilitate this, in 2001, the Corps invested \$1.6M in 100 copies of the XACTA tool by TELOS Corporation, which automates and simplifies the DITSCAP process. Additionally training and support for 3 years was also acquired under the same acquisition.

All AIS on the CEEIS network are password access controlled, both at the network access, and again at the information system access level. The corporate information systems database management system standard is ORACLE, which has a robust security architecture. The Corps AIS are implemented in ORACLE and take advantage of these security features, including the use of:

- **User-id's/Passwords** – independent passwords are issued for ORACLE access to selected databases.
- **Product user profile table** – users are restricted to the *specific* tools within the ORACLE tool suite necessary to accomplish their *specific* tasks within the AIS framework.
- **Roles** – roles are predefined object and system privileges which grant different classes of users the necessary capabilities to accomplish their tasks within the AIS framework.
- **Views** – views are used to segregate data access, permitting users to access *only* the data necessary to accomplish their tasks.
- **Encryption of data in Web applications** – depending on the specific applications requirement, Web-enabled applications may encrypt the session between the browser and the server (encryption is native to the ORACLE suite and may or may not include the use of the Secure Sockets Layer (SSL) protocols.
- **Auditing** – some applications make extensive use of how and when given SQL capabilities are executed, as well as how data definitions and data manipulation are executed.

The Corps was a pioneer within DoD in reducing paperwork and adopting electronic signatures (e-sigs). The Corps of Engineers Financial Management System (CEFMS) has incorporated e-sigs as a keystone of secure financial operations since 1994. The Corps is presently migrating this current secure e-sig standard from the FIPS 140-1 to a more robust PKI enabled FIPS 140-2 e-sig, in a cooperative effort between the Corps and the NIST, with oversight by the Government Accounting Office (GAO), who pioneered this process with us. At the same time, we will be cooperatively defining the requirements for a “secure Web enabled” application. This effort is being funded using DA RDT&E monies made available for this purpose as a result of CEFMS being a “legacy” electronic signatures (e-sig) system.

The Corps AIS are managed under an ongoing life cycle management of information systems (LCMIS) process, with security reviews included as a normal part of the systems architecture, design, and acceptance process. Under Army guidance,

additional AIS will be considered for migration to PKI enablement based upon risk assessments and sound business case review.

R.5 Ongoing Internal/External Reviews and Related Efforts

R.5.1 Health of the Network Study

As part of our efforts to maintain efficiency and enhance security, the Directorate of Information Management commissioned a Communications Architecture Assessment, which was completed in October of 2000. This study addressed network performance, documented our bandwidth deficiencies and some of the causes thereof, and projected the expected trends that we would have to deal with in the coming years. As a result of this study, the Corps acquired and installed **Sitara** network traffic prioritizers, and installed caching servers at selected sites to improve throughput.

In addition, the Corps conducted an Enterprise Management Systems (EMS) Pilot in partnership with our South Atlantic Division, deploying the **CA Unicenter** EMS products recommended by DA, to test the ability of these products to enhance management's "span of control," improve scarce personnel utilization, and offer improved security opportunities. This successful pilot demonstrated the potential for considerable improvement in efficiencies of operation at the field level, given adequate standardization and sufficient infrastructure investment.

R.5.2 External Reviews

R.5.2.1 Financial Information Systems Audit Control Manual (FISCAM):

During 2002, GAO in combination with the Corps Inspector General (IG) and the Army Audit Agency (AAA) participated in extensive Financial Management (FISCAM) reviews of general and applications controls. Through the use of a private contractor (Price-Waterhouse Coopers), these audits have identified weaknesses in the areas of:

- Access controls
- Software
- Segregation of duties

In response to this, access controls in the form of firewalls and intrusion detection systems are now monitored 24/7/365. New and stricter authentication procedures have been established at the INTERNET gateways and at each individual server. We have also implemented both random and "by request" inspection procedures to look for system vulnerabilities and unauthorized access through modem dial-up (using war-dialing techniques, as referenced previously).

We continue to limit physical access to devices or computer rooms via keypad access control locks, and we limit the number of persons having access as much as possible.

In areas where changes were not technically or fiscally possible, we have put in place other procedures to mitigate the security risks.

R.5.2.2 Army Audit Agency (AAA) Reviews:

During 2003, the AAA completed a separate and in-depth review of the Corps GAO sanctioned CEFMS electronic signature (e-sig) process. This review identified some operational policy issues, some of which may be mitigated by the issuance of the proposed AR 25-2 combined with the PKI enabling of CEFMS – which will require an additional 18-24 months to complete and implement. In the interim, the enterprise will re-emphasize the training of e-sig users in their responsibilities for sound fiscal management at the individual level. Technical policy issues will be addressed by additional procedural guidance issued through the CEFMS Project Office.

R.5.2.3 DoD Inspector General Audit of Previous Audit Efforts:

In July 2003, in response to a request by the Under Secretary of Defense (Comptroller)/Chief Financial Officer, the DoD IG initiated an audit of the follow-up on the GAO and AAA audit efforts. The scope of this effort includes CEEIS, the Corps Finance Center in Millington, TN, the Systems Development and Maintenance Directorate in Huntsville, AL, and selected field sites. The Corps is cooperating fully, and has already successfully demonstrated our corrective responses to some of the issues identified in the previous audits.

A separate audit review of previously identified issues in CEEIS alone began in February 2003 and is ongoing.

R.6 CEEIS Security Architecture Description

The following is a description of the USACE security architecture as it relates to the use of routers, firewalls and other security components to create a multi-tiered security infrastructure. This plan addresses the various information security threats to USACE and what the CEEIS program does to address these threats. It also identifies those areas that need improvement or that fall into the jurisdiction of local USACE sites to address. The description begins by describing the basic USACE network infrastructure and requirements for access. It then describes what known threats there would be to USACE if a security architecture were not in place. The text then describes the current security architecture in USACE and then evaluates each of the identified threats against the deployed configuration.

R.6.1 Network Descriptions

R.6.1.1 USACE network

USACE has a top-level, enterprise managed network infrastructure that interconnects all Corps sites at the FOA level. This includes approximately 70 major sites worldwide. In addition to these sites, many Corps sites also have connections up to local project offices. In some cases, sites have as many as 50 project offices, field offices, construction offices, dams and locks that are interconnected. This backbone network is

composed of T-1 frame relay connections into the Sprint and MCI FTS2001 frame clouds. In order to handle the traffic load of those applications that are centralized, there are 45-Mbps connections to each processing center from both Sprint and MCI. This network provides for the passing of traffic between Corps sites in support of engineering, financial, e-mail, real-time data collection and other USACE business functions. In addition, USACE has a very high number of external customers both military and non-military. These customers access USACE systems via the Internet gateways at the centers.

R.6.1.2 Primary external connections

In order to provide USACE staff access to non-Corps systems and to provide access by external customers to USACE systems, there are two external gateways located in Portland, OR, and Vicksburg, MS. These gateways provide 45-Mbps connections at each gateway site

R.6.1.3 Other external connections

At a few Corps sites there are also external connections to other agency networks in support of the Corps mission. These include EPA, USFS, USBR, NOAA, and other Federal, State and local entities.

R.6.1.4 Systems descriptions

- **Windows** – The USACE primary desktop computing infrastructure is Windows based and is used for office automation, e-mail, groupware access, access to corporate systems, systems at other Corps sites and systems outside the Corps.
- **E-mail** – Corps sites run MS Exchange servers in support of corporate e-mail and other collaboration functions (tasking, calendaring, etc). There is also some SMTP traffic that flows directly to UNIX workstations inside USACE. In addition, the CEEIS office is responsible for the e-mail infrastructure at the enterprise level. The routing of e-mail has a part in the overall security architecture and will be further described in this appendix.
- **Financial/business processing** – most financial and business processing in the Corps is based on thin-client/server configurations. The client systems are Windows based residing on the customer's desktop and the servers are typically Sun/Solaris based. Many applications are Web-based through the use of Oracle's Java engine.
- **Solaris** – There are two processing centers in the Corps that operate the primary business systems, one in Portland, OR, and one in Vicksburg, MS. These systems house a number of large multiprocessor Sun systems running Solaris.
- **MTS** – Some of the deployed application use the Microsoft Terminal Server (MTS) system. There are a number of large enterprise class W2K based servers located at the centers in support of MTS.
- **Database** – Most databases in use in the Corps are Oracle based. A few databases in use are built on Sybase.

R.6.2 External Customers

R.6.2.1 Civil works

The Corps has a large number of external customers that require access to Corps provided/generated data. This includes the posting and retrieval of information for water management functions, ACASS (DoD-wide architect/engineer registration system), retrieval of permit information/status, and regulatory information. In addition, the Corps is required to provide information to the public for fish studies and real-time fish count status, lockage reports (for commercial traffic processed through locks), and power generation reports (rolled-up and real-time). Some of the interfaces to the public involve “life and property” responsibilities as it relates to flood control information distribution, river levels and other related information.

R.6.2.2 External Corps employees

A number of Corps employees are located external to the Corps network. This includes those on work-at-home programs, DSL connections, ISDN, modems, construction staff on military bases and those in travel status.

R.6.2.3 Military funded customers

Since the Corps does a significant amount of military construction, there are various reports and data that the customer needs access to in order to track the execution and status of their project. This mission also requires access from outside the Corps network to internal USACE data. In addition, many Corps employees are located on military bases and need access to USACE internal systems.

R.6.3 Threats

The following outlines some of the basic threats to the USACE infrastructure that must be addressed within the deployed security architecture. These are common threats that would exist on any systems that are exposed to other systems and all pose a risk to the infrastructure. Later sections of this plan will outline what is done within the USACE security architecture to reduce the risk of these attacks occurring, or if they occur, reduce the scope of impact.

R.6.3.1 Internal corporately managed systems used as platforms to attack

If a site missed applying up-to-date patches on systems, these systems could be vulnerable to attack from within and from outside. Once compromised, these systems could be used to launch attacks against other systems within USACE.

R.6.3.2 Internal noncorporately managed systems used as platforms to attack USACE

Although systems administrators of known production systems regularly apply security patches and follow established security procedures, there are a large number of systems outside the realm of the Information Technology support staff that may fall through the cracks and leave other Corps systems vulnerable. These systems could be attacked, access could be gained and the platform would then be used to attack internal

USACE systems. This would make the traffic look like it was coming from inside the Corps, which could pose difficult to track.

R.6.3.3 Internal systems used as platforms to attack on Internet

While these attacks do not represent a risk to USACE internal systems, they do represent a risk to other external networks. These types of attacks must be prevented in order to remain good Internet “citizens.” There are actions that USACE can take to protect these networks from attack by USACE systems. However, much of the responsibility is in the hands of those who administer these remote systems and the level of trust that they give to systems external to their security boundaries.

R.6.3.4 Defacement of sites

Another possibility would be that those outside USACE may break into a system within USACE that is used to publish information internally or externally and replace the content either to embarrass USACE or make a political statement.

R.6.3.5 Denial of Service

Through the use of Distributed DOS attacks, there is a possibility that the bandwidth in/out of USACE would be consumed. This would deny service to valid internal or external customers.

R.6.3.6 .mil address

The fact that USACE addresses are followed by a .mil makes USACE an attractive target.

R.6.3.7 External access

There is a large amount of data provided to entities outside USACE including the public, other agencies, state and local governments, etc. In many cases, this access is required under Federal law or court order. In addition, public access to some data is crucial and the public’s inability to access systems can result in congressional complaints. For this reason, strict limitations on outside access are difficult to implement.

R.6.3.8 Decentralized information collection

USACE has investigated the possibility of consolidating all public accessible information at the gateways and locating these systems outside the firewalls. In many cases, however, the information that needs to be posted on these servers is gathered at each USACE site using automated data collection processes. As such the volume of information that would need to be transferred from each Corps site to central information distribution servers would be significant and not be cost effective to support over WAN links.

R.6.3.9 DNS

Each site provides systems administration support for their DNS infrastructure. This protocol could be used to map and attack USACE systems.

R.6.3.10 SMTP e-mail

Many systems within USACE are running the SMTP daemon which if not watched and patched diligently can also provide unintended access for external systems including violation of the system or use of the system as a spam relay agent.

R.6.3.11 Virus attack downloaded Web content

While viruses can propagate thru the e-mail system, they can also be downloaded from Web sites either through HTTP or HTTPS protocols.

R.6.3.12 Program (scumware) attack via Web

In the same way that viruses can be intentionally or accidentally downloaded to internal USACE workstations, these systems can also download and execute code that could install back doors or other types of utilities to provide for access to the system and possibly attack others.

R.6.3.13 Monitoring of unencrypted traffic from Internet to USACE

If traffic passes unencrypted from networks outside of USACE control, especially if they exist on a shared media like Ethernet or cable modems, they can be inspected and information can be gathered. There is a much lower probability of the traffic being monitored in nonbroadcast media like dedicated or frame circuits.

R.6.3.14 Mapping of the USACE infrastructure to gain information for an attack

Those wanting to launch attacks on USACE systems would use tools to scan and gather information about these systems prior to launching attacks.

R.6.3.15 Attack via unknown connection

In the following security plan, the concept of protecting connectivity outside of USACE is discussed. If there are connections to external entities that are not known, these connections could be used to violated the protections in place. This could be either a physical connection or a virtual connection using a VPN or encrypted stream.

R.6.3.16 Attack via in-dial

Attacks could be made thru the use of in-dial modem pools that have weak protections on them or accounts left active thru poor security procedures.

R.6.3.17 Foreign system attached to USACE local network

Either intentionally or un-intentionally, system could be violated if foreign, non-USACE administered systems were physically attached to the local network and used to either launch attacks locally, though the enterprise or spread malicious code.

R.6.3.18 Unsecured wireless access point

As wireless become more prevalent, this could be a major source of attacks through poorly configured or protected Wireless Access Points (WAPs) connection to the USACE network.

R.6.3.19 Unknown attacks

As technology advances in all areas, attacks could come from directions that are unknown and unsuspected. This will require that this security plan go thru major changes and require that deployed security architecture be able to be change rapidly to fend off these new attacks.

R.6.4 Description of Basic Concept

This section outlines the various components that make up the USACE security plan. This configuration is deployed in order to reduce or eliminate the threats described above.

R.6.4.1 Internet router

The Corps has two Internet connections, one in Portland, OR, and one in Vicksburg, MS. These connections are provided thru Cisco 7500 series routers. These routers have Access Control Lists (ACLs) that inspect traffic for various parameters and allow or deny traffic based on packet content. In this configuration, the router acts like a packet inspection filter. As it relates to Internet attacks, this is the 1st level of defense as most blocks that take place in this device apply to all systems within USACE.

- **Ports/protocols** – The ACLs on these routers block those ports and protocols that are not needed within USACE or that represent such a high risk that they are not allowed. This configuration prevents port scans on these blocked ports and partially prevents scans of USACE systems. This significantly reduces the exposure of the USACE network to attacks on these ports and reduces the ability to discover certain aspects about systems within the Corps.
- **Source addresses** – There are some source addresses that are not allowed in through these devices. Reasons for this include (1) addresses that have not been assigned by the Internet community, (2) reserved addresses that should not be coming toward the Corps, (3) Internal Corps addresses- since these would be seen coming from the outside it can be assumed that this would be “spoofed” traffic, (4) internal addresses being sent outside the Corps that do not belong to the USACE address space, and (5) addresses that have been deemed to be untrusted - this could be the result of a high level of attack activity or notices from other security sources that these source addresses should be blocked. This blocking provides a low level of risk management; however, the primary function is to make sure that traffic that does not belong inside USACE doesn't make it in the first place.

- **Remaining risks –**
 - *ACL leaks* – During heavy loading on the gateway routers, there is concern that packets may “leak” through the ACLs. The routers are designed primarily to route and as such are not specifically designed to act as firewalls. During heavy packet processing, there is a chance that routing will take precedence over packet filtering. Other portions of the USACE security configuration take this into account, such that the gateway router is not relied on as a security device.
 - *Log files* – there is a significant amount of information contained on the log files created off the gateway routers. The current CEEIS staff reviews these logs for major events but no correlation or long-term event tracking and data collection are performed.
 - *Future actions* – An activity that is currently unfunded related to the gateway routers is the creation of a logging server and database along with analysis software to perform correlation of the log files obtained off this router with the log files from other devices in the network.

R.6.4.2 Gateway firewall

As mentioned above, the Corps has two external connection points where the Internet connections are made. At each of these places, there are Cisco PIX firewalls. These devices act as the second layer of defense against attacks. These firewalls perform a number of functions related either to traffic entering or leaving the Corps. CEEIS Network Operations Security Center (NOSC) staff centrally manages them.

- **Ports and protocols** – While ports and protocols that do not belong inside USACE are blocked at the gateway routers, these are also placed into the PIX firewalls. As mentioned earlier, the router can, in some high-load cases, let through traffic that should have been blocked, whereas the PIX does not. This double blocking ensures that the majority of the blocking load takes place at the gateway routers but any traffic that “bleeds” through is stopped at the PIX.
- **Inbound traffic to IAS** – If a server needs to publish information to the public, this device is placed on an Internet Accessible Segment (IAS). Details related to this concept are contained elsewhere in this document. For those segments that are considered IASs, the IP address of this subnet is listed in the PIX firewalls with rules to allow certain traffic to be initiated from outside USACE to these segments.
- **Return-only traffic to Production** – For all other traffic through the PIX, only return traffic is allowed. Since the PIX is a stateful device, it keeps track of Transport Control Protocol (TCP) sessions and can determine if an incoming packet matches an internally generated request. With this rule in place, scans from external systems are not allowed since the scan packets do not have a corresponding outbound request.

- **SMTP traffic** – Currently there are a large number of systems within USACE that send and receive SMTP based e-mail traffic and as such are open to attacks based on the e-mail protocols. The PIX units are currently configured to allow SMTP traffic to Corps sites.
- **DNS traffic** – Currently DNS traffic is allowed into and out of all Corps sites. The current DNS configuration is such that while site servers are required to “forward-only” to specific gateway DNS servers, this configuration is not mandated thru firewall configuration until migration to the Army-protected DNS plan. In addition, internal USACE DNS servers are directly queried from external systems. This will also change after the migration to the Army DNS configuration.
- **VPN** – The VPN configuration is discussed later in this appendix. In order to support the VPN, the gateway firewall is configured to allow the inbound ports and protocols required to support Internet Protocol security (IPsec) traffic. This traffic is further restricted to the source/destination addresses of CEEIS-managed VPN concentrators.
- **Content filtering** – There are some instances where the gateway firewall is used to inspect URL content contained in Web requests or responses and based on the content, block traffic. This is commonly used for instances where a particular attack is based on a known URL request and as such is blocked from entering the USACE network even if it is returning as a reply to an internally generated request.
- **Firewall holes** – In order to provide support to some Corps sites for their external customer, there are some selected firewall holes that are created. These holes are the result of sites completing Firewall Action Requests (FAR), having these requests reviewed by the CEEIS team for security issues and implementing the hole. Some holes are created with a flag to remove them after a select period of time.
- **Remaining risks** –
 - *SMTP* – The passing of SMTP openly through the gateway firewall poses a risk in that poorly protected or misconfigured SMTP servers could be compromised and used to launch an attack, either internal or external.
 - *DNS* – There is a risk of attack or network mapping using the DNS protocol.
 - *Firewall holes* – The holes that are in the firewalls, at the request of internal customers, pose a risk in that attacks could either be launched from the site or spoofed from the address of the hole.
 - *Log files* – There is a significant amount of information contained on the log files created off the gateway firewalls. The current CEEIS staff reviews these logs for major events, but now correlation or long-term event tracking is performed.

- **Future actions –**
 - *Log analysis database* – An activity that is currently unfunded related to the gateway firewall is the creation of a logging server and database along with analysis software to perform correlation of the log files obtained off this gateway firewall with the log files from other devices in the network.
 - *SMTP* – The CEEIS office is developing configurations that would force all inbound and outbound SMTP e-mail through tightly managed servers located at the two centers. This would significantly reduce the exposure of USACE internal systems to SMTP attack. When this initiative has been completed, the gateway firewall would be configured to block all inbound and outbound SMTP traffic unless it was directed to the two e-mail gateway servers.
 - *DNS* – Upon migration to the Army-protected DNS configuration, internal DNS servers will be required to forward all of their requests to two protected DNS servers located at the centers. These servers will forward all of their outbound DNS requests to Army Tier 2 DNS servers. This configuration will move inbound DNS queries to the Army Tier 0 server. Once this migration is completed, the gateway firewall will be configured to block all inbound and outbound DNS unless it is coming from the Army servers and is destined for the protected DNS servers located at the centers.
 - *Firewall holes* – There is currently an intense effort by the CEEIS team to identify each firewall hole and work with sites to convert this to VPN where possible. In cases where VPN cannot be used and as such the hole needs to remain, filters will be placed into the IDS system at the gateway and site to more closely watch traffic from the source and destination of the hole. This will allow us to detect attacks that may come through these holes.

R.6.4.3 Site firewalls

As part of the multitiered Security infrastructure, USACE also has centrally managed firewalls located at each site. Traffic, upon passing through the PIX firewall, enters the network infrastructure composed of local connections, dedicated circuits and frame relay circuits. A basic tenet of the security policy is that for ANY connection to this cloud, there is a firewall in the path. These are Secure Computing Gauntlet firewalls on Sun Solaris systems. Since this is a proxy-based firewall, this also ensures that there are two different technologies in use within USACE for firewalls—stateful packet filters (PIX) and Gauntlet (proxies).

- **IAS** – One of the major functions of the site firewalls is to allow the creation of an IAS. This is a special LAN segment attached to the firewall that is configured to allow access from anywhere (Internet, Corps production, etc.). The limitation on the IAS, however, is that systems on the IAS cannot initiate traffic outside of the segment. This configuration prevents someone from gaining unauthorized access to systems on the IAS and then using this as a launching point to attack Corps production systems. This configuration also requires that any information

to be contained on systems that are located on the IAS must be pushed to this segment. In some cases, a large amount of data is collected on systems that are on the production segments. This data is then transferred (in real-time or on a schedule) to the system(s) on the IAS. For this reason, for these sites, it is best if the IAS is located at the same site as the production system that is gathering the information. This ensures that the bandwidth between these two segments is high and cost-effective (typically 100-Mbps LAN connections). The IAS configuration essentially creates a DMZ at each Corps site for location of IASs. This DMZ, unlike a typical DMZ that is located in front of the firewall, is configured such that additional security can be applied to system located on this segment. The access to the IAS is limited to the proxies that have been configured for the segment. In most firewall installations, the only permissible network applications are HTTP to port 80 and FTP. There are instances where other ports are allowed for HTTP and other things like telnet and secure shell. Since these systems cannot be used to attack USACE internal devices, a violation of security on them is not critical to overall USACE security. However, they need to be protected as if they could. In cases where access is required through applications like FTP and telnet, sites are encouraged, but not required to use secure forms of these protocols. There are limited cases where the IAS is allowed to make connections to production segments; however, in these cases, they are heavily restricted by port/machine to what they can connect to. This is most often typically of small holes used to query production databases. This is also used where systems on the IAS need to make requests of production systems to back up the IAS server.

- **CIAS (Controlled IAS/Network)** – These segments are similar to the IAS segments discussed above; however, unlike IAS, they can be allowed to initiate connections to the Internet, to other IAS segments and to other CIAS segments. These systems are not allowed to initiate connections to the productions segments. This type of segment is typically used to create small isolated “community of interest” networks within USACE. Examples may be a group of Water Control segments that can interface with each other within a particular region or water basin and also be configured so that these systems can go out to external networks to collect information.
- **Outbound production accesses to other USACE nets** – the site firewalls are configured to allow open inbound and outbound access to the destination addresses of other Corps internal systems. This currently creates an open trust between USACE production systems.
- **Outbound production access to external systems** – the site firewalls are configured to “proxy” all traffic that is destined to leave the USACE network. This creates isolation between production systems and external systems. With the proxies, there is a connection created between the production system and the site firewall and a separate connection between the site firewall, and the external system. This creates a high level of isolation between the systems. All traffic to external systems takes on the source IP address of the firewall not the address of the production system. This creates an additional layer of security by hiding

the internal infrastructure from the external system. In addition, the proxy creates an additional layer of inbound protection since it does not allow inbound connections to production systems unless this traffic is in response to a requested outbound session. The production network contains a majority of all USACE systems including Corps staff workstations, servers, e-mail systems, financial systems, internal Web servers, etc. Systems located on production networks are allowed to initiate connections out to other production networks, to the Internet and to other Corps Internet accessible systems. Inbound initiated access is allowed to production segments only from other production segments. This configuration prevents Internet-initiated access to production systems. In effect, this creates a USACE-wide network of all production systems that are allowed to talk to each other and to the outside world but cannot be accessed externally.

- **SMTP traffic to/from production** – Currently there are a large number of systems within each USACE site that send and receive SMTP based e-mail traffic and as such are open to attacks based on the e-mail protocols. The site firewalls are currently configured to allow SMTP traffic inbound and outbound to all production systems.
- **SMTP traffic to/from IAS** – In order to protect other SMTP systems within USACE, SMTP traffic from IAS systems is forced through the corporate e-mail servers.
- **DNS traffic to/from production** – Currently DNS traffic is allowed into and out of each Corps site through the site firewall. The current DNS configuration is such that while site servers are required to “forward-only” to specific gateway DNS servers, this configuration is not mandated through site firewall configurations and will not be until complete migration to the Army-protected DNS plan. In addition, internal USACE DNS servers are directly queried from external systems. This will also change after the migration to the Army DNS configuration.
- **DNS traffic to/from IAS** – To prevent DNS interactions between IAS systems, which are exposed to the Internet and the production DNS infrastructure, a separate “cache-only” DNS infrastructure exists at both processing centers. This DNS infrastructure is in place to allow servers that are on IAS segments to perform DNS lookups for internal and external addresses. The site firewalls are configured to allow IAS segments to pass only DNS traffic to/from these IAS DNS servers.
- **VPN** – In most cases, VPN connections are terminated at the VPN concentrators located at the processing centers. For this reason, there are no current filters in place for the processing of VPN protocols through site firewalls. There are, however, rules in the gateway firewalls to allow inbound VPN sessions to the corporate VPN concentrators.
- **Firewall holes** – In order to provide support to some Corps sites for their external customer, there are some selected firewall holes in the site firewalls that are created. These holes are the result of sites completing FAR, having these

requests reviewed by the CEEIS team for security issues and implementing the hole. Some holes are created with a flag to remove them after a select period of time. These holes are created in concert with corresponding holes that are created in the gateway firewall to create full end-to-end connectivity.

- **Remaining risks –**

- *SMTP* – The passing of SMTP openly through the site firewall poses a risk in that poorly protected or misconfigured SMTP servers could be compromised and used to launch an attack, either internal or external. With the current site firewall configuration, this attack could be launched from external or internal systems.
- *DNS* – There is a risk of attack or network mapping using the DNS protocol since the current site firewall rule set is very permissive for DNS to/from production segments.
- *Firewall holes* – The holes that are in the site firewalls at the request of internal customers pose a risk in that attacks could either be launched from the site or spoofed from the address of the hole.
- *Log files* – there is a significant amount of information contained on the log files created off each site firewalls. The current CEEIS staff reviews these logs for major events but now correlation or long-term event tracking is performed. In addition, due to the number of these devices there is a large amount of data that should be processed in order to adequately analyze security incidents.
- *Site-to-Site trust* – The current site firewall configurations are highly permissive as it relates to connectivity between one site's production network and another. This poses a risk to sites in that a system that is compromised at one site can be used to attack other USACE systems. In addition, this configuration also poses a risk in that internal attackers can attack other systems at other USACE sites.
- *CIAS attacks to Internet* – since some CIAS servers are allowed to initiate connection out to external networks, this poses a risk to these other networks. There are actions that USACE can take to protect these external networks from attack by USACE systems. However, much of the responsibility is in the hands of those who administer these remote systems and the level of trust that they give to systems external to their security boundaries.

- **Future actions –**

- *Log analysis database* - An activity that is currently unfunded related to the site firewalls is the creation of log servers located at each site that can gather firewall logs and ship them to central logging servers and databases. This information could then be processed with analysis software to perform correlation of the log files obtained off other devices.

- *Site-to-Site trust reduction* - The CEEIS team is currently analyzing site-to-site traffic requirements in order to develop a complete set of locked-down site-to-site trust rules in the firewalls. These configurations could be radically different from one site to another due to different levels of interoperation between Corps sites and could result in a significant security workload to initially implement and to manage.
- *SMTP* - The CEEIS office is developing configurations that would force all inbound and outbound SMTP e-mail through tightly managed servers located at the two centers. In addition, site firewalls would then be configured to block all inbound SMTP from external sources and allow SMTP from internal USACE systems to identified servers within the Site. These site firewall rules would strictly control the flow of SMTP traffic.
- *DNS* - Upon migration to the Army-protected DNS configuration, internal DNS servers will be required to forward all of their requests to two protected DNS servers located at the centers. The site firewall will be configured to only all DNS traffic between a few site DNS servers and the root servers located at the centers and other identified DNS servers within USACE All other DNS traffic would be denied. This will significantly reduce a site's exposure to DNS-based attacks and also prevent the enabling of "rogue" DNS servers at a site.
- *Firewall holes* - There is currently an intense effort by the CEEIS team to identify each site firewall hole and work with sites to convert this to VPN where possible. In cases where VPN cannot be used and as such the hole needs to remain, filters will be placed into the IDS system at the gateway and site to more closely watch traffic from the source and destination of the hole. This will allow us to detect attacks that may come through these holes.

R.6.4.4 Site routers –

Each Corps site has one or more CEEIS-managed routers. These routers are used to connect the site into the CEEIS infrastructure. These routers have small ACLs that provide a security function.

- **Antispoofing, inbound** – The ACLs on these routers inspect inbound packets to see if the source address is an address that actually belongs within that site. If this occurs, then either this packet is the result of spoofing or it is the result of misconfigurations at another site. In either case, these packets are discarded. Since all connectivity to a site must also pass through either the gateway firewalls (If the traffic is coming from outside USACE) or pass thru a site firewall (if the traffic is coming from another USACE site), the probability of matches on this filter is very low.
- **Antispoofing, outbound** – The ACLs on these routers also inspect outbound packets to see if the source address is not an address that belongs within that site. If this occurs, then either this packet is the result of spoofing from within the site or it is the result of misconfigurations at the site. In either case, these packets

are discarded. Since all connectivity to this router from the site is through the site firewall, the probability of matches on this filter is also very low.

- **Remaining risks –**

- *Log files* - there is a significant amount of information contained on the log files created off the gateway firewalls. The current CEEIS staff reviews these logs for major events but now correlation or long-term event tracking is performed.

- **Future actions –**

- *Log analysis database* - An activity that is currently unfunded related to the site routers is the creation of log servers located at each site that can gather site router logs and ship them to central logging servers and databases. This information could then be processed with analysis software to perform correlation of the log files obtained off other devices.

R.6.4.5 Intrusion Detection Infrastructure

CEEIS installs, configures and manages an IDS infrastructure that provides visibility across all of USACE. This includes probes at each Corps site, probes on special interest segments, gateway connections and backdoors.

- **IDS event monitoring –** Using the Real Secure Site Protector console system located at both processing centers, IDS events are centrally reported and analyzed both by the software in the console system and by CEEIS staff. Events are classified based on the level of severity and are reacted to based on knowledge of the USACE infrastructure. In some cases, the offending site is blocked; however, in most cases, CEEIS staff evaluates the attack and determines if it could have succeeded. In some cases, site contact is required to work with them if a server is suspected of being violated or being vulnerable. A separate document outlines the various incident-handling SOPs that are used to respond to events.
- **Remaining risks –**
 - *Log files* - As with other security devices there is a significant amount of information contained off the IDS probes. Much of this is stored in the site protector database; however, there is no ability to correlate this data with log files from other devices.
 - *In-dial* - Currently, connections that are made thru the site in-dial systems are not observed through the IDS infrastructure. If someone were to gain access through the site in-dial, they would be able to attack production systems at that site. If they attempted to attack outside that site, the IDS located at the site would detect this activity. If they were able to attack an internal site

production system and gain access, they could use this system to attack other systems.

- *Backdoors* - There are currently backdoors to other networks at some Corps sites. These backdoors are protected by the firewalls; however, there is no corporate visibility on this traffic in that there are no IDS sensors on these segments.

- **Future actions –**

- *Log analysis database* - If a log analysis database gets funded, the IDS log files would be fed into this database for correlation analysis.
- *In-dial* - CEEIS, in coordination with CECI-A is working with sites to migrate all in-dial connections so that they can be monitored by CEEIS IDS systems.
- *In-dial*- If funded, CEEIS will place IDS systems on backdoor connections.
- *Snort* - Due to the high cost of additional Real-Secure IDS licenses, CEEIS is evaluating the deployment of a Snort infrastructure to augment the IDS systems. This will allow additional monitoring at a lower cost.
- *Site Access* - CEEIS has found an effective and manageable way to provide IDS information to each site. This will be a future initiative.

R.6.4.6 DNS

The overall USACE DNS configuration is detailed in a separate document. This document outlines the USACE configuration as it relates to the Army-Protected DNS plan.

- **Remaining risks –**

- *Internal attack* - Once USACE has fully migrated to the Army-Protected DNS configuration and once all needed firewall blocks are in place, there is a very low risk of external DNS server attack for USACE. However, there is still a possibility that one DNS server at a site could attack another sites DNS using poisoned responses of some sort. Due to site firewall filters that are in place, there will be a very low risk of this happening.
- *Future actions* - Future actions are outlined in the more detailed USACE migration plan to Army-Protected DNS.

R.6.4.7 E-mail Anti-virus protections

The Corps has a centralized e-mail service as part of the CEEIS program. This staff manages e-mail at the corporate level and works with Corps sites on other e-mail issues. The CEEIS office provides some of the security protection for viruses and sites provide other protections.

- **Inbound e-mail to Exchange accounts** – Inbound e-mail destined to Exchange servers is routed through UNIX systems located at the two processing centers. This e-mail is scanned for viruses and quarantined as needed. The tool used to perform these scans is Antigen. The CEEIS e-mail team monitors outputs from this tool. This team also applies the updates to the signatures for Virus detection.
- **Site Exchange servers** – Each USACE site runs either Norton or MacAfee anti-virus protection on their Exchange servers to prevent workstation-to-workstation infection within their site and to prevent their site from sending viruses to other sites.
- **Site workstation** – Each USACE workstation is required to run updated anti-virus protection. This is the responsibility of each site.
- **Remaining risks** –
 - *Non-Exchange SMTP inbound* - There are currently ways for SMTP e-mail to be delivered into USACE without passing through the gateway e-mail servers at the processing centers. This is either by delivering e-mail to non-Exchange servers at USACE sites via MX records or delivering e-mail using A records to individual workstations. Virus-infected messages could still be delivered through this path and bypass the virus protections in place.
 - *Enterprise visibility* - Since Site Exchange servers and the workstations at sites are managed by each site independently, there is no corporate visibility of virus status. When an infection occurs, sites must be individually contacted to determine their status of cleanups.
- **Future actions** –
 - *SMTP analysis* - The CEEIS office has developed scripts to scan each USACE site to determine which devices are answering to the SMTP port. Once these are identified, we will work with each site to reduce the number of devices and then place firewall blocks for all SMTP traffic except that traffic to specific devices that have virus protection on them.
 - *SMTP lockdown* - An even more secure configuration would be to block all inbound/outbound SMTP traffic except that traffic to/from the processing center e-mail gateways. This block would take place at the gateway devices. In addition, similar blocks would be placed on site firewalls to further reduce the risk of virus infection through devices that do not have protection.

R.6.4.8 Client VPN

As discussed above, systems located outside the USACE network cannot initiate connections to production systems within USACE. In order to provide this capability to those that need it, an enterprise-level VPN configuration has been deployed.

R.6.4.9 Site to USACE VPNs

In addition to individual customers located outside of the USACE network, there are also small field sites that may want to connect to USACE via the Internet. In order to support this type of connection in a secure manner, USACE has also deployed an enterprisewide site-to-site VPN solution.

R.6.4.10 Non-E-mail Antivirus protections

In the future, this section will address anti-virus protections in place for non-e-mail related infections thru protocols like HTTP, HTTPS and FTP.

R.6.4.11 Vulnerability assessments

In order to better evaluate the security situation for USACE, there are a number of initiatives that relate to vulnerability assessments. These actions are taken either by the CEEIS office or by local offices to evaluate their internal security.

- **ISS Internet Scanner** – The CEEIS team has copies of the ISS scanner tool that can be used to assess vulnerabilities remotely. This tool is used on request from a site to evaluate IAS attached systems and used in response to observed IDS events.
- **STAT** – Each USACE District office has a licensed copy of the HARRIS Stat tool for use in performing internal vulnerability assessments and to check for IAVA compliance. In addition, the CEEIS team has copies to assess corporate level resources.
- **Open source** – The CEEIS team and sites use open source tools as appropriate in order to augment the capabilities of the tools described above.
- **Remaining risks** –
 - *Frequency of scans* - The CEEIS team attempts to perform scans on sites as needed; however, due to staffing levels, there is no program in place to perform periodic, scheduled full scans of sites.
 - *Scan analysis* - Running a scan is a simple task. Many times, companies offer to run a scan and sites end up with reams of printouts with little analysis. While the CEEIS team runs scans for sites and attempts are made to add value by analyzing the results and providing guidance to a site, the staffing levels are not such that more intense analysis can be performed.
 - *Admin access* - In order to perform enterprise-level vulnerability assessments, each site would need to create an admin account on systems that would be enabled only when the scan was to be run and disabled when the scan was completed. This is a possible future initiative.

R.6.4.12 E-mail

- **Inbound e-mail to Exchange accounts** – Inbound e-mail destined to Exchange servers is routed through UNIX systems located at the two processing centers.

These servers are closely watched and patched to ensure that e-mail vulnerabilities are closed. This configuration protects site Exchange servers in that they do not need to run the SMTP daemons and do not need to be exposed to the Internet.

- **Remaining risks –**

- *Non-Exchange SMTP inbound* - There are currently ways for SMTP e-mail to be delivered into USACE without passing through the gateway e-mail servers at the processing centers. This is either by delivering e-mail to non-Exchange servers at USACE sites via MX records or delivering e-mail using A records to individual workstations. These servers are still exposed to SMTP attacks and need to be patched to ensure that these vulnerabilities are closed.
- *Enterprise visibility* - Since Site Exchange servers and the workstations at sites are managed by each site independently, there is no corporate visibility of virus status. When an infection occurs, sites must be individually contacted to determine their status of cleanups.

- **Future actions –**

- *SMTP analysis* - The CEEIS office has developed scripts to scan each USACE site to determine which devices are answering to the SMTP port. Once these are identified we will work with each site to reduce the number of devices and then place firewall blocks in place for all SMTP traffic except that traffic to specific devices that have virus protection on them.
- *SMTP lockdown* - An even more secure configuration would be to block all inbound/outbound SMTP traffic except that traffic to/from the processing center e-mail gateways. This block would take place at the gateway devices. In addition, similar blocks would be placed on site firewalls to further reduce the risk of virus infection through devices that do not have protection.

R.6.4.13 Threat mitigation

In the following section, each of the above threats is analyzed and related to the deployed USACE security architecture.

- **Internal corporately managed systems used as platforms to attack –**

Corporately managed systems are placed behind multiple layers of firewalls with rules preventing access thru other than selected ports and protocols. In addition, access to these systems is restricted to USACE production systems. Traffic from these systems outside the Corps is configured to allow inbound traffic only if there are corresponding outbound requests for this information. The IDS sensors are also tuned to watch for any abnormal activity against or from these systems so that staff can react. In addition, the DoD IAVA process is used to ensure that patches are applied as needed. The corporately managed systems are managed by the CEEIS office with a process in place to track patches and perform vulnerability scans.

- **Internal noncorporately managed systems used as platforms to attack on USACE** - Attacks from an internal system can currently be launched to other Corps sites due to the site-to-site trust rules in place. These attacks, however would be detected at the site IDS that is monitored by the CEEIS office. As mentioned above, there are initiatives in place to begin to restrict site-to-site traffic. These systems are managed and patched by each Corps site using the IAVA process. In addition, sites have vulnerability assessment tools to perform scans to see if systems need patches. USACE has a live, Web-based tracking system that is used to assure that CERT notices and IAVA compliance notices are acknowledged and applied as necessary.
- **Internal systems used as platforms to attack on Internet** – Internal USACE production systems can gain access to non-USACE systems; however, in order to do this they must pass their traffic through proxies on the site’s firewall and also through port blocks on the gateway firewalls and routers. This reduces the ability of site production systems being used to attack non-USACE systems.
- **Defacement of sites** – The likelihood of site defacements is significantly reduced through the creation of IASs. This reduces the number of sites that are accessible from outside USACE and allows the firewalls and IDS systems to be tuned to watch for this type of activity.
- **Denial of Service**
 - **.mil address** – While currently this exposure cannot be eliminated, it is significantly reduced through the use of proxies and network address translation such that very few addresses are exposed to outside of USACE.
 - **External access** – The USACE security design, through the creation of IAS segments on the site firewalls, allows for external access to systems as appropriate yet at the same time prevents access to internal systems.
 - **De-centralized information collection** – The USACE security design, which allows local site publishing of information, allows for data to be collected on production segments and then streamed off to IAS servers.
 - **DNS** – Currently there are vulnerabilities in the USACE DNS infrastructure. Upon migration to the USACE version of the Army-protected DNS plan these will be eliminated. The site and gateway firewalls will have a role in creating this configuration.
 - **SMTP e-mail** – Currently there are vulnerabilities in the USACE SMTP infrastructure. The CEEIS team is evaluating current configurations and will propose a configuration where all traffic flows through secured gateways located at the centers. The site and gateway firewalls will have a role in enforcing this configuration.
 - **Virus attack downloaded Web content** – There are no enterprisewide initiatives to detect and eliminate malicious code that is delivered through a means other than SMTP. Protections here depend on site virus signatures being up to date and enforced.

- **Program (scumware) attack via Web** – There are no enterprisewide initiatives to detect and eliminate scumware. Protections here depend on site virus signatures being up to date and enforced.
- **Monitoring of unencrypted traffic from Internet to USACE** – The migration of most Internet to production access to VPNs rather than firewall holes significantly reduces the amount of unencrypted traffic that can be captured for USACE.
- **Mapping of the USACE infrastructure to gain information for an attack** – The deployment of the gateway router, gateway firewalls and site firewalls reduces the visibility of the USACE infrastructure. In addition, by hiding all production devices by using the IP address of the firewall, little information can be gained by scanning the Corps.
- **Attack via unknown connection** – For unknown physical backdoors, there are some actions that can be taken thru the use of IDS sensors to detect traffic; however, these backdoors could still be used to gain access to production systems and then these production systems could be used to then attack other internal USACE systems. This could be reduced thru the use of aggressive backdoor policy enforcement and frequent scans.
- **Attack via in-dial** – In-dial systems will migrate to their own segments so that IDS sensors can monitor their activity.
- **Foreign system attached to USACE local network** – Sites may need to enforce port security so that foreign systems cannot be physically connected to systems. In addition, IDS probes and strong anti-virus protections can reduce these risks.
- **Unsecured wireless access point** – USACE is developing an enterprise-wide wireless policy as an annex to this security plan.
- **Unknown attacks** – The CEEIS team and site IA staff will need to remain aware of new vulnerabilities as they are discovered and develop plans to reduce these risks.

R.6.4.14 Comparison to Army objective IA architecture

The above described configuration of gateway filtering routers, gateway stateful packet filter firewalls, site proxy firewalls and site filtering routers is identical in design to the Army's future security architecture plans. The Army plans outline the use of stateful packet filters at the entry points to the network. There are differences in the USACE architecture is managed at the enterprise level with MACOM-wide visibility and control.

R.6.4.15 Training

As part of the overall USACE security plan, an increased effort will be placed on the training and security certification of these staff members that are responsible for IDS and firewall management. This could include professional type certifications in the security and forensics field. In addition, effort will be placed on training site staff in security areas including mandatory Systems/Network administrator training by Army.

R.6.4.16 Review of basic tenets of USACE security architecture/design

The following outlines some basic rules in deploying security within USACE.

- **Gateways** – The gateways that provide for connections outside of the USACE/CEEIS network are managed at an enterprise level by CEEIS. These gateways have routers with Access control lists and a stateful packet filter (PIX).
- **Exiting the CEEIS ‘cloud’** – Every connection into the CEEIS cloud requires a firewall. When sites connect to the CEEIS frame network (MCI or Sprint), or when sites have dedicated connections to other Corps sites, an enterprise-managed firewall is required.
- **Circles around sites** – If you draw an imaginary circle around a site that is connected to the CEEIS infrastructure, the only thing that punctures this circle are CEEIS-managed connections and security stacks. If there are backdoors that puncture this circuit, they must be connected to the CEEIS firewall and treated with the same types of rules as all other non-USACE traffic. It is acceptable to make backdoor connections onto the IAS since these segments cannot initiate traffic out.
- **IDS deployments** – There must be CEEIS-managed intrusion detection probes on all site connections to CEEIS, all in-dial connections and all backdoor connections.
- **VPN** – The corporate VPN is the only inbound VPN solution that will be allowed into the USACE infrastructure.
- **Production segments** – Systems on the production segments cannot receive traffic initiated from outside USACE. There are some exceptions to this that are made using the FAR process; however, these are evaluated on a one-by-one basis for risk to USACE.
- **IAS segments** – Systems on IAS segments cannot initiate traffic out with the exception of selected holes for database queries, DNS and SMTP. Each of these requires individual analysis and site request and must be configured as tight as possible.
- **DNS** – Upon migrations to the Army-protected DNS plan, this section will be updated to reflect site requirements.
- **SMTP** – Upon migrations to the centralized SMTP gateways, this section will be updated to reflect site requirements.
- **Site-to-site trust** – Upon migrations to tighter firewall rules, access from site to site will be provided only for those systems and applications where the site can prove a business need for access. These rules must be coordinated with both the initiating site and the receiving site. This section will be updated to reflect these requirements.

Appendix S – Federal Enterprise Architecture (FEA) Background Information

S.1 FEA Reference Models



To facilitate efforts to transform the Federal Government to one that is citizen-centered, results-oriented, and market-based, the Office of Management and Budget (OMB) is developing the Federal Enterprise Architecture (FEA), a business-based framework for Government-wide improvement.

The FEA is being constructed through a collection of interrelated "reference models" (Figure S.1) designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal agencies.

FEDERAL REFERENCE MODELS

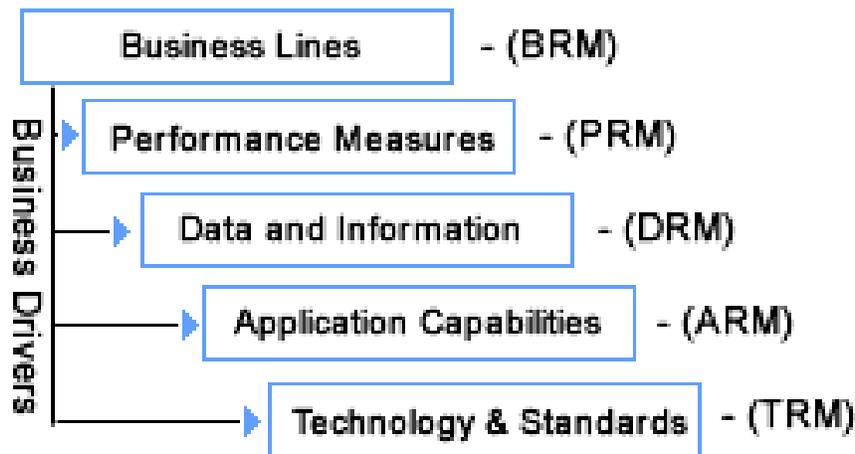


Figure S.1. Federal reference models

The Performance Reference Model (PRM) is a framework for performance measurement that provides common outcome and output measures throughout the Federal Government.

The Business Reference Model (BRM) is a framework for describing the business of the Federal Government independent of the agencies that perform it, and serves as the foundation for the FEA. The model describes the Federal Government's Lines of Business, including its internal operations and its services for the citizen, independent of the agencies, bureaus and offices that perform them.

The Service Component Reference Model (SRM) is a business-driven, functional framework that classifies Service Components with respect to how they support business and/or performance objectives. The SRM is structured across horizontal service areas that, independent of the business functions, can provide a leverageable foundation for reuse of applications, application capabilities, components, and business services.

The Data and Information Reference Model (DRM), still being developed, will describe, at an aggregate level, the data and information that support program and business line operations. The model will aid in describing the types of interactions and information exchanges that occur between the Federal Government and its various customers, constituencies, and business partners. It will categorize the Government's information along general content areas specific to BRM subfunctions and decompose those content areas into greater levels of detail, ultimately to data components that are common to many business processes or activities. The DRM will establish a commonly understood classification for Federal data and lead to the identification of duplicative data resources as well as enable information sharing between agencies.

The Technical Reference Model (TRM) is a hierarchical foundation used to describe how technology is supporting the delivery of Service Components and capabilities. The TRM will outline the technology elements that collectively support the adoption and implementation of component-based architectures, as well as the identification of proven products and toolsets that are embraced by Government-wide initiatives such as FirstGov.Gov, Pay.Gov, and the 24 Presidential Priority E-Government Initiatives.

S.2 What Is an Enterprise Architecture?

An Enterprise Architecture (EA) is the blueprint that is developed, implemented, maintained, and used to explain and guide how an organization's Information Technology (IT) and information management elements will work together to efficiently and effectively support the organization's business processes so it can accomplish its missions. It is essential to realize that information is a key part of architecture – standards for hardware and software alone do not compose a complete and effective EA. Likewise, having an EA with specific technology and information management goals does not mean that an organization must immediately change over all of its systems. An important part of an EA is a plan addressing how the organization will migrate information to new technology targets over time.

S.3 Why Is Enterprise Architecture Important?

USACE, responding to the dictates of good management as well as legislative requirements, now requires the development and implementation of an enterprise IT architecture. A staff or business owner may have a single architecture that covers all of its offices and business processes, or a number of architectures based on distinct and specific business processes within itself. The best reason for having an EA is the benefits it brings to the organization. Benefits have included the improved ability to

share and efficiently process information, the ability to respond faster to changes in technology and business needs, an increased ability to meet customer information needs efficiently, and reduced operational costs because of economies of scale and resource sharing.

S.4 What Are the Benefits of EA?

An EA offers tangible benefits to the enterprise and those responsible for evolving the enterprise. The EA can:

- Capture facts about the mission, functions, and business foundation in an understandable manner to promote better planning and decision making.
- Improve communication among the business organizations and IT organizations within the enterprise through a standardized vocabulary.
- Provide architectural views that help communicate the complexity of large systems and facilitate management of extensive, complex environments.
- Focus on the strategic use of emerging technologies to better manage the enterprise's information and consistently insert those technologies into the enterprise.
- Improve consistency, accuracy, timeliness, integrity, quality, availability, access and sharing of IT-managed information across the enterprise.
- Support the Capital Planning and Investment Control (CPIC) processes by providing a tool for assessment of benefits, impacts, and capital investment measurements and supporting analyses of alternatives, risks, and tradeoffs.
- Highlight opportunities for building greater quality and flexibility into applications without increasing cost.
- Achieve economies of scale by providing mechanisms for sharing services across the enterprise.
- Expedite integration of legacy, migration, and new systems.
- Ensure legal and regulatory compliance.

Therefore, the primary purpose of an EA is to inform, guide, and constrain the decisions for the enterprise, especially those related to IT investments. The true challenge of enterprise engineering is to maintain the architecture as a primary authoritative resource for enterprise IT planning. This goal is not met via enforced policy, but by the value and utility of the information provided by the EA.

S.5 EA Methodology

Enterprise architects and engineers have historically used models as their primary descriptive method. John Zachman and Steven Spewak are two of many recognized leaders in architecture conceptualization and enterprise architecture planning. This body

of work is key at level IV in that it presents transitions from the general to a more specific set of methods and approaches.

S.6 Zachman Framework

John Zachman is the author of the *Framework for Information Systems Architecture*, which is referred to as the Zachman Framework (Figure S.2). It has received worldwide acceptance as an integrated framework for managing change in enterprises and the systems that support them. As it applies to enterprises, the Zachman Framework is a logical structure for classifying and organizing the descriptive representations (i.e., models) of an enterprise that are significant to its management and the development of its systems. The rows of the Zachman Framework represent different perspectives, which may be used to view a business (i.e., Planner, Owner, Designer, Builder, and Subcontractor views). The columns represent the product abstractions or the focus (i.e., Entities = *what*, Activities = *how*, Locations = *where*, People = *who*, Time = *when*, and Motivation = *why*). The Zachman Framework is a comprehensive, logical structure for descriptive representations (i.e., models) of any complex objects. It is neutral with regard to specific processes or tools used for producing the descriptions. The Framework, as applied to enterprises, is helpful for sorting out complicated technology and methodology choices and issues that are significant to general and technology management and identifying the kinds of models for a given project.

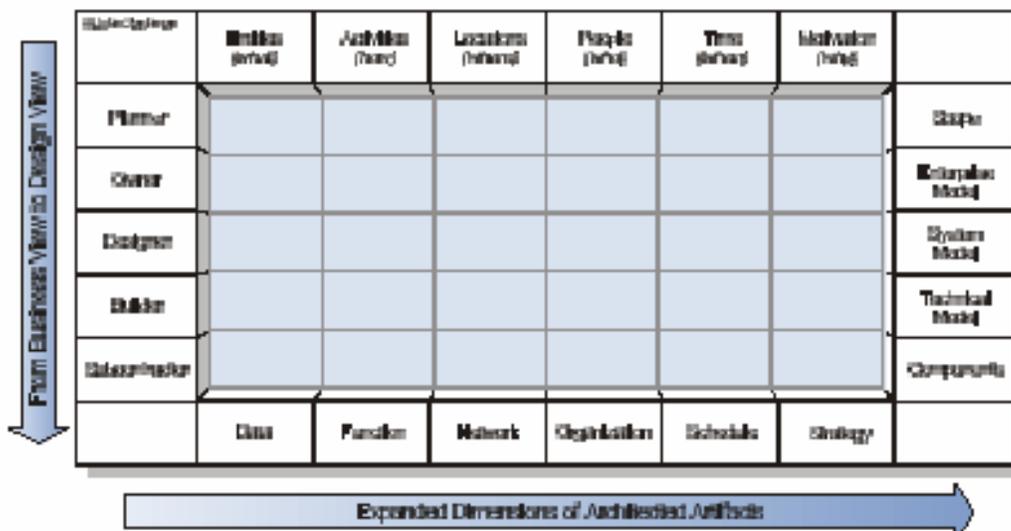


Figure S.2. The Zachman Framework

S.7 Enterprise Architecture Planning

Dr. Steven Spewak is the author of *Enterprise Architecture Planning: Developing a Blueprint for Data, Applications, and Technology*. His approach to FEA has helped organizations with modeling, business strategy planning, process improvement, data

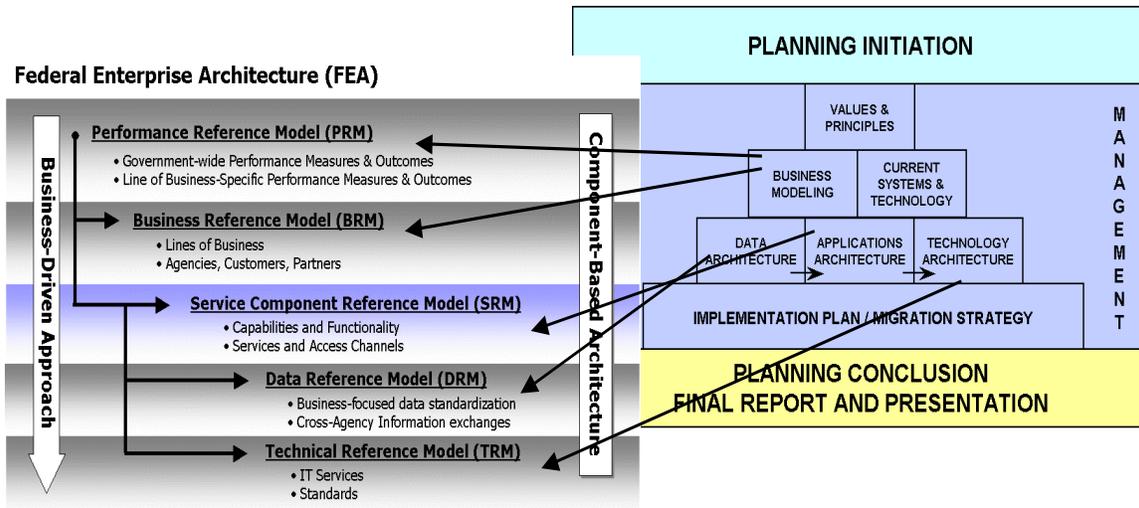


Figure S.4. Mapping EAP methods to FEA

The FEA is based upon Levels 1 and 2 of the Zachman Framework. Using the recommended steps outlined in Dr. Spewak's book, the PDT identified the USACE main business functions. Each function was validated against existing documentation. In turn, the USACE primary business function was described using IDEF0 (Integrated Definition) process for identifying the Inputs, Constraints, Outputs and Mechanisms (ICOM) down to the second layer of the organization. Then, these functions were mapped to the FEA BRM descriptors to ensure that USACE business functions met the OMB guidance.

While OMB has not released its guidance pertinent to the DRM, the PDT decided to develop a DRM so as to determine the relationship of its data to the business functions. The PDT commenced its initial DRM by identifying USACE's high-level data classes. The PDT identified 64 data classes and validated these against existing documentation. In turn, these data classes were elevated into 13 enterprise level data classes. Both an Entity-Relationship diagram and Create Read Update Delete (CRUD) Matrix were developed to depict the USACE data support to the Corps.

Appendix T – CeA As-Is and To-Be Architecture Framework

T.1 USACE Future Environment



The Corps Enterprise Architecture (**CeA**) assists the U.S. Army Corps of Engineers (USACE) by improving the way USACE defines, budgets, deploys, and maintains information technology (IT). Specifically, IT-related projects need to be approved and managed based on USACE business requirements and have accountable sponsorship. In order to effectively accomplish this, USACE needs to have a clear picture of its current business enterprise, a plan for its strategic direction, and the tools to manage the transition from its current state to its future state(s). The following questions are currently being addressed by USACE:

- How do the different entities that compose USACE enterprise relate and interact with one another?
- What is the future state(s) of USACE and what IT will need to be in place to support it?
- What business tools does Customs need to have in place to define, budget, deploy, and maintain IT projects effectively as it transitions to its future state(s)?

This appendix is one of many **CeA** products. Its purpose is to describe the state of practice in FY03 and outline an overall target framework (i.e., To-Be Architecture) that improves the ability of USACE to meet its future business strategy. The **CeA** framework provides a structure for organizing resources and for defining and managing enterprise architecture (EA) activities. The development and maintenance of an architecture is a continuing process of evaluating current conditions and seeking target solutions. Typical architecture segments captured in the framework include data, applications, technical, and security. The key linkages established within the framework incorporated in the five **CeA** models.

T.2 CeA across the Federal Government

Executive Order 13011, Federal Information Technology, established the Federal Chief Information Officers (CIO) Council as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal information resources. The Clinger-Cohen Act of 1996 assigned the CIOs the responsibility to develop information technology architectures (ITAs). The Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, November 28, 2000, requires agencies to ensure consistency with Federal,

agency, and bureau Enterprise Architectures (EAs) and to demonstrate consistency through compliance with agency business requirements and standards.

In support of these mandates, the Federal CIO Council developed and published the Federal Enterprise Architecture Framework (FEAF) in September 1999 to promote shared development for common Federal processes, interoperability, and sharing of information among the agencies of the Federal Government and other Governmental entities. In serving the strategic needs and direction of the Federal Government, the Federal CIO Council seeks to develop, maintain, and facilitate the implementation of the top-level EA for the Federal Enterprise. The Framework consists of various approaches, models, and definitions for communicating the overall organization and relationships of architecture components required for developing and maintaining a Federal Enterprise Architecture (FEA).

In response to the Clinger-Cohen Act of 1996 and the FEAF, most Federal agencies have initiated efforts to create EA awareness or to build an EA management foundation. The scope of these EA projects has ranged from functional area or subagency architectures (Zachman verticals) to agencywide definitions (Zachman horizontals) that extensively leverage process and technology commonality within an agency.

In 2001, The President's E-Government Taskforce identified 24 Presidential Priority E-Gov initiatives that are potentially transformational in nature and offer the opportunity to simplify, unify, and consolidate processes used by the Federal Government. These Initiatives will enable the Federal Government to better serve the public, promote interactions across governmental organizations, and perform business activities while continuously improving internal efficiency and effectiveness. The OMB's Federal Enterprise Architecture Program Management Office (FEAPMO) has continuing stewardship responsibilities for these E-Gov Initiatives, as they become the first real instantiation of the FEA. Whereas the Federal CIO Council defined a *framework* for the FEA in 1999, the FEAPMO, with the support of the Federal CIO Council, is now in the process of developing an FEA.

FEAPMO is developing five reference models: performance, data, services components, technical, and business. Working jointly, these models will drive standardization and cross-agency collaboration opportunities. They will also provide a structured approach to analyze overlapping functions, identify similarities across agencies, and provide a means by which agencies can leverage best practices from each other—promoting reuse in the Government.

The FEA is intended to provide a consistent, industry-aligned approach for defining and communicating the components needed to cost and plan E-Gov programs—both the 24 Presidential Priority E-Gov Initiatives and other IT initiatives across the Federal Government. It is based on the business requirements derived from the priority initiatives as well as system engineering design best practices. Such an approach is essential if the Federal Government is to 1) leverage information technology investments and avoid unnecessary duplication of infrastructure and major components, 2) link business processes through shared, yet sufficiently protected information

systems, and 3) leverage disparate business processes, services, and activities that are located outside agency boundaries.

T.3 Path to Automation

Starting in the late 1960s and continuing through the early 1990s the trend was to automate specific business areas. Over this 30-year period USACE automated a significant portion of its business. Today USACE employs 57 major systems and has an additional 50+ systems that have been developed for specific needs across USACE. A survey conducted by the science and engineering (S&E) community (represented by the Science and Engineering Technology (SET) Initiative) identified well over 500 different types of S&E applications throughout USACE. These 500 applications include the USACE products plus various commercial off-the-shelf (COTS) products such as Matlab, TableCurve, etc. The wake of automation resulted in a considerable sustainment cost for USACE. A common rule of thumb is that sustainment cost covers about 70 percent of the total cost of a system.

Of the 57 major systems most of them are centrally hosted by Corps of Engineers Enterprise Infrastructure Services (CEEIS). Keeping these systems operating 24/7/365 presents CEEIS with a significant challenge. Some systems have managed to keep abreast of new technology from, for example, Oracle (databases) and Sun and Microsoft (operating systems) while others have remained unchanged for years. Consequently USACE is required to sustain many combinations of hardware/operating systems as well as the underlying COTS products used by these systems.

In the late 1990s IT switched its focus from automation to interoperability. Interoperability is the method that allows systems and products to interchange information. An example would be information stored in Microsoft Excel that is freely exchanged with Microsoft Word. Over the past 10 years the IT industry has spent billions of R&D dollars to improve interoperability in their products. Interoperability will play a key role in the next generation of products used across USACE. However, true interoperability requires planning. Very few systems within USACE share information. However, there is a significant interest among the Automated Information System (AIS) developers and COTS vendors to develop systems that share information. Developing and sustaining such interfaces are not cheap. USACE needs to adopt a common approach and then apply it consistently across all systems.

The initial step in the architecture process is to define current state of practice in IT and its interface with the business components of USACE. An analysis took place in FY03 to better understand the USACE As-Is architecture. The finding illustrated in Figure T.1 indicates that common infrastructure and security models were established while the remaining sections of the architecture were subdivided along the business and S&E lines. Development of the As-Is architecture required analyses of the work the agency performs, the information the agency uses and the technology the agency implements to support the mission, vision, and goals of the organization. It included capturing the current business processes to determine the information needed and handled by the

agency and to identify additional opportunities for IT to support the mission of the agency. A thorough understanding of the current state of the agency, its business processes, and their relation to the agency missions is essential to enable the agency to develop and apply the **CeA** effectively. The subsequent sections summarize the results of the findings.

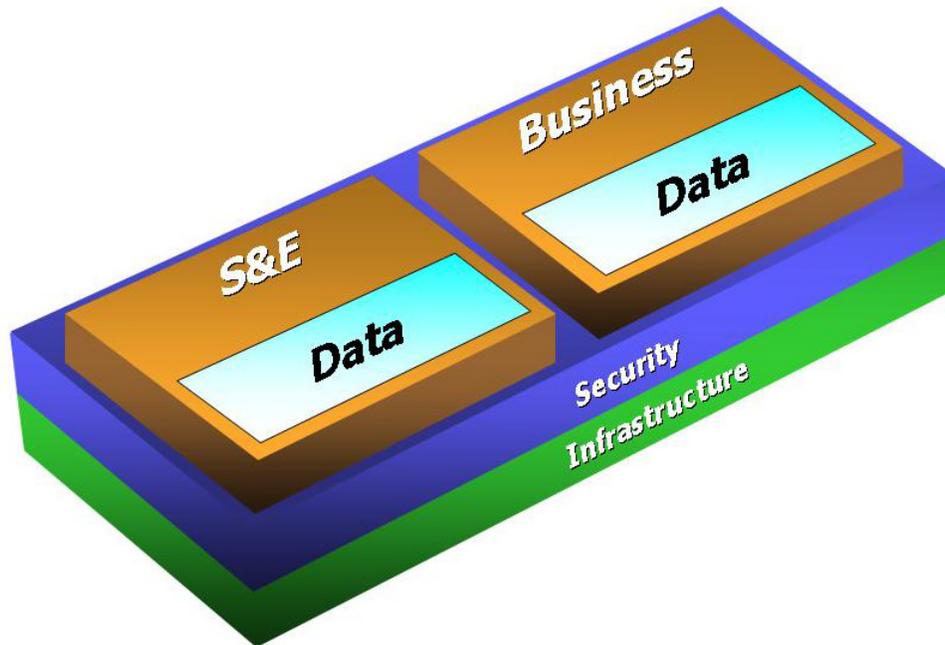


Figure T.1. USACE As-Is Model

T.3.1 Enterprise Business Data

Over the past two decades USACE has focused on automating specific business functions with limited consideration given to the interdependencies among their processes. Consequently, applications have had the tendency to lock data into their specific databases without any consideration given to the enterprise worthiness of their data. Recently, USACE has worked on consolidating most of its business data into an enterprise model managed by one of the two business processing centers.

Characteristics of the USACE business data are as follows:

- Most enterprise data are stored in Oracle
- Use of Oracle database drivers is inconsistent across business databases
- Enterprise data are centralized at one of the two USACE process centers (Western Processing Center (WPC) and Central Processing Center (CPC))

- WPC and CPC perform backups on data
- Enterprise license agreement with Oracle is required
- Some non-Oracle applications exist

Efforts to define the enterprise data model are the focus of the **CeA** Data and Information Reference Model. However, low-level details that describe the underlying technical aspects of data and information are covered in Chapters 4 and 6 of this document.

T.3.2 Applications and Tools

The information in this section is based on a combination of data provided by the USACE SET initiative and AIS information managed by the Directorate of Corporate Information (CECI). Note that some subjectivity was necessary to classify the information. A total of 593 software entities (applications, tools, models, AISs) commonly used within USACE were identified. The results of the investigation are as follows:

- 25 percent of the entries are classified as stand-alone numerical models
- 8 percent of the entries are hosted by the enterprise servers (i.e., CEEIS)
- 12 percent are Government off-the-shelf (GOTS)-based stand-alone tools developed and managed by the Computer-Aided Structural Engineering Research Program
- 30 percent of the entries are classified as COTS

T.3.3 Local Database

The majority of USACE data are collected and managed at the District level. Typically, the format and structure of the data as well as the technology used to house the data are project driven. Consequently, the ability to share and reuse data is minimized. This lack of interaction can be attributed to the following:

- Tendency of local data to be more S&E related.
- Based on a mixture of databases (Oracle, MS Access, MySQL, SQLServer).
- Limited linkages between locally stored data and enterprise data.
- Data not cataloged/referenced to data dictionary.
- Limited sharing of data among USACE offices.
- Inconsistent use of data standards.

T.3.4 Geographic Information Systems (GIS)/Computer-Aided Design and Drafting (CADD)

The following data are based on input from the DoD CADD/GIS Technology Center for Facilities, Infrastructure, and Environment and information collected by the USACE Geospatial program:

- Typically CADD and GIS data are managed at the individual project or application level.
- There is limited interoperability between CADD and GIS tools, but recent vendor products demonstrate a move toward interoperability.
- Microstation is the pseudo-corporate CADD Tool (>90 percent of Corps' CADD users).
- ESRI Arc products are the pseudo-corporate GIS Tool (>90 percent of Corps' GIS users)
- Several USACE projects are transitioning to Arc Version 8+. This requires a reworking of the data and tools.
- There is no enterprise GIS solution within the Corps, but several Divisions are actively planning and/or implementing regional GIS solutions.
- Most GIS activities are project-centric, which limits the reusability of the information.
- Arc tools lack interoperability with Microstation tools.
- 60 percent of the sites do not use GIS technology.
- 7 percent of GIS products used within USACE are a combination of MapInfo, Microstation, and Geomedia.
- There are 400+ ESRI product licenses with USACE.

T.3.5 Office Data

Office data are typified as information created, manipulated, and stored based on the common suite of office tools. Characteristics of office data and their usage are as follows:

- Data are managed locally.
- Little or no automated document management capability is utilized.
- There is no document management standard.
- Lack of corporate metadata repository complicates collaboration and locating documents.
- Microsoft Office is the standard tool for office data management.

T.3.6 Enterprise Wide Area Network (WAN)

CEEIS is responsible for the management of the Enterprise wide-area network (WAN), which consists of networking capabilities to the District, Division, and Headquarters. Note that it does not address how the individual sites manage their internal networks.

- Some systems at centers (CPC and WPC) connect at Gigabit, others at 100 megabit (Mbps)
- Center systems are migrating to Gigabit connection
- Centers connect to frame at 90 Mbps
- Existing network backup/failover capability
- Host
 - Internet (dual vendors with load balancing implemented)
 - SIPRnet (Secret Internet Protocol Router Network)
 - E-mail
 - DNS (Domain Name Service)
 - Network/information assurance (IA) skill sets at both centers
 - OCONUS (Outside the Continental United States) sites connected at 1.5 Mbps

T.3.7 Local Area Network (LAN)/Site WAN

The management of local area network (LAN) and site WANS occurs at the individual Districts or Divisions. In this document, site WAN is the network that connects Districts to their individual field sites. Characteristics of the LANs and site WANs are as follows:

- Sites manage own infrastructure
 - Network
 - IA
 - E-mail
 - DNS
- Wide variation in network/IA/e-mail/DNS skills
- Wide variation in internal site connectivity
- Connectivity to project offices often low speed
- Approximately 80 percent of traffic is from center to site
 - Internet, e-mail, enterprise applications
 - Some sites are running AIS and Web applications that tax their bandwidth

T.3.8 Science and Engineering (S&E)

USACE is the world's premiere public engineering organization. This is based on the ability to apply leading-edge science and engineering technologies to civil and environmental problems facing our military and nation. Traditionally, S&E-related activities leverage the latest technologies to solve complex engineering problems. As a

result, the technical landscape is consistently changing. Such dynamics in the application of technology have resulted in technical inconsistencies that reduce our ability to address many of the future problems facing USACE. Characteristics of the USACE S&E activities are as follows:

- Customer problems requiring coupled technology approaches
- System and basin-scale management involving coupled physics, models, tools, databases
- Limited computing power necessary to execute large regional problems
- Limited expertise in regional modeling
- Historically, studies and supporting technologies designed to address local (small-scale) problems
- Inability to effectively sustain S&E models/tools
- No standards for scientific data
- Scientific data collected, managed, and stored from a project-centric perspective
- Inconsistencies in how S&E data are stored and accessed limiting ability to address regional problems

T.3.9 Common Delivery Framework (CDF) Program

The Common Delivery Framework (CDF) program is an ongoing Civil Works R&D initiative begun in FY02 that focuses on identifying standards and technical approaches in support of the following objectives:

- Improve the ability for systems and data to interoperate
- Establish a corporate approach focused on reuse of software components and data

Additional information is available on the CDF Web site (<https://cdf.usace.army.mil>).

T.3.10 Collaboration

Historically, personnel needed to execute a project typically reside within the District to which the project is assigned. This simplified communications among the team members. However, in the future many of the project memberships may span several Districts and even Divisions. Furthermore, other Government and State agencies will team up with USACE on these efforts. Therefore, the technical aspects behind collaboration are critical in the support of Project Management Business Process (PMBP). Collaborative efforts are limited by the following:

- Network connectivity restrictions that limit the ability to interoperate with Federal and State agencies and private firms that operate outside the DoD network environment.

- No corporate solution that supports teaming of geographically dispersed USACE Project Delivery Teams (PDTs).

T.4 Evolving to the Future

One thing that is a given is that IT will change. Today's market is so competitive that if any company does not aggressively pursue the next-generation product, they could easily lose ground to their competition. So how can USACE as a whole adopt products and technology that will generate business value? Moving in a common direction requires planning and planning requires communication. The methodology that supports such planning and communicating within USACE is the **CeA**.

The **CeA** is organized around basic building blocks, referred to as the **CeA** framework, that describe the target baseline to support future enterprise business applications and data. Note that the framework is designed and structured around supporting the TWEs presentation in the BRM. Furthermore, it provides designers, developers, and users a common understanding of the technical components and standards affecting interoperability, portability, and scalability.

The framework is a hierarchical structure used to organize the **CeA** content in terms of a high-level (logical structure) view and a supporting low-level view described in the various **CeA** models. The high-level view, termed the **CeA** Framework, focuses on the structuring and organizational aspects of technology while a secondary view, the **CeA** models, outlines low-level technical categories and their supporting definitions, standards, and product standards. Figure T.2 illustrates the relationship between the framework and the other models.

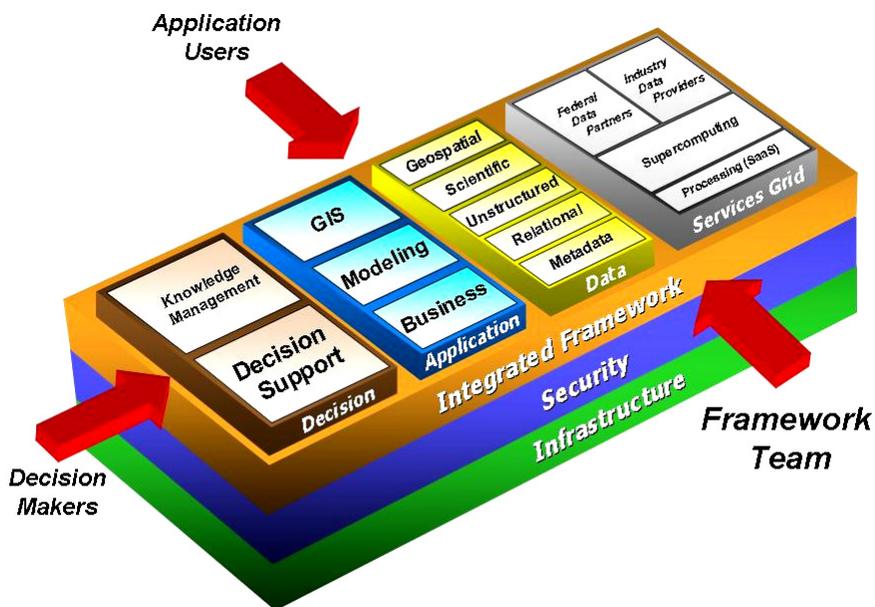


Figure T.2. **CeA** To-Be Framework

It is important to emphasize that the framework describes higher level organizational principles in the model, while the models describe the lower level technical pieces that enable the framework. Compliance is based on how an application fits into the framework as well as its compliance with the **CeA** models.

T.4.1 Background

This section introduces an enterprise computing framework that will assist in meeting the TWEs presentation in BRM. Additionally, this framework is supported by the guidelines and standards documented in the Technical Reference Model (TRM). As a result, the **CeA** framework is a high-level organizing structure that describes the logical topology of data, code, computers, and networks. More specifically, this section focuses on the organizational aspects while the **CeA** models are more standards focused. Furthermore, it is not the intention that the framework be created all at one time. Some parts of this section are in the early stages of building. Testing and evaluation efforts ongoing within USACE will assist in prototyping and testing candidate solutions. The objective is that components of the framework be developed, implemented, and refined over time.

T.4.2 Drivers

Inconsistencies in how USACE designs, purchases, and fields systems severely limit its ability to address many of the TWEs. Today most of the structuring of technology is performed at the project level or by the contractor. Over time, new technology solutions are stacked on or integrated with older solutions. This results in a patchwork of applications and data that work independently as opposed to an integrated environment.

In order to meet current and future business challenges, USACE must approach technology from an enterprise perspective. The purpose of the To-Be model is to define a common framework of how technology is organized. It is important to understand that the To-Be model is an evolving enterprise computing model. The To-Be model provides technical direction for software and hardware components that require interfacing at the USACE enterprise level.

T.4.3 To-Be Characteristics

The characteristics of the To-Be model are as follows:

- **Net-Centric.** Computer networks provide an infrastructure to move today's platform-centric applications to tomorrow's net-centric environment. By increasing richness and reach simultaneously, net-centricity allows USACE to connect its applications and data, thereby providing an information-rich environment.
- **Enterprise System.** The Common Computing Environment (CCE) is an enterprise model that guides how USACE develops and/or purchases technology. The enterprise includes regional business centers (RBCs), and their

supporting Districts, Centers, Laboratories, Government and industry partners, academia, and USACE customers.

- **Enterprise Agility.** The true benefit of the CCE is to enable the quick response to USACE customers and stakeholders. Members of the USACE PDTs operate as virtual teams composed of multidisciplinary experts that form the knowledge-base necessary to solve a problem. The enterprise focus of the CCE will minimize the impact of including PDT members that are geographically dispersed.
- **Regional Management of IT Assets.** Local Area Networks, helpdesk, acquisitions, and IT management will be provided at a regional level to gain efficiencies and increased compatibilities, through compliance with CCE guidelines across the enterprise.
- **Information Accessibility.** The CCE simplifies the access to enterprise information. Engineers have access to up-to-date S&E information, project/program managers have access to the schedule and business information, our partners have standard approaches to sharing information, and our customers are kept informed of our progress.
- **Tool Interfaces.** Both engineering capabilities such as AISs, tools, and models and our business AISs must work collectively in solving problems. The goal is to integrate our best capabilities and practices into CCE over time. The CCE with the associated Technical Reference Guides (TRGs) provide the guidelines for information exchange among disparate capabilities.
- **Systematic Reuse.** The CCE is intended to facilitate the systematic reuse, exploitation, and leveraging of enterprise resources across USACE.
- **Technical Consistency.** The CCE facilitates a common technical baseline across USACE. Such consistency supports the reuse of solutions and expertise across the organization.
- **Knowledge Multiplication.** The CCE treats information and its delivery as a central and important theme to its success. The knowledge-centric focus initiates the capturing and exploitation of knowledge whereby knowledge is reused throughout the organization.
- **Access Controls and Security.** The transformation into a net-centric environment improves the sharing and reuse of information; however, it does introduce challenges associated with securing the information. Authentication, authorization, and encryption are critical capabilities that protect the CCE.

T.4.4 Overview of CeA Framework

The **CeA** Framework is a four-tier (see Figure T.2) network-centric framework, built on open standards and designed for scalability, reliability, and modularity. Tiers include a Decision tier, an Application tier, a Data tier, and a Services Grid tier. Tiers are stacked on three cross-cutting layers that support integration, security, and the technical foundation for the entire framework.

- Decision Tier: provides a common set of components that deliver information/knowledge and serve as gateways to computational and data resources.
- Application Tier: consists of a collection of software components such as AISs, numerical models, S&E tools, GIS, code libraries, etc.
- Data Tier: provides an enterprise repository for storing and retrieving geospatial, CADD, scientific, and multimedia (i.e., unstructured) data.
- Services Grid Tier: Provides a set of corporately shared computational and data resources used to solve problems that exceed desktop capabilities.
- Integration Layer: provides a common set of standards and method that support integration and interoperability.
- Security Layer: outlines various security models and technologies that support the entire framework.
- Technical Layer: consists of the underlying technical aspects of the framework that address communications, computers, and software standards and guidance.

T.5 Summary

The To-Be framework is evolving through the coordination of developments occurring in the field offices, R&D activities, and advances in technology outside USACE. The intent is to continue adding details to the **CeA** framework and the underlying **CeA** reference models. For more information on the **CeA** please contact Mr. Tony Brunner, Robert.A.Brunner@hq02.usace.army.mil.

Appendix U – Glossary

U.1 CeA Glossary, Last Update 1 December 2004

POC is Tony Brunner, CECI-S

Information Source and Definition Validation: Terms and definitions used were derived from Public Laws, Federal, DoD, DA and USACE published regulations.

Note: An abbreviated Corps of Engineers Enterprise Infrastructure Services technical glossary follows this **CeA** glossary to explain technical acronyms and definitions related to the wide area network and infrastructure.

Acceptable Quality Level (AQL): The maximum percent defective, the maximum number of defects per hundred units, or the number of defects in the lot that can be considered satisfactory on the average, or the degree of deviation from perfect performance for a specific contract requirement before the Government will consider the contract performance unacceptable. As long as the defective performance does not exceed the AQL, the Government will not reject the services. However, performance at an AQL does not imply that the Service Provider may knowingly perform in an unsatisfactory manner.

Access (Information System): Ability and means to communicate with (i.e., input to or receive output from) or otherwise make use of any information, resource, or component in an Information System.

Access Control Mechanism: This permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform.

Accession: The transfer of the legal and physical custody of permanent records from an agency to the National Archives and Records Administration.

Accident: An unintentional or unexpected event or series of events resulting in an individual's occupational illness, injury, or death; damage to or loss of equipment or property; and/or damage to the environment.

Accountable Officer: An individual required to maintain accounting records for property or funds, whether public or in some degree thereof. The accountable officer may or may not have physical possession of the property or funds.

Accountable Personal Property: All nonexpendable personal property with a life expectancy of more than one year and an acquisition cost of \$5,000 or more; it includes all Sensitive Property.

Accounting: The act of receiving, controlling, validating, recording, classifying, and summarizing transactions in terms of money, analyzing and interpreting those transactions, and reporting the operating results and related resource management information to higher headquarters.

Accreditation: A formal declaration by a designated approving authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards.

ACERT (Army Computer Emergency Response Team): Army's top-level security team. All other subordinate Computer Emergency Response Teams (RCERT, FCERT, etc.) report to them. Located at Fort Belvoir.

Access Control List (ACL): Used in various CEEIS routers to filter traffic in/out.

Acquisition: The acquiring by contract with appropriated funds of supplies or services (including construction) by and for the use of the Federal government through purchase or lease, whether the supplies or services are already in existence or must be created, developed, demonstrated, and evaluated. Acquisition begins at the point when agency needs are established and includes the description of requirements to satisfy agency needs, solicitation and selection of sources, award of contracts, contract financing, contract performance, contract administration, and those technical and management functions directly related to the process of fulfilling agency needs by contract.

Action Copy: The copy of a document sent to the agency, office, or individual responsible for taking action.

Action Plan: A plan derived from recommendations that identifies the specific actions that will be taken to improve a process or a project and outlines a schedule for implementing those actions.

Active Directory: A directory service from Microsoft that is a part of Windows 2000, XP, and 2003. It stores information about objects on a network and makes this information available to users and network administrators. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive hierarchical view of the network and a single point of administration for all network objects.

Activities: An Information Technology Investment Management (ITIM) core element that describes the procedures necessary to implement a critical process. An activity occurs over time and has recognizable results. This core element typically involves establishing plans and procedures, performing the work, tracking it, and taking corrective actions as necessary.

Activity: An Army/USACE organization. Within the context of the Army Enterprise Architecture, it is 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.

Actual Cost Method: Billing method whereby actual costs are used as the billing basis in lieu of fixed prices/rates. The actual cost method is used for nongovernmental agencies; private parties, foreign military sales, and all other entities excluded from the rate stabilization provisions.

Active Directory Schema Configuration Control Board (AD-SCCB): It is used to control enterprise level active directory configurations and reports to the CEEIS CCB. Sam Bradley, CEEIS Configuration Program Manager, chairs this board.

Adjustment Factor: Amount that is deducted from the observed defect when random sampling with extrapolated deductions or random sampling without extrapolated deductions is used to calculate the defect rate for the entire population. This factor is determined from standard tables.

Administrative Approval: An approval officer's signature on a payment voucher to indicate that the voucher is correct. Or a statement by an approval officer that indicates that the proposed payment is approved. The approval officer must sign and date the statement.

Administrative Control: Any procedure that significantly limits exposure by control or manipulation of the work schedule or manner in which work is performed.

Administrative Limitation: Limitation in the funding regulation to control the obligation or expenditure of funds. Offices or agencies establishing other limitations on obligations and expenditures will monitor and enforce them, but not under the anti-deficiency statutes.

Administrative Offset: Withholding of money payable by the U.S. Government to satisfy a debt owed the U.S. Government. Administrative offset may include offset from salary when a specific statute so authorizes.

Administrative Subdivision of Funds: Any subdivision of an appropriation that makes funds available in a specified amount for incurring obligations or that can be further subdivided to make funds available in specified amounts for incurring obligations.

Army Enterprise Infostructure – Transport Reengineering Working Group (AEI-TRWG): Army initiative to create integrated Army network. CEEIS staff participates in this design effort.

After Action Review (AAR): A review that provides immediate feedback about a mission or task designed to improve individual and collective task performance.

Agency: A U.S. Government entity defined by 5 U.S.C. 551(1). It includes exchanges, commissaries, and any other organization that is operated exclusively as an instrument of an agency to administer one or more agency programs, or that is identified for this purpose by the head of the agency.

Automated Information Systems (AIS): Used to refer to any application that is used. Typically used to refer to larger applications like CEFMS, P2 etc.

Army Knowledge Management (AKM): Name used to describe multiple goals within Army to streamline Information Technology and provide information to all Army staff easily.

Army Knowledge Online (AKO): Refers to the Web site/portal www.us.army.mil.

Alias: Also known as redirecting. The practice of using a fictitious address for your outgoing and incoming e-mail.

Alignment: The degree of relational agreement, conformance, and consistency between organization's mission, vision, values and goals with its policies, guidance, structures, processes and systems, competencies, and individual behaviors.

Allocation: An authorization by the Department of the Army making funds available in prescribed amounts to an operating agency for suballocation or allotment.

ALPHA: A RISC microprocessor designed by Digital Equipment Corporation.

Alternate Standard: A standard developed in place of an existing regulatory standard. An alternate standard must provide equal or greater protection to exposed personnel than the prescribed standard and can be approved only by the agency that promulgated the standard.

American National Standards Institute (ANSI): A U.S. standards organization composed of representatives from industry, technical societies, consumer organizations, and government agencies.

Army Network Operation Security Center (ANOSC): Army's top-level center that monitors Army-wide network and security infrastructure. Located at Fort Belvoir.

Applicable Interest Rate: The interest rate that the Secretary of the U.S. Treasury announces semi-annually under Section 12 of the Contract Disputes Act of 1978 (41 U.S.C. 611). This interest rate is used to calculate the amount of interest to pay a vendor on a late payment. It is published in the Federal Register when Defense Finance and Accounting Service announces the amount by a message to all Finance and Accounting Offices/Defense Accounting Offices.

Application Software: Software that performs a specific task or function, such as word-processing, creation of spreadsheets, generation of graphics, or facilitating e-mail. An application should be considered a system for the purpose of reporting to the Army

Information Technology Registry unless it is part of a larger system already being reported.

Apportionment: A determination by the Office of Management and Budget specifying the amount of obligations allowed during a given period under an appropriation, contract authorization, other statutory authorization, or a combination of these per 31 U.S.C. 1512.

Appropriation: An authorization by an Act of the U.S. Congress to incur obligations for specified purposes and to make disbursements for them from the U.S. Treasury. This includes authorizations to create obligations in advance of appropriations or other fund authority.

Appropriation-Multi-Year: An appropriation that is available for incurring obligations for a definite period in excess of one fiscal year.

Appropriation Warrant: An official U.S. Treasury document that provides the dollar amounts established in the general and detailed appropriation accounts of the U.S. Treasury pursuant to Appropriation Acts authorized by law. It serves as a convenient source document for entries into accounts that establish the amount of money authorized to be withdrawn from the U.S. Treasury.

Approved Operating Budget: The approved financial funding level for a major activity director or activity, normally on an annual basis.

Architecture: The structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time.

Architecture Alignment & Assessment: The determination made about an Information Technology (IT) investment's alignment with the Corps Enterprise Architecture (**CeA**). Using criterion to evaluate whether or not, and to what degree, there is conformance determines the IT investment alignment. IT investment alignment is evaluated against each of the **CeA** architectural models – Business, Information, Solutions, Performance, and Technical.

Archives: The noncurrent records of an organization preserved because of their continuing or enduring value. An archive is also referred to as the organization or agency responsible for appraising, accessioning, preserving, and making available permanent records.

Archiving: In electronic records, the process of creating a backup copy of computer files, especially for long-term storage.

Archivist of the United States: The head of the National Archives and Records Administration.

Armed Forces: The Army, Navy, Air Force, Marine Corps, and Coast Guard.

Army Knowledge Management: The Army-wide effort to transform the Army and USACE into a net-centric self-learning organization that will improve operational and mission performance.

Army Management Structure: A structure established by regulation to provide a single, uniform classification of the nontactical (peacetime) activities of the U.S. Army for use in programming, budgeting, accounting, and reporting of cost, performance, and manpower data.

Army Occupational Safety and Health Program (ARMOSH): A program that addresses the overall maintenance of safe and healthy conditions in the workplace or the occupational environment. This includes OSHA compliance, industrial and production operations, and Research, Development, Test, and Evaluation activities. It is applicable to all Army civilian and military personnel and operations.

Army Records Information Management System (ARIMS): Cost-effective organization of Army files and records contained in any media so that records are readily retrievable. It 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.

Army Web Risk Assessment Cell: A team of information assurance personnel that conduct ongoing operational security and threat assessments of Army publicly accessible Web sites to ensure compliance with DoD and Army policy and best practices.

Artifact: See Work Product.

Army Security Router (ASR): Army managed devices that connect to NIPRNET circuits.

Assessment: An appraisal by a trained team of professionals to determine the state of an organization's current processes and to determine the high-priority process-related issues facing an organization. An assessment may also result in organizational support for process improvement.

Asset: Property, funding, technical knowledge, or other valuable items owned by the organization. Investments typically create assets.

Asset Management: The life cycle management of assets, encompassing not only the inventory of existing equipment, but also the acquisition, maintenance, and disposal of assets.

Asset Use Charge: A charge for the use of DoD assets (facilities and/or equipment) to recoup depreciation and interest on investment.

Assets: An item of economic value owned by a Federal agency. The item may be physical in nature (tangible) or a right to ownership (intangible) that is expressed in terms of cost or some other value.

Attribute: A property or characteristic of one or more entities. Also, a property inherent in an entity or associated with that entity for database purposes.

Audit Trail: Audit trail capabilities allow for readily tracing all transactions, including those that are computer-generated and computer-processed transactions, from initiation (individual source documents) to accounting reports and vice versa. For example, tracing a general ledger account and amount from a trial balance to the original transaction. Audit trails also provide for the detection and tracing of rejected or suspended transactions to ultimate correction.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Automatic Data Processing Manager: Organization responsible for the actual design and development of computer programs implementing the functional design.

Automation: Conversion of a procedure, process, or equipment to automatic operation. When allied to telecommunications facilities, automation may include the conversion to automatic operation of the message processing at an exchange or remote terminal.

Autoresponders: Also known as mailbots. Automated programs that return a canned message upon receipt of e-mail.

Bandwidth: The maximum rate at which an amount of data can be sent through a given transmission channel.

Bar Code: A series of rectangular marks and spaces in a planned manner.

Base Case System: A system that has been fielded and certified through the intra-Army interoperability process.

Base Operations Support (BASOPS): Support services and functions performed by the facility for the benefit of others. BASOPS includes real property maintenance, minor construction, environmental compliance, installation supply and maintenance services, transportation, and other installation common support services. Common-service support functions listed in DFAS-IN 37-1, Finance and Accounting Policy Implementation, regardless of the appropriation or fund account from which they are financed.

Basic Ordering Agreement (BOA): A written instrument of understanding negotiated between a contracting activity and a contractor. A BOA contains terms that apply to future orders, a description of services to be provided, and a method for pricing future

orders under this agreement. Service orders under a BOA are placed by an Ordering Officer.

Business Contingency Planning (BCP): Planning associated with continuing business process in the event of catastrophic failures.

Benchmarking: A structured approach for identifying the best practices from industry and Government and comparing and adapting them to the organization's operations. Such an approach is aimed at identifying more efficient and effective processes for achieving intended results based on outstanding practices of other organizations.

Benefit: A term used to indicate an advantage, profit, or gain attained by an individual or organization. Tangible benefits include benefits that can be explicitly quantified. Such benefits may include reducing costs, increasing productivity, decreasing cycle time, or improving service quality. Intangible benefits include benefits that may be easy to identify but that can be difficult to quantify. These benefits may include more efficient decision-making, greater data accuracy, improved data security, reduced customer burden, or increased organizational knowledge.

Border Gateway Protocol (BGP): Routing protocol used for external connections.

Bi-Annual: Occurs every 2 years. (It does not mean twice a year.)

Bi-Monthly: Occurs every 2 months. (It does not mean twice a month.)

Bi-Weekly: Occurs every 2 weeks. (It does not mean twice a week.)

Bill Balancing: The process of verifying that Summary Billing Record and related Detail Billing Record values are in agreement.

Billing: The process of sending an invoice listing amounts owed.

Billing Errors: Improper charges or credits resulting from billing office error.

Bit: The small unit of information (usually either 0 and 1) recognizable by a computer.

Blanket Purchase Agreement (BPA): A simplified method of filling anticipated repetitive needs for supplies or services by establishing "charge accounts" with qualified sources of supply. The BPA reduces the need for individual purchase documents.

Boot P: An arrangement allowing a computer on a network to act as an address server, automatically giving IP addresses on request.

Bounced Message: One that is returned to the sender because it is undeliverable.

Broadcast: The transmission of radio, television, and data signals through the air waves or fiber optic cable.

Budget: A planned program for a fiscal period in terms of (1) estimated costs, obligations, and expenditures; (2) source of funds for financing, including reimbursements anticipated, and other resources to be applied; (3) explanatory and workload data on the projected programs and activities.

Budget Year: That fiscal year arrived at by adding one fiscal year to the current fiscal year. During fiscal year 2004, the budget year would be fiscal year 2005.

Business Case: A structured method for organizing and presenting a business improvement proposal. A document, generally having a structured format, which articulates an initiative, action or change requiring the allocation of resource and a management decision. A business case typically includes a statement about why the initiative, action or change is required; assumptions, constraints, and risks; economic analysis on alternatives; return-on-investment (benefits and costs); and a recommendation. Organizational decision makers typically compare business cases when deciding to expend resources.

Business Concern: Any individual or organization engaged in a profession, trade, or business. It includes not-for-profit entities operating as contractors. This includes State and local governments but not Federal Government organizations. The term contractor, vendor, and firm are synonymous with business concern.

Business Function: A business action for which a person or thing is particularly fitted or employed. An assigned duty or activity related to another thing and dependent on it for its existence, value, or significance. Example: Environment impact assessments are a function of Environmental Monitoring.

Business Process: A systematic, disciplined and consistent means by which people perform work to produce products or achieve results/outcomes, or deliver services. Business processes usually have policy and guidance associated with them and, characteristically, have subprocesses, procedures, activities, events, and tasks. Business processes have inputs, controls, outputs, and mechanisms to ensure efficiency, effectiveness, quality, and customer satisfaction. Time-to-Delivery is generally used to measure business process performance.

Business Process Improvement: A systematic disciplined approach that critically examines, rethinks, and redesigns mission-delivery processes and subprocesses within a process management approach.

Business Reference Model (BRM) as Prescribed by OMB: The BRM describes the Federal Government's Lines of Business and its services to the citizen – independent of the agencies, bureaus, and offices that perform these business operations and provide these services. Developed with significant input from civilian Cabinet and other Federal agencies (work is currently underway to validate those areas of the model relevant to the DoD), the BRM identifies three Business Areas that provide a high-level view of the operations the Federal Government performs. The three Business Areas Prescribed by OMB comprise a total of 35 external and internal Lines of Business – the services and

products the Federal Government provides to its citizens – and 137 Subfunctions – the lower level activities that Federal agencies perform.

The **Services for Citizens** Business Area includes the delivery of citizen-focused, public, and collective goods and/or benefits as a service and/or obligation of the Federal Government to the benefit and protection of the Nation’s general population. This Business Area includes 22 Lines of Business and 82 Subfunctions.

The **Mode of Delivery** Business Area describes the mechanisms the Government uses to achieve the purpose of government, or its services for citizens. It includes financial vehicles, direct Government delivery, and indirect Government delivery.

The **Support Delivery of Services** Business Area provides the critical policy, programmatic and managerial underpinnings that facilitate the Federal Government’s delivery of services to citizens and other Federal, State and local agencies. This Business Area includes 9 Lines of Business and 32 Subfunctions.

The **Management of Government Resources** Business Area refers to the “back office” support activities that must be performed for the Federal Government to operate effectively. This Business Area includes 4 Lines of Business and 23 Subfunctions.

Byte: The number of bits representing a character to a computer, normally 8 bits.

DoD Common Access Card (CAC): This is the card that will replace all DoD ID cards.

Calendar Day: The 24-hour period of time beginning at 12:00 A.M. (Midnight).

Calendar Days: Consecutive days without regard to weekends or holidays.

Calendar Year: The 12-month period of time from January 1 to December 31.

Capitalization: The monetary value of inventories (materiel, supplies, and equipment) including undelivered orders due in undercapitalized contracts; also, allocations of cash less liabilities and equity, reservations. In those instances of transfer of logistic responsibility or materiel, the value will be at the current Army standard prices.

Capability Maturity Model: A descriptive model of the stages through which organizations progress as they define, implement, evolve, and improve their organizational processes. This model serves as a guide for selecting process improvement strategies by facilitating the determination of the current process capabilities and the identification of issues most critical to quality and process improvement.

Capital Planning and Investment Control (CPIC): The same as capital programming and is a decision-making process for ensuring that information technology (IT)

investments integrate strategic planning, budgeting, procurement, and the management of IT in support of agency missions and business needs. The term comes from the Clinger-Cohen Act of 1996 and generally is used in relationship to IT management issues.

Cartographic Records: Graphic representations drawn to scale of selected features of the earth's surface and atmosphere and of other planets and planetary satellites. Includes maps, charts, photomaps, orthophotomaps, atlases, cartograms, globes, relief models, and related records, such as field survey notes, map history files, etc.

CeA Chief Architect. Responsible for the definition and target planning of an Agency's Enterprise Architecture.

Corps of Engineers Enterprise Infrastructure Services (CEEIS): Name of entity that operates USACE infrastructure to FOA level including processing center, e-mail, network and security.

Central Files: Files accumulated by several offices or organizational units and maintained and supervised in one location.

Certification: Comprehensive evaluation of the technical and nontechnical security features of an Information System and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Certification Agent: Individual responsible for making a technical judgment of the system's compliance with stated requirements, identifying and assessing the risks associated with operating the system, coordinating the certification activities, and consolidating the final certification and accreditation packages.

Certificate of Conformance: A contractor's statement that the delivery conforms to contract specifications.

Certifying Officer: An individual authorized to certify the availability of funds on any documents or vouchers submitted for payment and/or indicate that payment is proper. The Certifying Officer is responsible for the correctness of the facts and computations and the legality of payment.

Change Management: Those activities involved in (1) defining and instilling new values, attitudes, norms, and behaviors within an organization that support new ways of doing work and overcome resistance to change; (2) building consensus among customers and stakeholders on specific changes designed to better meet their needs; and (3) planning, testing, and implementing all aspects of the transition from one organizational structure or business process to another.

Charge Out: The act and result of recording the removal and loan of a document or a file to indicate its location.

Civil Agencies: All agencies in the Federal Government other than DoD installations and activities, e.g., General Services Administration.

Classified Defense Information: Official information regarding the national security that has been designated top secret, secret, or confidential in accordance with Executive Order 12356.

Classified Material/Matter: Official information or matter, in any form or of any nature, that requires protection in the interest of national security. Material is classified CONFIDENTIAL, SECRET, or TOP SECRET or above under DoD 5200.1-R.

Commercial Item: The term commercial item has the meaning given that term in section 4(12) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(12)).

Commercial Voucher: A properly prepared public voucher that a vendor submits for goods or nonpersonal services. It must be supported by a contract, purchase or delivery order, receiving and acceptance report or performance certificate, and a vendor's invoice.

Communication 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.

Communication Security (COMSEC): Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security.

Communication Systems: A set of assets (transmission media, switching nodes, interfaces, and control devices) that establishes linkage between users and devices.

Community of Practice (COP): A community of practice 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. COP structures range from informal to formal. Also may be referred to as structured professional forums, knowledge networks, or collaborative environment.

Comparability: Relates to the similarity and consistency of information produced by an entity from period to period and by others operating in similar circumstances. The value and usefulness of information depends greatly on the degree to which it is comparable to information from prior periods and to similar information reported by others.

Compliance: A system that meets or is implementing an approved plan to meet all applicable Technical Architecture mandates.

Component: A self-contained business process or service with predetermined functionality that may be exposed through a business or technology interface.

Component Based Architecture (CBA): A technology architecture comprised of run-time services and control structures together with an application infrastructure. The CBA consists of the component model and the architecture services that are built around the model. Solutions based on a CBA are more dynamic, flexible, and maintainable than traditional monolithic solutions.

Computer: A machine capable of accepting data, performing calculations on or otherwise manipulating that data, storing it, and producing new data.

Computer Facility: Physical resources that include structures or parts of structures that support or house computer resources; the physical area where the equipment is located.

Computer Security: Measures and controls that ensure confidentiality, integrity, and availability of information processed and stored by a computer.

Computer-Aided Design and Drafting (CADD): An Automated Information System used by engineers and architects in the production of technical construction, mechanical, and electrical drawings. Often includes automated production of a bill of materials.

Condition: The status of personnel and equipment (readiness) as they interact with the operational environment during mission planning, preparation, and execution; a situation or circumstance.

Configuration: An expression in functional terms (that is, expected performance) and in physical terms (that is appearance and composition).

Configuration Management: The management of security features and assurances through control of changes made to hardware, software, firmware, documentation, tests, test fixtures, and test documentation of an Information System throughout the development and operational life of the system.

Consolidated Logistics Systems (CLS): A Government-furnished system that provides inventory management and other supply and tracking functions accomplished within USACE. CLS has been programmed using programming languages including, but not limited to, DCL, DEC C, FORTRAN, and Oracle 7 SQL Forms, SQL, PL/SQL, ProC and ProFortran. CLS Web site uses HTML, PERL Oracle Procedures, and Barcode Mill.

Constant Dollars: A term used when prices do not contain inflationary changes that have occurred and/or are forecasted to occur. Constant dollars are always identified with a specific time period, which is called a base year. Constant prices represent the total cost of an item or service if that item was purchased in the base year and the bill was completely paid in that year.

Consumable Supplies: An element of cost consisting of an expendable and those non-expendables that having a standard unit price of less than \$250 or that lose their identity on issue.

Continental United States (CONUS): The 48 contiguous states and the District of Columbia.

Continuing Resolution Authority: An interim appropriation until permanent appropriations are enacted. Authorizes continuation of normal operations at a rate not to exceed the latest congressional action or the previous year's rate and no new starts or expansions to a program.

Continuity of Operations Plan (COOP) and/or Contingency Plan: A plan maintained for emergency response, backup operations, and post-disaster recovery for an Information System, as a part of its security program, that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation, also known as a contingency plan.

Contract: Any enforceable agreement or order to buy supplies or services. The term is expanded in this document to include Letter of Obligation.

Contract Administration Office: The activity responsible for administering the contract.

Contract Authority: Statutory authority that permits obligations to be incurred in advance of appropriations or in anticipation of receipt to be credited to a revolving fund or other account. (By definition, contract authority is unfunded and must subsequently be funded by an appropriation to liquidate obligations incurred under the contract authority or by the collection and use of receipts.)

Contract Discrepancy Report: A report transmitted to the contractor by the Contracting Officer, initiated by the Contracting Officer's Technical Representative.

Contract Financing Payment: U.S. Government disbursement of monies to a contractor under a contract clause or other authorization before physical delivery and the acceptance of supplies or services by the U.S. Government.

Contract Liquidating Authority: An appropriation, or re-appropriation, enacted to pay the obligations incurred under the contract authority.

Contract Modification: Any written change in the terms of a contract. Only contracting officers acting within the scope of their authority are empowered to execute.

Contracting Officer (KO): A Department of the Army civilian employee or military officer who has a valid appointment as a contracting officer under the provisions of the Federal Acquisition Regulations. An appointed contracting officer has authority to enter into and administer contracts and make determinations and findings to such contracts. The term includes an authorized contracting officer's representative acting within the

limits of his or her authority. The term also includes purchasing and contracting officers and ordering officers.

Contracting Officer's Technical Representative (COR and/or COTR): An individual designated in writing by the Contracting Officer to act as an authorized representative of the Contracting Officer to perform specific contract administrative activities within the scope and limitations as defined by the Contracting Officer.

Contractor Acquired Property: Property procured or otherwise provided by a contractor for the performance of a contract. It does not include Government-furnished materiel or equipment.

Contractor Records: Data produced and/or maintained by a contractor for a Federal agency and required to provide adequate and proper documentation of that agency's programs and to manage them effectively.

Contractor Safety: Has the oversight of the safety and occupational health aspects of contract activities.

Contractor's Representative: An individual assigned by the Contractor who shall have full authority to act for the Contractor on all contract matters that relate to the daily operations of the contract. The contract representative shall be a single point of contact for all functional, technical, and contract-related services.

Core Element: The five standard parts common to each critical process that provide for its successful implementation. The five core elements are purpose, prerequisites, activities, organizational commitment, and evidence of performance.

Corps Enterprise Architecture (CeA): See Enterprise Architecture.

Correspondence: Letters, post cards, memoranda, notes, telecommunications, and any other form of addressed written communication that are sent and received.

Cost: A term used to indicate the obligation and expenditure of funds or as a means to express the aggregation of difference types of costs over time. It is not unusual for "cost" to be preceded or followed by a noun, adverb, or adjective to clarify or emphasis its meaning, such as "overhead cost" or "recurring cost."

Cost/Benefit Analysis: A technique used to compare the various costs associated with an investment with the benefits that it proposes to return. Both tangible and intangible factors should be addressed and accounted for in the analysis.

Cost Analysis: The systematic examination of the cost of interrelated activities and equipment to determine the relative costs of alternative courses of action.

Cost Benefits: A measure of the expense of obtaining certain information compared with the benefits to be derived by having the information. Information should not be

provided if the costs of providing it exceed the benefits to be derived, unless it is required to meet legal or other specified purposes.

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.

Critical Process: A structured set of key practices that, when performed collectively, contributes to the attainment of a maturity stage. Each critical process is structured using the five core elements.

Cross-functional Assessment Team (CFAT): This is a management team, with field representation, whose primary function is to assess the business value and risk of USACE-wide Information Technology investments, the costs associated with the operations and maintenance incurred by commands for command-wide, standard information systems, prioritize (rank) IT investments, and make recommendations to the Program Budget Advisory Councils on funding (fully, partially, or not at all). The Cross-Functional Assessment Team representatives are appointed by HQUSACE staff principles and Major Subordinate Command commanders and is chaired by the HQUSACE Chief of Staff. Team member representation is a combination of lines-of-business program managers and senior executives.

Current Year: The fiscal year in progress

Customer: Individual(s) or organizational entity for whom the product or service is rendered. The customer may also be the end user.

Customer Complaints: Complaints made by customers that, if validated, may be used by the Government for the purpose of assessing the contractor's quality assurance or for taking deductions to the contract price.

Data: The representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means.

Data Administration: The comprehensive management of an organization's data, such as by ensuring consistent definitions of data elements and coordinating the development of data dictionaries.

Data Attributes: Attributes are data objects that define or denote characteristics of a unique entity.

Data Base: In electronic records, a set of data, consisting of at least one file or of a group of integrated files, usually stored in one location and made available to several users at the same time for various applications.

Data Calls: A call for data from an individual or several groups used to compile information for specific purposes within the organization.

Data Class: Parent data object composed of lower level or primitive entities that have a common purpose and data function. Data Classes are composed of lower level entities, which are data objects that represent things of importance to the enterprise.

Data Column: A data column (e.g., field) is a piece of information that is characteristic of a table.

Data Element: A basic information unit template built on standard semantics and structures that in turn governs the distinct values of one or more columns of data within a row of data within a database table or field within a file.

Data Management: The process of creating a basis for posting, sorting, identifying, and organizing the 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 (DPP): An organized and structured approach to the specification and collection of enterprise artifacts in support of community of interest (COI) objectives that 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 Performance Plan System (DPPS): A centralized repository for enterprisewide storing, viewing, and reusing architectures, data models, business rules, and other artifacts associated with functional Army systems.

Data Synchronization: Policies and procedures that govern the consistency, accuracy, reliability, and timeliness of data used and generated by the Army. It addresses data planning, storage, scheduling, maintenance, and exchange among authorized users.

Data Table: A table is a physical data object within a database used for business processing. Physical tables can be produced from the logical representation of an Entity Relationship Diagram. Conversely, a physical table can be reverse engineered into an Erwin data model.

Database: A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications.

Database Management Systems: The program or programs that control a database so that the information it contains can be stored, retrieved, updated, and sorted.

Declassification: The process or result of determining that information no longer requires classification for national security reasons.

DEC Server 700: A Digital Equipment Corporation (DEC) product that supports the local or remote connection of PCs, video terminals, serial printers, modems, and data switches.

DECnet: A proprietary network protocol designed by Digital Equipment Corporation.

Decrement: A listing prepared to facilitate funding reductions that are received after approval of the initial operating program. Items that are already included within the funded operating program are listed in inverse (opposite order) priority, that is, lesser priority first. The decrement list reflects the order of those funded requirements that would be deleted first if funds were withdrawn.

Defect: Any failure of a unit of product or service to conform with specified requirements.

Defect Rate: The ratio, expressed as a percentage, of the number of defects to the total number of occurrences in the population. Alternatively, the defect rate may be expressed as a whole number representing the number of defects over a specified period of time. When planned sampling is used, the defect rate is calculated by dividing the total of all defects by the total population.

Deferrals: Executive action or inaction that withholds, delays, or precludes the obligation or expenditure of available budget authority that the installation could otherwise effectively and legally use. Deferrals may be initiated by the Office of Management and Budget or the agency involved; generally the budget authority deferred is intended for use at a later time.

Delegation of Authority: The transfer of authority for certification of funds availability from major activity directors to others. This delegation must be in writing.

Delivery Order: A document issued by the contracting officer under a basic agreement or indefinite quantity-type contract (open-end or call-type contracts).

Designated Billing Office: The office or individual named in a procurement document who is first to receive invoices or bills from vendors. This is usually the Finance and Accounting Office, but contracting officers can name other individuals or offices. The date bills or invoices reach the designated billing office is used to determine the correct payment due date under the Prompt Payment Act.

Designated Payment Office: The office named in the contract that will pay the vendor. If the contract requires invoice approval before it is sent to the payment office, vendors

must send the invoice to the address stated in the contract (the designated billing office).

Differential Global Positioning System (DGPS): A Global Positioning System (GPS) with an additional correction (differential) signal added. This correction signal improves the accuracy of the GPS and can be broadcast over any authorized communication channel.

Digital Signature: The product of an asymmetric cryptographic system that is created when the owner of the private signing key uses that key to create a unique mark (the signature) on an electronic document or file. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he/she claims to be.

Direct Costs: Cost (labor, material, contracts, travel, and transportation) that can be identified directly with a final cost objective (i.e., customer order or work authorization).

Directive: A written instruction communicating policy and/or procedures in the form of orders, regulations, bulletins, circulars, handbooks, manuals, notices, numbered memorandums and similar issuances.

Directory Services: A network service that identifies all resources on a network and makes them accessible to users and applications. Resources include e-mail addresses, computers, and peripheral devices such as printers. An active directory would be an example of a Directory Service.

Disbursement: The payment of a legal liability of the U.S. Government that decreases the accountability of the finance and accounting office making the disbursement. Disbursements are made to transfer funds, advance funds, or liquidate valid obligations of the U.S. Government.

Disbursing Officer: An individual who is held accountable for disbursing monies only on the basis of vouchers certified by an authorized certifying office.

Discount: A vendor's offer to accept a reduced payment in exchange for receiving an earlier payment. Discount offers can be in the contract, offered only on the vendor's invoice, or both. Discounts are usually stated in percentages, such as 2%/10 days. In this example, the vendor will accept a 2% payment reduction in exchange for a check dated 10 days after the date on the invoice. Commercial accounts payable personnel can accept discounts from Financial Management offers only if they are advantageous to the U.S. Government. The Office of the Assistant Secretary of the Army sends an annual message to all finance offices giving the current value of funds to the Treasury and examples of cost-effective discounts. Discount information is reported on the Prompt Payment Act report. Cost-effective discounts that cannot be taken because supporting documents allowing payment do not reach the commercial accounts payable office 4 days or more before the discount payment date are not reported as offered or

lost. Although every effort should be taken to accept cost-effective discounts, a discount of \$10 or more that cannot be taken is not reported on the Prompt Payment Act report.

Discount Trade: A reduction in price, usually varying in percentage with volume of transactions, made by vendors to those engaged in certain businesses and allowable irrespective of the time when the account is paid.

Disk: Flat, circular information system media used to record, store, manipulate, and retrieve data and information. As applied to information management, “disc” and “disk” are synonymous. Examples of disks are phonograph records, videodisks, computer disks, floppy disks, optical disks, and compact disks.

Disposition: The actions taken regarding records no longer needed for current Government business. These actions include transfer to agency storage facilities or Federal Record Centers, transfer from one Federal agency to another, transfer of permanent records to the National Archives and Records Administration, and disposal of temporary records.

Document: Recorded information regardless of physical form or characteristics. Often used interchangeably with “record.”

Documentation: The act or process of substantiating by recording actions and/or decisions.

DoD Information Technology Security Certification and Accreditation Process (DITSCAP): The standard DoD management process for identifying information security requirements, providing security solutions, and managing information system security activities.

Domain: An area of common operational and functional requirements. Currently, there are four domains: command, control, communications, and intelligence.

Duplicate Emergency Files: The essential files, directives, instructions, programs plans, standing operating procedures, operation and maintenance manuals, and other documents (including microfilm and computer software) that are required to perform essential functions. The emergency files are maintained at the Emergency Relocation Site.

Earned Reimbursement: The amount recognized when a performing organization renders actual or constructive performance on a reimbursable order.

Earned Value Management (EVM): A project management tool that effectively integrates the project scope of work with schedule and cost elements for optimum project planning and control. The qualities and operating characteristics of earned value management systems are described in American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard –748–1998, Earned Value Management Systems, approved May 19, 1998. A copy of Standard 748 is available

from Global Engineering Documents (1-800-854-7179). Information on earned value management systems is available at <http://www.acq.osd.mil/pm>.

Electronic Business (E-business): Means doing business online. E-business is often used as an umbrella term for having an interactive presence on the Web. A Government e-business initiative or project includes Web-services type technologies, component-based architectures, and open systems architectures designed around the needs of the customer (citizens, business, governments, and internal Federal operations).

Electronic Army (e-Army): The strategic employment of Information Technology to provide products, services, or knowledge to intended users—whether they are customers, constituents, internal operations employees, information providers, or business partners—that results in enhanced value to the Army. E-Army encompasses the full range of self-service applications available on Army Knowledge Online, Web services, enterprise resource planning systems; e-content and e-pubs programs; e-commerce activities; digital signatures; and automated processes that facilitate knowledge exchange.

Electronic Bid Solicitation (EBS): A means of placing service and supply solicitations and construction drawings and specifications on the Internet so that contractors can easily download the data and bid on the project. When there are hundreds of pages of specifications and drawings involved, it may not be practical to download the data from the World Wide Web. In that case, the Government contracting office may place the data on a CD-ROM.

Electronic Government (E-government or e-Gov): Use by the Government of Web-based Internet applications and other information technologies, combined with processes that implement these technologies, to “(A) enhance the access to and delivery of Government information and services to the public, other agencies, and other Government entities; or (B) bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation; (4) enterprise architecture (A) means (i) a strategic information asset base, which defines the mission; (ii) the information necessary to perform the mission; (iii) the technologies necessary to perform the mission; and (iv) the transitional processes for implementing new technologies in response to changing mission needs; and (B) includes (i) a baseline architecture; (ii) a target architecture; and (iii) a sequencing plan.

Electronic Government: The use by government of information technologies that have the ability to transform relations with citizens, employees, businesses partners, and other government organizations. Analogous to e-commerce, which allows businesses to transact with each other more efficiently and brings customers closer to businesses, e-government aims to make the interaction between government and citizens, government and business enterprises, and interagency relationships more friendly, convenient, transparent, and inexpensive.

Electronic Recordkeeping: The operation of recordkeeping systems requiring a machine interface for the human use of records. Examples of record media include magnetic tapes, disks and drums, video files, and optical disks.

Electronic Records: Records stored in a form that only a computer can process.

Emergency (As Related to Information Technology): Situations demanding immediate attention and resolution. Examples of situations that require emergency support are when problems are affecting mission production, when the local area network is not available, when the voice mail network is not available, when electronic mail is not available, or when calls are received from Commanding Officers or their representatives (i.e., Generals, Colonels and civilian equivalents, and their support staffs).

Emergency Operating Records: That type of vital records essential to the continued functioning or reconstitution of an organization during and after an emergency. (See Vital Records.)

Emergency Operations Center (EOC): A facility accommodating essential life support facilities, administrative equipment, communications capabilities, and personnel essential to the commander for planning, directing, and controlling emergency operations of assigned missions.

Emergency Preparedness and Operations: All aspects of accident prevention associated with the planning and execution of emergency and disaster preparedness, and response and recovery.

Emergency Relocation Site (ERS): A remote location, away from a USACE Division and/or District Office, where work activities can continue in an emergency. If the emergency renders the normal office space inaccessible, the ERS would be used to conduct regular business. The ERS is required to be capable of sustaining operations for up to 30 days. The ERS is required to have voice and data communications' capabilities in both secure and unsecured mode.

End User: The individual or groups who will operate the system for its intended purpose when it is deployed.

End-User-Operated Equipment: Information systems equipment operated by the end user.

Engineering Change Proposal (ECP): Form to officially request and document changes to the existing USACE Information Management/Information Technology infrastructure. The form is also used to track the review and approval infrastructure change process.

Enterprise: The **term** Enterprise, when used in the context to U.S. Army Corps of Engineers Enterprise Architecture, refers to activities spanning the work environment at

the corporate level that span the entire organization (HQ, Divisions, Districts, U.S. Army Corps of Engineers Research and Development Center, Field Operating Activities, and projects.

Enterprise Architecture (EA): A strategic, representational view that defines the business, information, applications (information systems), and information technologies (IT) necessary to support the mission, programs, and projects of the enterprise. The EA identifies the current “state” (Baseline or AS-IS) as well as the “objective, end-state” (Target or TO-BE) of the organization, and serves as a “blueprint” for implementing changes to the business, information, applications, and information technology needs of the enterprise. The EA is a “tool” used in the architecture alignment and assessment management process and is a critical component in the IT capital planning and investment control process for selecting, controlling and evaluation IT investments.

Enterprise Architecture Framework (EAF): A graphical presentation that documents the linkages between an enterprise’s business (mission and processes), information requirements, information system (applications), and information technology infrastructure (Information Assurance assets and technical standards). The EAF serves as a guide (and tool) for Information Technology capital planning and investment control, both at the strategic and operational levels.

Entity Relationship Diagram (ERD): Representing the enterprise as a data model within the DRM (EDM) will be at a conceptual, high-level composed of “data classes.”

Evaluate: To download and test software free for a limited time to determine whether you really want or need to purchase it.

Evidence of Performance: An Information Technology Investment Management (ITIM) core element that describes the artifacts, documents, or other proofs that support a contention that the key practices within a critical process have been or are being executed. This core element typically consists of physical, documentary, or testimonial evidence.

Environment: The conditions (physical, political, economic, and so on) within which an architectural configuration must operate.

Expenditures: A payment by check or equivalent action that constitutes a charge against the appropriation cites.

Extensible Markup Language (XML): A tagging language used to describe and annotate data so that it can be consumed by human and system interactions. XML is typically arranged hierarchically using XML elements and attributes. It also uses semantically rich labels to describe elements and attributes to enable comprehension.

Extranet: A private network that uses Internet protocols and the public telecommunications system to securely share information among selected external

users. A Extranet requires the use of firewalls, authentication, encryption, and virtual private networks (VPNs) that tunnel through the public network.

Facilities: Industrial property (other than materiel, special tooling, special test equipment, and military property) for production, maintenance, research, development, or testing, including real property (other than land) and rights therein, buildings, structures, improvements, and plant equipment (including capital leases).

Failure: The inability of a system or component to perform its required functions within specified performance requirements.

Federal Enterprise Architecture (FEA): A framework for describing the relationship between business functions and the technologies and information that support them. Major Information Technology (IT) investments will be aligned against each reference model within the FEA framework. The reference models required to be used during the FY 2005 budget formulation process are briefly described below.

Business Reference Model (BRM) – The BRM is a function-driven framework to describe the Lines of Business and Internal Functions performed by the Federal government independent of the agencies that perform them. Major IT investments are mapped to the BRM to identify collaboration opportunities.

Performance Reference Model (PRM) - The PRM is a standardized performance measurement framework to characterize performance in a common manner where necessary. The PRM will help agencies produce enhanced performance information; improve the alignment and better articulate the contribution of inputs, such as technology, to outputs and outcomes; and identify improvement opportunities that span traditional organizational boundaries.

Service Component Reference Model (SRM) – The SRM provides a common framework and vocabulary for characterizing the IT and business components that collectively compose an IT investment. The SRM will help agencies rapidly assemble IT solutions through the sharing and reuse of business and IT components. A Component is a self-contained process, service, or IT capability with predetermined functionality that may be exposed through a business or technology interface.

Technical Reference Model (TRM) – The TRM provides a foundation to describe the standards, specifications, and technologies supporting the delivery, exchange, and construction of business (or Service) components and e-Gov solutions. The TRM unifies existing Agency TRMs and electronic Government (e-Gov) guidance by providing a foundation to advance the reuse of technology and component services from a Government-wide perspective.

Federal Information Processing (FIP): Equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control display, switching, interchange, transmission, or reception of data for information by a Federal agency.

Some samples of FIP resources are software, services, support services, maintenance, related supplies, and systems.

Federal Occupational Safety and Health Administration (OSHA) Officer:

Investigator or compliance officer employed by; assigned to; or under contract to OSHA.

Federal Protective Service: The law enforcement organization within the Department of Homeland Security.

Federal Telecommunications System 2001: A long-distance telecommunications service including functionality such as switched voice service for voice or data; switched data service; switched digital integrated service for voice, data, image, and video; packet-switched service for data in packet form; video transmission for both compressed and wideband video; and dedicated point-to-point private lines for voice and data. GSA has in place two 8-year, fixed-price contracts covering FTS2001 services from 1999 through 2007.

Fiber Optic Cable: A cable using one or more optical fibers as the propagation medium.

Field Service Engineer: A person authorized by the contractor to perform maintenance (corrective and/or preventive) services at a facility.

File Server: Computer hardware used to provide storage for user data and software applications, processing capabilities for user workstations, and connection and control of workstations to the Local Area Network.

Financial Management System: Financial systems and the financial portion of mixed systems (see definitions below) that support the interrelationships and interdependencies between budget, cost and management functions, and the information associated with business activities.

Financial Systems: One or more applications used for any of the following: collecting, processing, maintaining, transmitting, and reporting data about financial events; supporting financial planning or budgeting activities; accumulating and reporting cost information; or supporting the preparation of financial statements. A financial system supports the processes necessary to record the financial consequences of events that occur as a result of business activities. Such events include information related to the receipt of appropriations or resources; acquisition of goods or services; payment or collections; recognition of guarantees, benefits to be provided, or other potential liabilities or other reportable activities.

Fire Prevention: Measures directed toward avoiding the inception of fire. Methods used to control or extinguish a fire.

Fire Safety Deficiency: A condition that reduces fire safety below the acceptable level, including noncompliance with standards, but that by itself cannot cause a fire to occur.

Firewall: System or group of systems that enforces an access control policy between two networks with the properties of allowing only authorized traffic to pass between the networks from inside and outside the controlled environment and is immune to penetration.

Firmware: Software (programs or data) that has been written onto read-only memory (ROM). Firmware is a combination of software and hardware. An example of firmware is a computer program in a read-only memory (ROM) integrated circuit chip. Another example is a program embedded in an erasable programmable read-only memory (EPROM) chip that may be modified by special external hardware but not by an application program.

Fiscal Quarter: The four quarters in a fiscal year (1 October through 30 September). First quarter is 1 October through 31 December; second quarter is 1 January through 31 March; third quarter is 1 April through 30 June; and fourth quarter is 1 July through 30 September.

Fiscal Year (FY): Any yearly accounting period without regard to its relationship to a calendar year. The fiscal year for the Federal Government begins on 1 October and ends on 30 September. The fiscal year is designated by the calendar year in which it ends; for example, fiscal year 1999 (FY 99) is the year beginning 1 October 1998 and ending 30 September 1999.

Fiscal Year Designation: A digit indicating the fiscal year in which the appropriation is available for obligation. In a funds citation, the FY is one digit. In many other uses, it is two digits. If funds are no-year funds (non-expiring), the FY designation is "X."

Full-Duplex: A circuit that permits simultaneous transmission in both directions.

Function: Within the context of the Army Enterprise Architecture framework, a synonym for activity.

Functional Manager: The senior operating official at all levels exercising managerial control of an activity or operation. This individual usually can acquire and commit resources for the abatement of occupational safety and health hazards.

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).

Funding Source: Any budgetary resource used for funding the Information Technology (IT) Investment. Budgetary resource is defined in section 20. For each funding source, identify the budgetary resources (direct appropriation or other specific budgetary resources such as working capital funds, revolving funds, user fees, etc.) for a project or investment. Identify the budget account and organization or operating division. Add as many funding source line items as are appropriate for the investment or project. To avoid double counting, do not report any accounts receiving intra-governmental payments to purchase IT investments or services.

Funding Source Subtotal: The totals of all funding sources used for funding the Information Technology Investment.

Geographic Information System (GIS): A system that has tools used to gather, transform, manipulate, analyze, and produce information related to the surface of the earth. This data may exist as maps, 3D virtual models, tables, and/or lists.

Global Positioning System (GPS): A worldwide satellite navigational system formed by 24 earth-orbiting satellites and their corresponding receivers on the earth.

Governmental In Nature/Inherently Governmental: Inherently governmental functions that are so intimately related to the public interest as to mandate performance by Government employees or military personnel. These functions include those activities that require either the exercise of discretion in applying Government authority or the making of value judgments in making decisions for the Government. Governmental functions normally fall into two categories: 1) the act of governing, i.e., the discretionary exercise of Government authority, and 2) monetary transactions and entitlements. All functions are either Governmental In Nature functions or commercial activities.

Government-Furnished Equipment (GFE): Equipment originally in the possession of or acquired by the Government. This is a subset of Government-furnished property. GFE items are delivered or otherwise made available to the Service Provider for use in performing this contract.

Government-Furnished Property (GFP): All equipment, materials, supplies, facilities, contracts, and land possessed by the Government and, subsequently, delivered or otherwise made available to the Service Provider for use in performing this contract.

Hardware: The generic term dealing with physical items (as distinguished from the capabilities or functions), such as equipment, tools, implements, instruments, devices, sets, fittings, trimmings, assemblies, subassemblies, components, or parts. The term is often used in regard to the stage of development, as in passage of a device or component from the design stage into the hardware stage as the finished object. In data automation, the physical equipment or devices forming a computer and peripheral components.

Hazardous Material (HM): Any material that because of its quantity, concentration, or physical, chemical, or infectious characteristics, may pose a substantial hazard to human health or the environment. This definition includes all extremely hazardous substances, hazardous chemicals, hazardous substances, and toxic chemicals. HM is any material regulated as HM, per reference 40 CFR Part 261, or any material that requires a material safety data sheet (MSDS), per reference 40 CFR Part 261. HM is also any material having components that meet or have the potential to meet the definition of hazardous waste per reference 40 CFR 261, during any phase of its existence: end use, treatment, handling, packaging, storage, transportation, or disposal.

Hazardous Waste: A solid waste or combination of solid wastes that, because of quantity, concentration, or physical, chemical, or infectious characteristics, may 1) cause, or significantly contribute to, an increase in mortality or an increase in serious irreversible or incapacitating reversible illness, or 2) pose a substantial actual or potential hazard to human health or the environment when improperly treated, stored, transported, disposed of, or otherwise managed.

Help Desk: Structured contact organizational section that responds to technical assistance questions and calls pertaining to software- or hardware-related computer questions.

High Interest Areas: Work areas or operations that require additional attention or added inspections because of increased accident potential due to the nature of work performed, physical conditions, type of materials handled, or increased accident experience. These areas are designated by a Major Army Command or installation safety, fire protection, or industrial hygienist official.

Horizontal Portal: A portal which pulls together several vertical portals and which is standardized across an enterprise.

Imagery: A pictorial representation of a person, place, thing, idea, or concept, either real or abstract, used to convey information.

Indirect Cost: Cost (labor, material, contracts, travel, and transportation) that cannot be identified directly with the final cost objective (that is, customer orders or work authorization).

Inflation: A general increase in price levels (economist's definition); an increase in cost of an item without a corresponding increase in real value received, that is, no change in quality or quantity received (consumer's definition).

Information: The meaning that a human assigns to data by means of the known conventions used in their representations. Information is a shared resource and is not owned by any organization within the restrictions of security, sensitivity, and proprietary rights.

Information Exchange Requirement: Substantive content, format, throughput requirements, and classification level.

Information Management (IM): Planning, budgeting, manipulating, and controlling of information throughout its life cycle.

Information Management Plan (IMP): A 5-year strategic plan based on the overall Director of Information Management corporate goals in meeting the Corps' missions and responsibilities to satisfy customer information needs, provide focused IM leadership, produce a quality product, apply IM technology wisely, and accomplish missions within the funding environment.

Information Mission Area (IMA): The resource requirements and associated information management activities employed in the development, use, integration, and management of information. The umbrella term covering all activities involving information as a resource, specifically the disciplines of telecommunications, automation, visual information, records management, and publications and printing. Includes management of libraries.

Information Requirement: The expression of need for data or information to carry out specified and authorized functions for management purposes that require the establishment or maintenance of forms or formats, or reporting or recordkeeping systems, whether manual or automated.

Information Resources: The term information resources has the meaning given such term in section 3502(6) of title 44, United States Code.

Information Resources Management: The term information resources management has the meaning given such term in section 3502(7) of title 44, United States Code.

Information Resources Management (IRM) Strategic Plan: Strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency Information Resource Management Strategic Plan (IRM) as required by 44 U.S.C. 3506 (b) (2). IRM Strategic Plans should support the agency Strategic Plan required in OMB Circular A-11, provide a description of how information resources management activities help accomplish agency missions, and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

Information System (IS): The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or not. IS means a discrete set of information technology, data, and related resources, such as personnel, hardware, software, and associated information technology services organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

IS Security Incident: An unexplained event that could result in the loss, corruption, or the denial of access to data, as well as any event that cannot be easily dismissed or explained as normal operations of the system. Also, an occurrence involving classified or sensitive information being processed by an IS where there may be: 1) a deviation from the requirements of the governing security regulations; 2) a suspected or confirmed compromise or unauthorized disclosure of the information; 3) questionable data or information integrity (for example unauthorized modification); 4) unauthorized modification data; or 5) unavailable information for a period of time.

IS Serious Incident: Any event that poses grave danger to the Army's ability to conduct established information operations.

Information Technology (IT): Defined by the Clinger-Cohen Act of 1996, sections 5002, 5141, and 5142, 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. For purposes of this definition, equipment is “used” by an agency whether the agency uses the equipment directly or it is used by a contractor under a contract with the agency that (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. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Information Technology (IT) Architecture: An integrated framework for evolving or maintaining existing IT and acquiring new IT to achieve the organization’s strategic and business goals. A complete IT architecture should consist of both logical and technical components. The logical architecture provides the high-level description of the agency’s mission, functional requirements, information requirements, system components, and information flows among the components. The technical architecture defines the specific IT standards and rules that will be used to implement the logical architecture.

Information Technology (IT) Capital Planning and Investment Control: An end-to-end integrative process that frames and manages the life cycle of an IT investment. Its purpose is to maximize the value and to assess and manage the risks of the IT acquisitions of the Army. The process includes the selection, management, and evaluation of IT investments.

Information Technology (IT) Facility: An organizationally defined set of personnel, hardware, software, and physical facilities, operated within or on behalf of the DoD, a primary function of which is the operation of information technology. An Information Technology Facility includes 1) personnel who operate computers or telecommunications systems; develop or maintain software; provide user liaison and training; schedule computers; prepare and control input data; control, reproduce, and distribute output data; maintain tape and disk libraries; provide security; and provide administrative support to personnel engaged in these activities; 2) the owned or leased computer and telecommunications hardware, including central processing units; associated peripheral equipment such as disk drives, tape drives, printers, and consoles; data entry equipment; telecommunications equipment including control units, terminals, modems, and dedicated telephone and satellite links provided by the facility to enable data transfer and access to users (hardware acquired and maintained by users of the facility is excluded); 3) the software, including operating system software, utilities, language processors, access methods, database processors, and similar multiuser software required by the facility for support of the facility and/or general use by users of the facility; 4) the physical facilities, including computer rooms, tape and disk libraries, stockrooms and warehouse space, office space, and physical fixtures.

Information Technology (IT) Functional Proponent (FP): The organization or person that sponsors/identified the IT requirement/investment and submitted the requirement for funding. The functional proponent for an IT investment, and the individual held accountable for value/benefit realization.

Information Technology (IT) Investment: An asset, initiative, program, or project as well as service and support service for which the enterprise is or will allocate resources, in particular funds. Also, the “decision” by the organization to expend resources or the actual expenditure of resources on selected information technologies or IT-related initiatives for which there is an expectation that the benefits from the expenditure exceed the value of the resources expended.

Information Technology (IT) Investment Board: A decision-making body made up of senior program, financial, and information managers that is responsible for making decisions about IT projects and systems, based on comparisons and trade-offs between competing projects with an emphasis on meeting mission goals.

Information Technology (IT) Investment Decision Authority: The organization's commander or designated senior management official having the authority to approve the proposed IT investment and/or aggregation of IT investments as having value/benefit to the organization, i.e., approve the authority levels recommended via the Capital Planning and Investment Control Process.

Information Technology (IT) Investment Portfolio: The combination of all IT assets, resources, and investments owned or planned by an organization in order to achieve its strategic goals, objectives, and mission.

Information Technology (IT) Investment Portfolio System (ITIPS): The sole official source for all USACE IT investment information.

Information Technology (IT) Management: An approach used by IT project managers to direct, control, administer, and regulate a project team creating an IT asset such that the resultant product meets its requirements upon delivery.

Information Technology (IT) Management Process: An end-to-end integrated process that includes the information management/ information technology (IM/IT) business planning, business/functional process improvement, capital investment planning and investment control IT management and oversight, acquisition of C4/IT, fielding, and prioritization.

Information Technology (IT) Project: An organizational initiative employing or producing IT or IT-related assets. Each project has or will incur costs for the initiative, has expected or realized benefits arising from the initiative, has a schedule of project activities and deadlines, and has or will incur risks associated with engaging in this initiative.

Information Technology (IT) Support Agreement: An agreement to provide recurring IT support, the basis for reimbursement (if any) for each category of support, the billing and payment process, and other terms and conditions of the agreement.

Inspection: The process of determining compliance with standards through formal and informal surveys of workplaces, operations, and facilities.

Installation Service Support Agreement: The document that dictates the agreement between tenant organizations for installation support and general services.

Instance (Instantiation): In programming, the creation of a real instance or particular realization of an abstraction or template such as a class of objects or a computer process. To instantiate is to create such an instance by, for example, defining one particular variation of object within a class, giving it a name, and locating it in some physical place.

Institutionalization: The building of corporate culture that supports methods, practices, and procedures so that they are the ongoing way of doing business.

Integrity (of information): Assurance of protection from unauthorized change. A degree of protection for data from intentional or unintentional alteration or misuse.

Integrated Project Team (IPT): A multidisciplinary team lead by a program manager responsible and accountable for planning, budgeting, procurement and life-cycle management of the project to achieve its cost, schedule and performance goals. Team skills include budgetary, financial, capital planning, procurement, user, program, value management, earned value management, and other staff as appropriate.

Integrated Service Delivery: The provision of Internet-based Federal Government information or services integrated according to function or topic rather than separated according to the boundaries of agency jurisdiction.

INTEL: A US microelectronics manufacturer.

Interest: A service charge for the use of money commonly computed as an annual percentage of outstanding principal.

Interface: A boundary or point common to two or more similar or dissimilar telecommunications systems, subsystems, or other entities at which necessary information flows take place.

Internal Control: A plan or organization intended to coordinate methods and measures within an organization to safeguard assets, check the accuracy and reliability of accounting and related data, promote operating efficiency, and encourage adherence to managerial policies.

Internal Control Documentation: Written policies, organization charts, procedural write-ups, manuals, memoranda, flow charts, decision tables, completed

questionnaires, software, and related written materials used to describe the internal control methods and measures, to communicate responsibilities and authorities for operating such methods and measures, and to serve as a reference for persons reviewing the internal controls.

Internal Control Standards: The standards issued by the Comptroller General for use in establishing and maintaining systems of internal control. Those standards are applicable to all operations and administrative functions but are not intended to limit or interfere with duly granted authority for the development of legislation, rule making, or other discretionary policy making in an agency.

Internal Control Techniques: The application of prescribed processes and documents to efficiently and effectively accomplish an internal control objective and to help safeguard an activity from waste, loss, unauthorized use, or misappropriation.

Internal Controls: The manner in which financial, manpower, and property resources are to be controlled and safeguarded by the regular authorization, approval, documentation, recording, reconciling, reporting, and related accounting processes.

Internet: A global collaboration of data networks that are connected to each other, using common protocols (for example, TCP/IP) to provide instant access to an almost indescribable wealth of information from components around the world.

Interoperability: The ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner.

Intra-Agency Agreement: A formal agreement between two entities within the DoD usually involving a transfer of funds.

Intra-Government Agreements: A project order under 41 U.S.C. 23, an Economy Act (31 U.S.C. 1535), or a procurement order to another military department for reimbursable procurement or direct citation.

Intranet: Similar to the Internet but accessible only by the organization's employees or others with authorization. Usually internal to a specific organization.

Inventory: The organized and itemized list of assets, e.g., IT products, services, or contracts.

Investment Description (ID): Narrative information and funding requirements prepared by the Information Technology (IT) Functional Proponent/Project Manager which describe the business value and risk of the IT investment. The Functional Proponent/Project Manager submits the ID at the beginning of the Capital Planning and Investment Control Process.

Inventory of Federal Government Property: Consists of tangible personal property (goods) 1) to be consumed in normal operations, 2) to be incorporated in production of

goods for later consumption in normal operations, or 3) in process or finished that will ultimately be sold. Included are goods in the hands of others, yet owned by the Government. Goods issued for use in construction of real or personal property are accountable as construction in progress and are excluded from inventory.

Javits-Wagner-O'Day (JWOD): The JWOD Program creates jobs and training opportunities for people who are blind or who have other severe disabilities. Its primary means of doing so is by requiring Government agencies to purchase selected products and services from nonprofit agencies employing such individuals.

Joint Technical Architecture-Army (JTA-A): The complete set of rules derived from the JTA that prescribes the technical standards for Army Information Technology systems and enables interoperability among joint systems.

Key: Information (usually a sequence of random or pseudo-random binary digits) used initially to set up and periodically change the operations performed in crypt-equipment for the purpose of encrypting or decrypting electronic signals, determining electronic countermeasures patterns (e.g., frequency hopping or spread spectrum), or producing other keys.

Key Practices: The infrastructures and activities that contribute most to the effective implementation and institutionalization of a critical process.

Key Management: Process by which a key is generated, stored, protected, transferred, loaded, used, and destroyed.

Knowledge Management (KM): Knowledge Management is an integrated, systematic approach to identifying, managing, and sharing all of an enterprise's information assets, including databases, documents, policies and procedures, as well as previously unarticulated expertise and experience resident in individual workers. Informally, KM is a way of putting information, communities, processes, and tools together to allow people to do better work and make better decisions.

Lease Agreement: An agreement to convey the use of an asset or part of an asset (such a part of a building) from one entity, the lessor, to another, the lessee, for a specified period of time in return for rent or other compensation.

Legacy: Refers to both software and/or hardware from previous technology generations. From a software perspective, legacy in the Technical Reference Model refers to any technologies that are not Internet enabled and not component-based.

Letter of Obligation: A binding agreement between government entities for products or services.

Liability: A debt or other legal obligation that must be liquidated by payment, renewed, or refunded at some future date.

Life Cycle: The total phases through which an item progresses from the time it is initially developed until the time it is either consumed, in use, or disposed of as being excess.

Life-cycle Costs: Means the overall estimated cost, both Government and contractor, for a particular program alternative over the time period corresponding to the life of the program, including direct and indirect initial costs plus any periodic or continuing costs of operation and maintenance.

Life Cycle of Records: The management concept that records pass through three stages: creation, maintenance and use, and disposition.

Lines of Business: Groups of customers and/or suppliers working in the same business sector. Example: Environmental Management

Liquidated Damages: An advance contractual agreement as to the damages one party will suffer if the other fails to perform. The liquidated damages referred to the “Consequences of Contractor’s Failure to Perform Required Services” clause are to compensate the Government for additional administrative expenses incurred by the Government as a result of the defects and represents an amount in addition to the price of the defects.

Local Area Network (LAN): A system that allows microcomputers to share information and resources within a limited (local) area.

Local Area Transport (LAT): A DEC-specific, nonroutable network protocol for connecting terminals to a LAN. Connections are typically between a DEC terminal server and a Virtual Address extension. LAT operates at the transport layer. LAT is not routable because it lacks a network layer and therefore must be bridged in an enterprise network instead of routed.

Lost Time: Time lost due to accident(s) resulting in traumatic injury or death and of accidents resulting in damage to Government-furnished property.

Lot: A collection of product or service outputs from which a sample is to be drawn and inspected to determine conformance with the standard made available to the Service Provider for performance under the contract or Letter of Obligation.

Lot Size: The total number of product or service outputs in a lot.

Machine Readable: Data and information storage media requiring the use of one or more information system components for translation into a medium understandable and usable to humans.

Mainframe: Computer system that is characterized by dedicated operators (beyond the system users); high-capacity, distinct storage devices; special environmental considerations; and an identifiable computer room or complex.

Maintenance: The process of modifying a system or component after delivery to correct faults, improve performance or other attributes, or adapt to a changed environment. Preventative measures, normal repairs, replacement of parts and structural components, and other activities needed to preserve an asset so that it continues to provide acceptable services and achieves its expected life.

Maintenance and Repair Expense: Any costs incurred for an asset that do not significantly improve the quality or quantity of outputs of the original asset or that fail to significantly increase the economic life of the original asset. These costs, regardless of the dollar amount, should be recognized as maintenance and repair expenses (i.e., not added to the depreciable basis of the original asset nor capitalized separately).

Major IT Investment: Major IT investment means a system or investment that requires special management attention because of its importance to the Corps' mission; investment was a major investment in FY04 and is continuing; investment is for financial management and spends more than \$500,000; investment is directly tied to the top two layers of the Federal Enterprise Architecture (Services to Citizens and Mode of Delivery); investment is an integral part of the Corps' modernization blueprint (EA); investment has significant program or policy implications; investment has high executive visibility; and all e-government investments or those that use e-business technologies regardless of costs. If you are unsure about what investments to consider as "major," consult your agency budget officer or OMB representative. Systems not considered "major" are "non-major."

Management Decision Evaluation Package (MDEP): An 8-year package of dollars and manpower to support a given program or function. The Budget Increment package is the first three budget and execution years of the Management Decision Evaluation Package, and the Program Development Increment Package is the 5 program years following.

Management Information System: An organized method of providing past, present, and projected information relating to internal operations and external developments. It supports the planning, control, and operating functions of an organization by furnishing necessary information to decision makers in a timely fashion.

Master Plan: An enterprise-wide planning directive that establishes the vision, goals, and objectives of the enterprise; establishes an enterprise-level procedure for achieving the vision, goals, and objectives; specifies actions required to achieve the vision, goals, and objectives; identifies roles and assigns responsibilities for executing the specified actions; establishes priorities among actions and relevant supporting programs; and establishes performance measures and responsibilities for measuring performance.

Master/Community Antenna Television (M/CATV) System: A facility consisting of a television reception service that receives broadcast radio-frequency television signals and/or FM radio programs and distributes them via signal generation, reception, and control equipment.

Maturity Model: A model of the stages through which organizations progress as they define, implement, evolve, and improve their processes. This model serves as a guide for selecting process improvement strategies by facilitating the determination of current process capabilities and identification of the issues most critical to quality and process improvement.

Maturity Stage: A well-defined evolutionary plateau toward achieving mature processes.

Maximum Allowable Defect Rate (MADR): The defect rate for the population above which the contractor's quality control for a particular work requirement is unsatisfactory. MADR does not represent a threshold above which deductions are taken. Deductions to the contract price are taken for all defects (with credit for rework to the extent appropriate) irrespective of whether the MADR is exceeded or not.

Measure: One of several measurable values that contribute to the understanding and quantification of a key performance indicator.

Message (Telecommunications): Record information expressed in plain or encrypted language and prepared in a format specified for intended transmission by a telecommunications system.

Metadata: Information describing the characteristics of data; data or information about data; and descriptive information about an organization's data, data activities, systems, and holdings.

Methodology: A documented approach for performing activities in a coherent, consistent, accountable, and repeatable manner.

Metrics: The elements of a measurement system consisting of key performance indicators, measures, and measurement methodologies.

Microcode: A very low level code that defines how a computer operates. It specifies what the computer processor does when it executes a machine-code instruction.

Milestone: A point-in-time or event that an expected deliverable or activity is scheduled to be started, completed or is in the process of being completed. A milestone is typically used to measure progress, and to hold an individual, team, or organization accountable for success or failure.

Mission: The enduring, chartered, long-term goal(s) of an organization.

Mission Critical (MC) Information System: A system that meets the definitions of "information system" and "national security system" in the Clinger–Cohen Act, the loss of which would cause the stoppage of war-fighter operations or direct mission support of war-fighter operations.

Mission Essential (ME) Information System: A system that meets the definitions of “information system” and “national security system” in the Clinger–Cohen Act that the acquiring component head or designee determines is basic and necessary for the accomplishment of the organizational mission. (The definition of “the Organizational Mission” is one of the organizational missions of the Army—not just a single MACOM or DA functional proponent.)

Mission-Related: Processes and functions that are closely related to the mission (for example, the mission of Direct and Resource the Force has the mission-related functions of planning, programming, policy development, and allocating of resources).

Mixed System: An information system that supports both financial and non-financial functions of the Federal Government or components thereof.

Modification: The act of changing a system or component to improve performance or some other attribute or to adapt the system or component to function in a changed environment.

Morale, Welfare, and Recreation (MWR) Programs: Programs that provide for the mission sustainment and community support for authorized DoD personnel. Military MWR programs (exclusive of private organizations as defined in DoDI 1000.15) are located on DoD installations or on property controlled (by lease or other means) by DoD or furnished by a DoD contractor.

Motion Media: A series of images viewed in rapid succession, giving the illusion of motion, obtained with a motion picture or video camera.

Multimedia: The synchronized use of two or more types of media, regardless of the delivery medium.

Need: A capability shortfall such as those documented in a mission needs statement, deficiency report, or engineering change proposal. A new technology application or breakthrough may create a new expressed need by the customer.

Negotiation: The communication by any means of a position or an offer on behalf of the United States, DoD, or any office or organizational element thereof, to an agent or representative of a foreign government (including an agency, instrumentality, or political subdivision thereof) or of an international organization in such detail that the acceptance in substance of such position or offer would result in an international agreement. The term also includes any communication conditional on subsequent approval by higher authority but excludes mere preliminary, exploratory, or informal discussions or routine meetings conducted on the understanding that the views communicated do not and will not bind any side. (Normally, the approval authority will authorize the requesting command to initiate and conduct the negotiation.)

Negotiated Contract: A purchase or sales agreement made by a Government agency, normally without employing formal advertising.

Network: Communications medium and all components attached to that medium that is used to transfer information. Components may include Information Systems, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Networthiness: Risk management accomplished through the identification, measurement, control, and minimization of security risks in Information Technology systems to a level commensurate with the value of the Army enterprise.

Networthiness: Certification: To be defined by the Department of Army at a future date.

New IT Investment: Means an IT investment that is newly proposed by the agency and has not been previously funded by OMB. This does not include projects that have existed within the agency but have not previously been reported to OMB.

News Clip: A news story of an event recorded and released on motion picture or videotape for viewing by an internal Army audience or the general public.

Non-Appropriated Fund(s) (NAF): Cash and other assets received from sources other than monies appropriated by the Congress of the United States. (NAF must be resources of an approved Non-Appropriated Fund Instrumentality.) NAF are U.S. Government funds, but they are separate from funds that are recorded in the books of the Treasury of the United States. They are used for the collective benefit of the authorized patrons who generate them.

Non-Appropriated Fund Instrumentalities (NAFIs): Legally constituted “instrumentalities of the United States” that are separate from appropriated funds (APF) of the U.S. Treasury. Funds in NAFI accounts are Government funds, and NAF property, including buildings, is Government property. They are not commingled with APF and are managed separately, even when supporting a common program or activity.

Non-Consumable Supplies: A program expense classified as a capital expendable consisting of net issues of non-expendable supplies that are valued at \$250 or more per item and that do not lose their identity upon issue.

Non-Expendable: Property that maintains its identity throughout its entire period of usefulness and must be accounted for until properly disposed of by authorized procedures.

Non-Financial System: A system that supports management functions of the Federal Government or components thereof and does not record financial events or report financial information.

Non-Major Information Technology (IT) Investment: Any initiative or project not meeting the definition of major defined above but that is part of the agency's IT investments. All non-major investments must be reported individually on the Exhibit 53.

Non-Public Data/Information: Data/information that is personally identifiable and subject to the Privacy Act, classified according to the National Security Act, subject to a Freedom of Information Act exemption, or sensitive.

Objectives: Quantified goals identifying performance measures that strive to improve the effectiveness or efficiency of agency programs in support of mission goals.

Occupational Hazard: Conditions, procedures, and practices directly related to the work environment that create a potential for producing occupational injuries or illnesses.

Occupational Illness: Any abnormal physical condition or disorder other than one resulting from an injury caused by long-term or short-term exposure to chemical, biological, or physical agents associated with the occupational environment.

Occupational Injury: An on-duty injury to Government personnel caused by events or conditions in the occupational environment.

Occupational Safety and Health Deficiency: A deficiency not in compliance with Occupational Safety and Health Administration or Army Occupational Safety and Health Program requirements, but do not, in themselves, create a potential for producing an occupational injury or illness. Deficiencies may, however, create a potential for secondary injuries or illnesses or may contribute to the severity of an injury or illness that has already occurred. Examples include lack of fire detection or suppression equipment and system, a broken smoke alarm, lack of exit signs, and railings that are two inches below standard height. A clear distinction between hazards and deficiencies may not always be possible; therefore, the judgment and experience of qualified safety, fire protection, and health personnel must be relied upon.

Occupational Safety and Health Hazard Abatement: The elimination or permanent reduction of an occupational safety and health hazard or deficiency by bringing it into compliance with applicable safety, fire prevention, and health requirements or by taking equivalent protective measures.

Occupational Safety, Fire Prevention, and Health Guidance: Occupational safety, fire prevention, and health requirements that are included in Occupational Safety and Health Administration standards, Army Occupational Safety and Health standards, technical manuals, Army directives, national consensus standards, or other regulatory Federal standards or directives.

Office Automation: The USACE working definition of Office Automation is the use of computer systems and communications technology to perform general, everyday tasks such as document management, electronic mail, archiving and retrieval of text/graphics groups. The operation of systems in which a machine interface is required for the user

to create, work with, display or delete records within a general office environment. Office Automation embodies a core group of functionality consisting of word processing, spreadsheet, presentation, office database, electronic forms, calendar/scheduler, electronic mail, Web browser and operating systems used to support day-to-day office operations. These generic software tools are used for general office functions not specific to any Business Area. Local Area Networks/Wide Area Networks (LANs/WANS) used only for communications are reported under the classification for LAN.

Offsetting Collections: Collections from Government accounts or from transactions with the public. The two major categories of offsetting collections are offsetting receipts (amounts deposited to receipt accounts) and offsetting collections credited to appropriation or fund accounts.

Offsetting Receipts: Collections that are deposited into proprietary Miscellaneous Receipt Accounts of the Department of the Treasury. Applicable deposits offset the collecting Agency's budget authority and outlays.

Ongoing IT Investment: Means a project that has been through a complete budget cycle with OMB and represents budget decisions consistent with the President's Budget for the current year (BY-1).

Operational and Available: This refers to a system(s) functioning within vendors' hardware, software, and application specifications and being available for use by the user community.

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 (OV) (Architecture): A description (often graphic) of the operational elements, assigned tasks, and information flows required to accomplish or support a war-fighting function. It defines the type of information, the frequency of exchange, and the tasks supported by these information exchanges.

Optical Disk: A non-contact, random-access disk typically tracked by optical laser beams and used for mass storage and retrieval of generally digitized text and graphics.

Organizational Messaging: Correspondence that is used to conduct the official business of the Army. Any message that commits resources, directs action, clarifies an official position, or issues official guidance is considered an organizational message.

Original Equipment Manufacturer (OEM): The actual manufacturer and point of origin of the equipment. The OEM provides schematics and standards for maintenance and

repair of the equipment, and equipment shall be maintained in accordance with these practices.

Operational (Steady State): Means an asset or part of an asset that has been delivered and is performing the mission.

Organizational Commitment: An INFORMATION TECHNOLOGY INVESTMENT MANAGEMENT (ITIM) core element that describes the management actions that ensure that the critical process is established and will endure. This core element typically involves establishing organizational policies and senior management sponsorship. Outcome: The actual results, effects, or impacts of a business initiative, program, or support function. Actual outcomes typically are compared to expected outcomes.

Overhead: Expenses incurred in support of the overall mission that are not identifiable to a customer order and are equitably shared by all customers of the activity (for example, supervisory and administrative salaries).

Overhead Rate: The rate, determined by performing organizations, used to allocate operating costs not directly identifiable to the work order. Includes supervisory and general and administrative expenses as well as miscellaneous materiel and supplies.

Outcome: The actual results, effects, or impacts of a business process, procedure, activity, task or action taken or not taken. Actual outcomes typically are compared to expected outcomes.

Password: Protected, private character string used to authenticate an identity or to authorize access to data.

Paying Office: A disbursing office. In the case of contracts, the place named in the contract for forwarding invoices for payment.

Payment Due Date: The date on which payment is to be made. If the date falls on a nonworking day, payment is made on the following workday.

Performance Certificate: A written statement prepared by an authorizing official that the goods or services called for in a contract have been delivered or performed satisfactorily.

Performance Indicator: A characteristic of a work output that can be measured.

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 those goals, and report on the success in meeting those goals.

Performance Measure: A quantitative or qualitative characterization of performance.

Performance Measurement: A process of assessing progress toward achieving predetermined goals, including information on the efficiency with which resources are transformed into goods and services (outputs), the quality of those outputs (how well they are delivered to clients and the extent to which they are satisfied), and outcomes (the results of a program activity compared to its specific contributions to program objectives).

Periodical: A nondirective classified or unclassified Army magazine or newsletter type publication published annually or more often to disseminate information necessary to the issuing activity with a continuing policy regarding format, content, and purpose. A periodical is usually published to inform, motivate, increase knowledge, or improve performance. It contains official or unofficial information or both.

Peripheral: A computer device, such as a CD-ROM drive or printer, that is not part of the essential computer, i.e., the memory and microprocessor. Peripheral devices can be external, such as a mouse, keyboard, printer, monitor, external Zip drive or scanner, or they can be internal, such as a CD-ROM drive or internal modem.

Permanent Record: Information that has been determined by the Archivist of the United States to have sufficient value to warrant its preservation by the National Archives and Records Administration for the life of the Republic.

Persistent Cookies: Cookies that can be used to track users over time and across different Web sites to collect personal information.

Personal Computer: A computer (normally a small desktop type) Information System that contains an operating system and software applications.

Personal Property: Property of any kind except real property and records of the Federal Government. It includes all equipment, materials, and supplies unless permanently affixed to real property.

Photojournalism: The collection and presentation of a story, through still photography, of a significant event, normally to support the news media or internal publications.

Planning: Means preparing, developing or acquiring the information you will use to design the project; assess the benefits, risks, and risk-adjusted life-cycle costs of alternative solutions; and establish realistic cost, schedule, and performance goals, for the selected alternative, before either proceeding to full acquisition of the capital project or useful segment or terminating the project. Planning must progress to the point where you are ready to commit to achieving specific goals for the completion of the acquisition. Information gathering activities may include market research of available solutions, architectural drawings, geological studies, engineering and design studies, and prototypes. Planning is a useful segment of a capital project. Depending on the nature of the project, one or more planning segments may be necessary.

Policy: A guiding principle, typically established by management, to influence and determine the results or outcomes of business processes or personnel practices.

Portability: The ease with which a system or component can be transferred from one hardware or software environment to another.

Portal: A portal can be defined as software that provides access through a browser to a wide range of data stores—e-mail, data bases, analytical software, the Internet, billing and sales records, and other sources. A portal is different from other Web pages in that a portal is customizable by the user as his needs and interests change.

Horizontal Enterprise Portal: A portal which pulls together several vertical portals and which is standardized across an enterprise.

Vertical Enterprise Portal: A portal which serves a specific community of interest. An organization may have several vertical portals, but will probably have only one horizontal portal.

Portfolio: see Information Technology Investment Portfolio.

Prerequisites: An Information Technology Investment Management (ITIM) core element that describes the conditions that must exist within an organization to successfully implement a critical process. This core element typically involves resources, organizational structures, and training.

Preventive Maintenance (PM): Services that are periodic in nature and are required to maintain the equipment in such condition that it may be operated in accordance with its intended design and functional capacity with minimal incidence of malfunction or inoperative conditions.

Principles (CeA-Specific):

Printing: The processes of composition, plate making, presswork, and binding, including micropublishing, for the production of publications.

Private Parties: U.S. Government activities; foreign Governments, firms, and organizations; and international organizations, other than Foreign Military Sales (FMS) customers and FMS/International Military Education and Training recipients and U.S. companies.

Procedure: A written description of a sequence of actions to be taken to perform a given task.

Process: A sequence of procedures, activities/events, and tasks/actions performed for a given purpose.

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, with a beginning, an end, and clearly defined inputs and outputs that deliver value to customers.

Process Maturity: The extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates the sophistication of an organization's process and the consistency with which it conducts these processes.

Process Owners: HQDA functional proponents, MACOMs, and others who have responsibility for any mission-related or administrative work process.

Procurement/Contracting: Purchasing, renting, leasing, or otherwise obtaining supplies or services from non-Federal sources. Includes description (but not determination) of supplies and services required, selection and solicitation of sources, preparation and award of contracts, and all phases of contract administration. Does not include making grants or cooperative agreements.

Product Development Team (PDT): A group of people, each with assigned responsibilities, who work closely together to achieve the shared objective of delivering, operating, or maintaining an information system. The project team may work together on tasks that are highly interdependent and may exercise a level of autonomy in managing their activities in pursuit of those objectives. The project team may vary in size from a single individual assigned part-time to a large organization assigned full-time.

Program Managers: Responsible for assembling components and technology to support the implementation of a project or program that may require cross-agency collaboration and the reuse of agency assets.

Program/Project Delivery Team (PDT): The individuals serving on a team who share collective responsibility for the successful delivery of the service, product, program or project assigned the team. A PDT is often composed of individuals with diverse competencies needed to ensure delivery success.

Program/Project Manager (PM): The individual appointed, verbally or in writing, by a management official responsible for the delivery of agreed upon deliverables to the Information Technology investment sponsor. A steward responsible for the resources provided and for the execution of the approved program/project management plan.

Project Management Business Process (PMBP): The fundamental USACE practices and procedures used to deliver quality projects. It embodies communication, leadership, systematic and coordinated management, teamwork, partnering, effective balancing of competing demands, and primary accountability for the life cycle of a project.

Project Manager: The individual with business responsibility for an entire project. This individual typically directs, controls, administers, and regulates a project developing or acquiring an information system.

Project Plan: A document that describes the technical and management approach to be followed for a project. The plan typically describes the work to be done, the resources required, the methods to be used, the procedures to be followed, the schedules to be met, and the way that the project will be organized.

Property: Anything that may be legally owned.

Property Custodian: An individual, provided by the service provider, designated in writing and located at the activity site who has physical custody and control over personal property.

Proponent: An Army organization or staff that has been assigned primary responsibility for material or subject matter in its area of interest.

Public Key Infrastructure (PKI): A system of registration authorities that authenticate the validity of each party involved in a transaction.

Publications: Items of information that are printed or reproduced, whether mechanically or electronically, for distribution or dissemination, usually to a predetermined audience. Generally, they are directives, books, pamphlets, posters, forms, manuals, brochures, magazines, and newspapers produced in any media by or for the Army.

Publicly Accessible Web site (or public Web site) on the World Wide Web: A Web site with access unrestricted by password or PKI user authorization. “Public” refers to the at-large audience on the Internet, anyone who can access a Web site through a browser.

Publishing: Actions involved in issuing publications; involves creating, preparing, coordinating, approving, processing, printing, and distributing or disseminating publications.

Purchase Order: A document that the contracting officer issues to a vendor for supplies, equipment, or services which total \$25,000 or less. It becomes a contract upon acceptance by the vendor.

Purchase Request: A document which is the first step in the procurement process. It can be reviewed by all interested activity officials before a purchase is made.

Purpose: The desired outcome for each critical process.

Quality Assurance (QA): Management of the output quality and responsiveness of a facility support contractor, starting with the early stages of quality development and running through every phase to contract close-out. The term quality assurance is used colloquially as meaning post-award surveillance of the contractor’s work.

Quality Assurance Evaluator (QAE): Individual assigned to perform quality assurance surveillance of products or services procured and to record and document the findings.

Quality Assurance Plan (QAP): A plan that, for a particular contract, includes a series of individual Surveillance Guides (SGs). The QAP also contains a copy of the performance requirements (PRS) for reference by the Quality Assurance Evaluator (QAE) together with inspection and report forms as appropriate.

Quality Assurance Surveillance Plan (QASP): A written document used by the Government for implementing the inspection and acceptance of Service Provider performance. The document contains specific methods to be used by the Government to evaluate satisfactory performance.

Quality Control: Those actions taken by the Service Provider to control the production of goods or services so that they meet the requirements of the contract.

Random Number Table: A table of numbers arranged in a random fashion.

Random Sample: A sample of services that has been selected according to rules that ensure that each member of the population has an equal chance of being selected.

Real Property: Land and the rights to land, fixtures, and buildings, including capitalized additions, alterations, improvements, and rehabilitation, and other structures and facilities. Real property does not include personal property (for example, weapons systems and other military equipment).

Receipt of E-Mail: The date and time that a message is posted to the e-mailbox.

Receiving Report: An acknowledgment by a Government representative that the supplies or services conform with applicable contract quantity and quality requirements. Receiving Reports are the Contracting Officer's responsibility or may be delegated to another official. A Receiving Report is completed and sent to the Finance and Accounting Office after the delivery of goods or services.

Record: All books, papers, maps, photographs, machine-readable items (such as disks, tapes, cards, printouts, aperture cards, roll microfilm, microfiche, laser disks, optical disks, optical cards, 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 Department of the Army as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities because of the informational value of the data.

Records Centers: Locations established in CONUS to receive and maintain records with long-term or permanent value, pending their ultimate destruction or accession into the National Archives and Records Administration.

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 medium. 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 implementation of responsibilities under the Freedom of Information Act and the Privacy Act.

Regional Business Center (RBC): The group formerly known as the Major Subordinate Command (MSC). Consists of the MSC office and USACE Districts.

Regional Management Board (RMB): A board with the goal of stimulating the development and execution of plans, using the resources to accomplish the goals and objectives of the RBC.

Relationship to BRM: Environmental Monitoring is a subfunction of the Environmental Management Line of Business.

Remote Terminal: A terminal that is not in the immediate vicinity of the Information System it accesses. This is usually associated with a mainframe environment. Terminals usually cannot operate in a stand-alone mode.

Replacement Cost: Obligations to be incurred at a future time to procure equipment or materiel in place of items that have been sold or transferred. There are two methods used to determine replacement cost: 1) Replacement cost may be determined by applying the Office of the Secretary of Defense prescribed inflation factor to the most recent contract price of the item to be replaced. The inflation factor is applied to each fiscal year between the year the item was sold, transferred, or acquired and the fiscal year in which the replacement item will be delivered. 2) Replacement cost may also be determined by obtaining a current contractor quote for the replacement item. Normally the second method is the most accurate.

Requirements Generation Process: The formal method of determining military operational deficiencies and the preferred set of solutions.

Return on Investment (ROI): A financial management approach used to explain how well a project delivers benefits in relationship to its cost. Several methods are commonly used to calculate a return on investment, including Economic Value Added (EVA), Internal Rate of Return (IRR), Net Present Value (NPV), Payback, and the use of nominal qualitative measures.

Reusability: The degree to which a software module or other work product can be used in more than one computing program or software system.

Rework: The performance of services that were found to be defective as a result of contract surveillance or other validated sources.

Risk: A term used to define the class of factors which (1) have a measurable probability of occurring during an investment's life cycle, (2) have an associated cost or effect on the investment's output or outcome (typically an adverse affect that jeopardizes the success of an investment), and (3) have alternatives from which the organization may choose.

Risk Assessment Code: An expression of the risk associated with a hazard that combines the hazard severity and accident probability into a single Arabic numeral.

Risk Decision: The decision to accept or not accept the risk(s) associated with an action; made by the commander, leader, or individual responsible for performing that action.

Risk Management: An approach for addressing the risks associated with an investment. Risk management includes identification, analysis, prioritization, and control of risks. Especially critical are those techniques that help define preventive measures to reduce the probability of these factors from occurring and identify countermeasures to successfully deal with these constraints if they develop.

Risk Management: The process of identifying, assessing, and controlling risk arising from operational factors and making decisions that balance risk cost with mission benefits.

Risk Management Integration: The embedding of Risk Management principles and practices into Army Operations, culture, organizations, systems, and individual behavior.

Safety: Freedom from those conditions that can cause injury, occupational illness, death, or damage to, or loss of, equipment or property.

Safety Assessment Report: A formal summary of the safety data collected during the design and development of the system. In it, the materiel developer summarizes the hazard potential of the item, provides a risk assessment, and recommends procedures or other corrective actions to reduce these hazards to an acceptable level.

Salvage: An item of personal property that has parts that are usable or can be recycled. The item as a whole is in such poor shape that its repair is not practical, but its total destruction is not warranted.

Sample: A sample consists of one or more work requirements drawn from a population. The number of work requirements selected for evaluation is the sample size.

Sample Size: The number of outputs in the sample; a group of one or more outputs drawn from the specified performance.

Schedule: A term used to define the time period corresponding to the life of the investment. The investment schedule typically contains associated phases and milestones that include planning, proposal generation, acquisition or development, implementation, operations and maintenance, and succession/retirement.

Scripting: A high-level programming language that is interpreted by another program at runtime rather than compiled by the computer's processor as other programming languages are. Scripting languages, which can be embedded within HTML, commonly are used to add functionality to a Web page, such as different menu styles or graphic displays or dynamic advertisements.

Selection Criteria: Factors that are identified for use by an investment review board to identify and discriminate investments for subsequent funding.

Sensitive Property: Those items that can be easily converted to private use or that have high potential for theft, regardless of cost (e.g., laptops, notebooks, and other portable computers, video cameras, televisions, external disk drives).

Server: A computer program that provides services to other computer programs in the same computer or other computers. The computer in which a server program runs is also frequently referred to as a "server."

Service Area: A technical tier that supports the secure construction, exchange, and delivery of business or service components. Each Service Area groups the requirements of component-based architectures within the Federal Government into functional areas.

Service Category. A sub-tier of the Service Area to classify lower levels of technologies, standards, and specifications in respect to the business or technology function they serve.

Service Component Reference Model Component. A Component is defined as "a self contained business process or service with predetermined functionality that may be exposed through a business or technology interface."

Service Component Reference Model (SRM). The Service Component Reference Model (SRM) is a business and performance-driven, functional framework that classifies Service Components with respect to how they support business and/or performance objectives.

Service Component Reference Model (SRM) Back Office Services. The Back Office Services Domain refers to the set of capabilities that support the management of enterprise planning transactional-based functions.

Service Component Reference Model (SRM) Business Analytical Services. The Business Analytical Services Domain defines the set of capabilities supporting the

extraction, aggregation and presentation of information to facilitate decision analysis and business evaluation.

Service Component Reference Model (SRM) Business Management Services. The Business Management Services Domain defines the set of capabilities that support the management of business functions and organizational activities that maintain continuity across the business and value-chain participants. The Business Management Services domain represents those capabilities and services that are necessary for projects, programs and planning within a business operation to successfully be managed.

Service Component Reference Model (SRM) Customer Services. The Customer Services Domain defines the set of capabilities that are directly related to an internal or external customer, the interaction of the business with the customer, and the customer-driven activities or functions. The Customer Services domain represents those capabilities and services that are at the front end of a business, and interface at varying levels with the customer.

Service Component Reference Model (SRM) Digital Asset Services. The Digital Asset Services Domain defines the set of capabilities that support the generation, management and distribution of intellectual capital and electronic media across the business and extended enterprise.

Service Component Reference Model (SRM) Process Automation Services. The Process Automation Services Domain defines the set of capabilities that support the automation of process and management activities that assist in effectively managing the business. The Process Automation Services domain represents those services and capabilities that serve to automate and facilitate the processes associated with tracking, monitoring, maintaining liaison throughout the business cycle of an organization.

Service Component Reference Model (SRM) Support Services. The Support Services Domain defines the set of cross-functional capabilities that can be leveraged independent of Service Domain objective and /or mission.

Service Contract: A contract that directly engages the time and effort of a contractor whose primary purpose is to perform an identifiable task rather than to furnish an end item of supply. A service contract may be either a non-persona or personal contract.

Service Level Agreement (SLA): 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.

Service Order: A customer order issued for work that does not define quantities or a scheduled completion date.

Service Provider: The commercial sector organization, its subsidiaries and affiliates, joint ventures involving the commercial entity, or any entity with which the commercial entity may have merged or any individual or entity that assisted or advised the

commercial entity in the preparation of a proposal under this solicitation. Includes Government employees if service is provided by public sector.

Service Request: A request for assistance to correct a problem usually associated with hardware.

Smart card: A credit-card-size device, normally to be carried and used by personnel, that contains one or more integrated circuit chips and may also employ one or more of the following technologies: 1) magnetic stripe; 2) barcodes, linear or two-dimensional; 3) non-contact radio frequency transmitters; 4) biometric information; 5) encryption and authentication; and 6) photo identification. It may be used to generate, store, or process data.

Software: A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system (for example, compiler, library routines, manuals, circuit diagrams); usually contrasted with hardware.

Spam: Widely disseminated “junk” e-mail.

Specification: A formal layout/blueprint/design of an application development model for developing distributed component-based architectures.

Stakeholder: An individual or group with an interest in the success of an organization in delivering intended results and maintaining the viability of the organization’s products and services. Stakeholders influence programs, products, and services.

Standard: Within the context of the Army Enterprise Architecture, a document that establishes uniform engineering and technical requirements for processes, procedures, practices, and methods. It may also establish requirements for the selection, application, and design criteria of materiel.

Standard: Hardware, software, or specifications that are widely used and accepted (de facto), or are sanctioned by a standards organization (de jure). Standards are typically categorized as follows:

- Programming Language Standards
- Character Code Standards
- Hardware Interface Standards
- Storage Media Standards
- Operating System Standards
- Communication and Networking Standards
- Machine Language Standards
- File System Management Standards
- Database Management System Standards
- Text Systems Standards
- Graphic Systems Standards
- Internet Standards

Standard Operating Procedures (SOP): A sequence of detailed procedures and guidance for performing a specific task or tasks.

Steady State: See Operational.

Still photography: The medium used to record still imagery; includes negative and positive images.

Strategic Metrics: A metric used at USACE level to monitor, control, and report strategic projects.

Strategic Plan: A document used by an organization to align its organization and budget structure with organizational priorities, missions, and objectives.

Strategic Planning: A continuous and systematic process whereby guiding members of an organization make decisions about its future, develop the necessary procedures and operations to achieve that future, and determine how success is to be measured.

Subscriber: Any person, group, organization (including concessionaire), or appropriated or non-appropriated fund activity that procures services made available pursuant to the terms of the franchise agreement.

Succession Management: An approach for determining when and how to replace current investments with other investments that provide greater benefits at lower costs.

Support Agreement: Formal agreement between a service provider and service receiver that typically includes such details as a description of the service to be provided, service availability, hours of delivery, response times, security requirements, continuity targets, responsibilities of all parties as well as critical business periods and exceptions such as holidays.

Surveillance: The process of monitoring contractor performance by direct evaluation, observation, or other information means.

Surveillance Guide (SG): A guide prepared for each contract requirement or group of contract requirements shown on the performance requirements summary (PRS). The SG's primary focus is on the service or the end result to be achieved by the contractor, rather than on the details of how the work is to be accomplished.

Synchronization: Coordination and alignment of the development of the Army Enterprise Architectures in both timing and direction for mutual reinforcement and support.

System: An organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. Within the context of the Army Enterprise Architecture, systems are people, machines, and methods organized to accomplish a set of specific functions; provide a capability or satisfy a stated need or objective; 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.

System Design Manager: The individual responsible for the functional design, development, implementation, and maintenance of an automatic data processing system supporting a business process or functional area.

Systems Architect: An individual responsible for integration and oversight of Army information systems.

Systems Architecture: Descriptions, including graphics, of systems and interconnections providing for or supporting functions.

System/Solution Architects/Developers: Responsible for building / assembling systems, and selecting technologies and standards that leverage existing assets and services across the Government and industry.

T-1 (T1): The most commonly used digital line in the U.S. T-1 carries 24 pulse code modulation signals using time-division multiplexing at an overall rate of 1.544 million bits per second.

Task: A discrete event or action, not specific to a single unit, weapon system, or individual, that enables a mission or function to be accomplished by individuals or organizations.

Technical Architecture (TA): A description of a technical system’s implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed.

Technical Reference Guide (TRG): Identifies and describes the standards pertaining to information technology and IT service delivery (e.g., databases, communications, security, software, hardware, Intranet, etc.) to be used throughout the Corps.

Technical Reference Model (TRM): Identifies and describes the information technology standards and IT service delivery used for a specific IT investment. The TRM is a subset of the Technical Reference Guide (TRG). There may be many TRMs associated with the TRG. Provides a foundation to describe the standards, specifications, and technologies to support the construction, delivery, and exchange of business and application components (Service Components) that may be used and leveraged in a Component-Based or Service-Orientated Architecture. The TRM unifies existing Agency TRMs and electronic Government (e-Gov) guidance by providing a foundation to advance the reuse of technology and component services from a Government-wide perspective.

TRM Component Framework: The Component Framework Area defines the underlying foundation and technical elements by which Service Components are built, integrated and deployed across Component-Based and Distributed Architectures. The Component Framework consists of the design of application or system software that incorporates interfaces for interacting with other programs and for future flexibility and expandability. This includes, but is not limited to, modules that are designed to interoperate with each other at runtime. Components can be large or small, written by different programmers using different development environments and may be platform independent. Components can be executed on stand-alone machines, a Local Area Network, Intranet or on the Internet.

TRM Service Access and Delivery Area: Refers to the collection standard and specifications to support external access, exchange, and delivery of Service Components or capabilities. This area also includes the Legislative and Regulator requirements governing the access and usage of the specific Service Component.

TRM Service Interface and Integration: The Service Interface and Integration Area defines the discovery, interaction and communication technologies joining disparate systems and information providers. Component-based architectures leverage and incorporate Service Interface and Integration specifications to provide interoperability and scalability.

TRM Service Platform and Infrastructure: The Service Platform and Infrastructure Area defines the collection of platforms, hardware and infrastructure specifications that enable Component-Based Architectures and Service Component reuse.

TRM Technologies: Refers to a specific implementation of a standard within the context of a given specification. The following describes for illustrative purpose the use of the term technologies as used in the TRM.

PL/SQL is an Oracle implementation of the SQL Standard.

ISQL/w is a Microsoft implementation of the SQL Standard.

ODBC is an implementation of a data access standard within various Microsoft specifications.

JDBC is an implementation of a data access standard within the Sun Microsoft specifications.

Telecommunications: Any transmission, emission, or reception of signs, signals, writings, images, and sounds or information of any nature by wire, radio, visual, or other electromagnetic systems.

Telework: Work at an alternative site.

Tenant: A unit or activity of one commander that occupies facilities on and receives specified types of supply and other support from an installation of another commander. On-post is synonymous with tenant.

Terminal: Any device that is used to access an Information System, including “dumb” terminals, which function only to access another IS, as well as personal computers or other sophisticated IS devices, which may access other ISs as one of their functions.

Test Agency: An organization that conducts development tests or user tests.

Third-Party Cookies: Cookies placed on a user’s hard drive by Internet advertising networks. The most common third-party cookies are placed by companies that serve the banner ads that appear across many Web sites.

Tier I: Mainframe systems, mainframe gateways, mainframe print queues, and any other mainframe operation that is not an end-user device.

Tier II: Minicomputer, Unix systems, servers, network hubs, network routers, and any other operation that is not an end-user device.

Tier III: End-user devices used to communicate with or within systems that are not Tier I or Tier II.

Twisted Pair: A type of cable in which pairs of conductors are twisted together to randomize possible cross talk from nearby wiring. Inadequate twisting is detectable using modern cable testing instruments.

Threshold: The limiting acceptable value of a measurement or technical parameter, typically a performance requirement.

Uninterruptible Power Supply (UPS): A device that allows a computer to keep running for a short time when the primary power source is lost. It also provides protection from power surges.

Uniform Resource Locator (URL): A Web address a person uses to direct a browser program to a particular Internet resource (for example, a file, a Web page application, and so on). All Web addresses have URLs.

USACE 2012: USACE 2012 is an enterprise-wide management study that prescribes the “*The Objective Organization*.” The year 2012 is the target date to fully transition to the *Objective Organization*. Transition began in FY03. For IM/IT purposes, USACE 2012 is often referred to as the Modernization Blueprint for making IT investment decisions. See *Target Work Environment* for more information.

Useful Segment: An economically and programmatically separate component of a capital project that provides a measurable performance outcome for which the benefits exceed the costs, even if no further funding is appropriated.

User Fee: The periodic service charge paid by a subscriber to a franchise for service.

User ID: Unique symbol or character string that is used by an Information System to uniquely identify a specific user.

User(s): Any person, organization, or unit that uses the services of an information processing system.

Validation: The process of determining whether or not the product delivered at the end of the development process satisfies predefined *requirements*.

Value: A term used to identify intangible benefits that may be easy to identify but that can be difficult to quantify. These benefits may include more efficient decision making, brand recognition, goodwill, valued partner, greater data accuracy, improved data security, reduced customer burden, or increased organizational knowledge.

Verification: The process of determining whether or not the products of a given phase of development fulfill the requirements established at the start *of the phase*.

Video: Pertaining to the bandwidth and spectrum position of the signal that results from television scanning and used to produce an electronic image.

Video Teleconferencing: Two-way electronic voice and video communication between two or more locations; may be fully interactive voice or two-way voice and one-way video; includes full motion video, compressed video, and sometimes freeze-frame (still) video.

Virtual Team: Team working across geographic or organizational boundaries without physical collocation.

Virus: Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no external signs of its presence.

Vision: A description of the future; the most abstract description of the desired end state of an organization or activity at an unspecified point in the future.

Visual Information (VI): Information in the form of visual or pictorial representations of person(s), place(s), or thing(s), either with or without sound. VI includes still photographs, digital still images, motion pictures, analog and digital video recordings, and hand- or computer-generated art and animations that depict real or imaginary person(s), place(s), and/or thing(s), and related captions, overlays, and intellectual control data.

Visual Information (VI) Activity: An organizational element or a function within an organization in which one or more individuals are classified as VI specialists, or whose principal responsibility is to provide VI services. VI activities include those that expose and process original photography; record, distribute, and broadcast electronically (video and audio); reproduce or acquire VI products; provide VI services; distribute or preserve VI products; prepare graphic artwork; fabricate VI aids, models, and displays; and provide presentation services or manage any of these activities.

Visual Information (VI) Documentation (VIDOC): Motion media, still photography, and audio recording of technical and nontechnical events, as they occur, usually not controlled by the recording crew.

Visual Information (VI) Equipment: Items capable of continuing or repetitive use by an individual or organization for recording, producing, reproducing, processing, broadcasting, editing, distributing, exhibiting, and storing visual information. Items otherwise identified as VI equipment that are integral parts of a non-VI system or device (existing or under development) will be managed as a part of that non-VI system or device.

Visual Information (VI) Functions: Individual VI processes, such as production, documentation, reproduction, distribution, records preservation, presentation services, VI aids, fabrication of models and displays, and related technical services.

Visual Information (VI) Library: A VI activity that loans, issues, and maintains an inventory of motion media, imagery, and/or equipment.

Visual Information (VI) Materials: All of the various VI still and motion films, tapes, discs, or graphic arts collectively. Includes the original, intermediate, and master copies and any other related recorded imagery.

Visual Information (VI) Production: The combination of motion media with sound in a self-contained, complete presentation, developed according to a plan or script for the purpose of conveying information to, or communicating with, an audience. A production is also the end item of the production process. Used collectively, VI production refers to the functions of procurement, production, or adoption from all sources, such as in-house or contract production, off-the-shelf purchase, or adoption from another Federal agency.

Visual Information (VI) Products: VI media elements such as motion picture and still photography (photographs, transparencies, slides, film strips), audio and video recordings (tapes or disks), graphic arts (including computer-generated products), models, and exhibits.

Visual Information (VI) Records: VI materials (regardless of format), related captions, and intellectual control data.

Visual Information (VI) Records Center: A facility, sometimes specially designed and constructed, for the low cost and efficient storage and referencing of semi-current records pending their ultimate disposition.

Visual Information (VI) Report: VI documentation assembled to report on a particular subject or event.

Visual Information (VI) Resources: The personnel, facilities, equipment, products, budgets, and supplies making up DoD visual information support.

Visual Information (VI) Services: Those actions that 1) result in a visual information product; 2) support the preparation of a completed VI production, such as photographing, processing, duplicating, sound and video recording, instrumentation recording, film-to-video transferring, editing, scripting, designing, and preparing graphic arts; 3) support existing VI products such as distribution and records center operations; and 4) use existing VI products, equipment, maintenance, and activities to support other functions such as projection services operation of conference facilities, or other presentation systems.

Vital Records: Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the rights and interests of that organization and of the individuals directly affected by its activities. These include both emergency operating and rights-and-interests records. Vital records are a part of an agency's records disaster prevention and recovery program.

Web Portals: Web sites that serve as starting points to other destinations or activities on the Web. Initially thought of as a "home base" type of Web page, portals attempt to provide all of a user's Internet needs in one location. Portals commonly provide services such as e-mail, collaboration centers, online chat forums, searching, content, news-feeds, and others.

Web Site: A location on the Internet; specifically, the point of location in which it resides. All Web sites are referenced using an addressing scheme called a URL. A Web site can mean a single HTML file or hundreds of files placed on the Internet by an enterprise.

Work Order: Individual task/line item associated with a contract for efficient response to a particular requirement.

Work Station: A PC terminal setup in or on a network and connected to a domain or mainframe computer.

Workload: Everything that is done by the organization utilizing in-house or contractual resources. Workload involves anything for which the organization incurs costs (accrued expenditures) for a given fiscal year for both direct and reimbursable customers.

World Wide Web (WWW): A part of the Internet designed to allow easier navigation of the network through the use of graphical user interfaces and hypertext links between different addresses. It is also called the Web.

Worm: Independent program that reproduces by copying itself from one system to another, usually over a network. Like a virus, a worm may damage data directly, or it may degrade system performance by consuming system resources and even shutting down a network.

U.2 Corps of Engineers Enterprise Infrastructure Services (CEEIS) Glossary



Updated: 16 June 2003 1/7

TERMS AND ACRONYMS

ACERT

Army Computer Emergency Response Team: Army's top-level security team. All other subordinate CERTS (RCERT, FCERT etc.) report to them. Located at Ft. Belvoir.

ACL

Access Control List: Used in various CEEIS routers to filter traffic in/out.

AD-SCCB

Active Directory Schema Configuration Control Board: It is used to control enterprise level active directory configurations and reports to the CEEIS CCB. Sam Bradley, CEEIS Configuration Program Manager, chairs this board.

AEI-TRWG

Army Enterprise Infostructure - Transport Reengineering Working group. Army initiative to create integrated Army network. CEEIS staff participates in this design effort.

AIS

Automated Information Systems: Used to refer to any application that is used. Typically used to refer to larger applications like CEFMS, P2, etc.

AKM

Army Knowledge Management: Name used to describe multiple goals within Army to streamline Information Technology and provide information to all Army staff easily.

AKO

Army Knowledge Online: Refers to the Web site/portal www.us.army.mil.

Alias

Also known as redirecting: The practice of using a fictitious address for your outgoing and incoming e-mail.

ANOSC

Army Network Operation Security Center: Army's top-level center that monitors Army-wide network and security infrastructure. Located at Ft. Belvoir.

ASR

Army Security Router: Army-managed devices that connect to NIPRNET circuits.

Autoresponders

Also known as mailbots: Automated programs that return a canned message upon receipt of e-mail.

BCP

Business Contingency Planning: Planning associated with continuing business process in the event of catastrophic failures.

BGP

Border Gateway Protocol: Routing protocol used for external connections.

Bounced Message

One that is returned to the sender because it is undeliverable.

CAC

DoD Common Access Card: This is the card that will replace all DoD ID cards.

CBT

Computer Based Training: Training based around use of PC. Also used to refer to Army CBT program.

CCB

CEEIS Configuration Control Board (Board that reviews changes to CEEIS baseline configuration).

CEEIS

Corps of Engineers Enterprise Infrastructure Services: Name of entity that operates USACE infrastructure to FOA level including processing center, e-mail, network and security.

CEEIS NetAB

CEEIS Network Advisory Board: A board reporting to CEEIS PM for networking issues. Currently Chaired by Greg Bigelow.

CEEIS SecAB

CEEIS Security Advisory Board: A board reporting to CEEIS PM for security issues. Currently chaired by Greg Bigelow.

CEEIS SysAB

CEEIS Systems Advisory Board: A board reporting to CEEIS PM for systems and e-mail issues. Currently chaired by Sanda Smith.

CEFMS

Corps of Engineers Financial Management System: USACE financial processing system.

CERP

Comprehensive Environmental Restoration Program: Program run by South Florida Water Management District and SAJ. CEEIS provides COOP for the CERP program.

CERT

Computer Emergency Response Team- Teams that handle security incidents.

CIO

Chief Information Officer (For USACE this is Wil Berrios).

CIR

Confirmed Information Rate: Used to provision frame relay services. Defines the guaranteed bandwidth over a frame service.

CNSS

CEEIS Network/Security Stack: This is used to refer to the standardized rack of equipment that is being deployed to site. This rack creates a standard CEEIS point of presence for all CEEIS connected sites. This was previously referred to as the ROF.

CON

Certificate of Networkiness (Approval provided by CIO/G6 for applications to run on Army networks): Certification that the AIS complies with Army Enterprise Architecture (AEA) system support requirements. A CON is required prior to the issuance of a CTO.

COOP

Continuity of Operations Plan: Same as a BCP. Used to define what to do in case of various outage scenarios including catastrophic events.

COTS

Commercial Off-The-Shelf: Software bought in shrink-wrap and used as is or modified slightly.

CPC

Central Processing Center: CEEIS processing center located at U.S. Army Engineer Research and Development Center (ERDC), Information Technology Laboratory (ITL), in Vicksburg, MS.

CPOC

Centralized Personnel Operation Center: Where personal processing is done. Sometime used to refer to location of staff and sometimes used to refer to location of computer. In near future, all CPOC computers will be centralized to Rock Island.

CRD

Compliance Reporting Database: Used to report IAVA compliances by site and system.

C-TNOSC

CONUS Theater Network Operations Security Center: This is the NOSC located at Fort Huachuca, AZ, that manages CONUS Army NIPRNET connections.

CTO

Certificate to Operate: Provided by NETCOM for applications to run on Army networks. Certification that the AISs comply with security, operational, technical, and system support requirements from a central location view. A CTO is required for an AIS to operate on the Army Enterprise Infostructure.

DDOS

Distributed Denial of Service: Attacks launched by having large numbers of systems participate.

DISA

Defense Information Security Agency

DISN

Defense Information Systems Network: DoD-wide network for voice and data.

DITSCAP

DoD Information Technology Security Certification and Accreditation Process: A process for ensuring security of DoD systems.

DMS

Defense Message System: A DoD e-mail messaging system.

DNS

Domain Name Service: IP service used to associate IP address with a name or name with an IP address.

DOS

Denial of Service: An attack intended to prevent site access.

DSAWG

Defense Information Systems Network Security Accreditation Working Group.

DSCO

Document/Suspense Control Officer: For the CEEIS Program Management Office it is Tracey Pruitt.

DSL

Digital Subscriber Line: Passing of high-speed data traffic over a standard phone line.

ECP

Engineering Change Proposal: Used to request, document, and evaluate changes to infrastructure. Note: All CEEIS ECPs should be routed to Tracey Pruitt for logging and processing.

E-mail Thread

A series of e-mail messages or newsgroups postings all related to the same topic or thread.

EROC

Engineer Reporting Organization Codes

FAR

Firewall Action Request: Used by sites to request changes in CEEIS managed firewalls.

FCERT

Functional Computer Emergency Response Team: A security analysis entity managed by one of the Functional regions (USACE, ARNG, USAR, etc.).

FEM

Facilities Equipment Maintenance: Maintenance management system run at the center.

F-NOSC

Functional Network Operations Security Center: A network/security monitoring entity managed by one of the Functional regions (USACE, ARNG, USAR, etc.).

FTP

File Transfer Protocol: A common method of moving files between two Internet sites. FTP is a special way to login to another Internet site for the purposes of retrieving and/or sending files.

FCIO

Functional Chief Information Officer: An Army term used to refer to entities that NETCOM provides technical control to but does not operate. Dr Wright is the FCIO for the USACE functional region. Mr. Greg Bigelow is the Deputy FCIO for the USACE functional region. Other entities that have FCIOS are MEDCOM, ARNG, USAR and CFSC (Classroom facilities).

Fuzzy Addressing/Approximate Naming

Mail-hub uses this to compare e-mail addresses to the X500 directory. If the e-mail address is close enough to match a valid e-mail address, Mail-hub rewrites the e-mail address to the correct exact e-mail address.

GAL

Global Address List: Corps-wide listing of addresses in Exchange.

GAO

Government Accountability Office

GIG

Global Information Grid: used to refer to the entire DISA network including voice, data and processing.

Headers

The part of an e-mail message that describes the sender, the addressee and other recipients, message priority level, and so forth. It's at the top, or head, of a message.

IAVA

Information Assurance Vulnerability Alert: Alerts sent out informing site of security vulnerabilities and incidents.

IDS

Intrusion Detection System: Deployed on networks through the Corps, monitored by CEEIS NOSC.

IMAP

Internet Message Access Protocol: A method of accessing electronic mail or bulletin board messages that are kept on a mail server, possibly shared.

ISS Scanner

Information Security System Scanner: Tool used by NOSC to perform vulnerability assessments (scans).

ITL

Information Technology Laboratory: ERDC laboratory that hosts the CEEIS Program Management Office and the Central Processing Center (CPC).

LDAP

Lightweight Directory Access Protocol: An open-standard protocol for accessing information services. For e-mail, LDAP is used to store e-mail alias to e-mail address translations.

List Server

A program that automatically redistributes e-mail to names on a mailing list. The two most common list servers are listserv and Majordomo. People sharing an interest may "subscribe" to a given discussion, and other subscribers' contributions to the thread are distributed to the entire subscriber base via e-mail. The result is similar to a newsgroup, except that the messages are transmitted as e-mail and are therefore available only to individuals on the list.

MACOM

Major Command

Mailer Daemon

A Unix program used in the management of e-mail messages. Not generally encountered by a user unless the user gets a bounced message.

Mailing List Manager

An automated program that handles the administrative functions of adding/removing subscribers, disseminating the message postings, sending topic-related and help files for the entire Mailing List.

Mailing List

A collection of e-mail addresses of people who have asked to receive regular mail discussions on a particular topic, and for which they can sometimes submit messages for disbursement to the entire group.

Majordomo

E-mail addressed to a Majordomo mailing list is automatically broadcast to everyone on the list. Unlike postings to a newsgroup or forum, which can be viewed by anyone, submissions to a majordomo list are accessible only to those on the mailing list. Majordomo is written in PERL and can be run on any operating system platform with a PERL interpreter.

MIME

Multipurpose Internet Mail Extension: A standard system for identifying the type of data contained in a file based on its extension. MIME is an Internet protocol that allows you to send non-ASCII/textual data, such as graphics, photos, sound and video files, and formatted text documents, across the Internet as attachments to e-mail messages.

NDR

Non-Delivery Report: Your mail server determines that a message cannot be delivered and sends an NDR e-mail message back to the sender of the original message.

NETCOM

Network Enterprise Technology Command: Entity that provides operational control (OPCON) to RCIO-managed entities including Army post/camps/stations and provides technical control (TECHCON) to FCIO-managed entities.

NIAP

National Information Assurance Partnership: A Government-wide testing, evaluation, and assessment of security products. List of products that have passed these tests are available at <http://niap.nist.gov/cc-scheme/ValidatedProducts.html>

NIST

National Institute for Standards and Technology

NIPRNET

Non-Secure Internet Protocol Router Network

NOSC

Network Operations Security Center: Entity that tracks networking and security for USACE. This is located at Portland and Vicksburg.

OSPF

Open Shortest Path First: Routing protocols used in backbone.

OWA

Outlook Web Access: Used to refer to accessing Outlook e-mail using a Web browser.

P2

Promis-2: Next-generation project management AIS.

P3e

Primera P3e: A Network Analysis System (NAS) used in project management. Being combined with ORACLE products to make up "P2". Often used to refer to the "fat-client" for P2.

PKI

Public Key Infrastructure

PMO

Program Management Office: Used to refer to the CEEIS Program Manager (PM) office/staff as a whole.

POP

Post Office Protocol: POP is the Internet standard for e-mail and the protocol used for receiving e-mail from another Internet user.

Primavision

The Web interface to the Primavera software. Most customers will access P2 using this interface and their Web browser.

PVC

Permanent Virtual Circuit: Software defined connection in frame relay.

QOS

Quality of Service: Function provided by Sitara units to allocate bandwidth among applications and provide defined levels of service.

Queue

A monitoring count used to measure the performance and delivery of incoming or outgoing e-mails to sites.

RAS

Remote Access Services: Feature in Windows that enables users to log into a Windows-based network using a modem.

RASP

Remote Access Security Program

RCERT

Regional Computer Emergency Response Team: A CERT that is responsible for a particular Army region.

RCIO

Regional Chief Information Officer: Army NETCOM term used to refer to the NETCOM RCIOs that have geographic responsibilities. These include NW, NE, SW, SE, EUR, ROK and PAC.

RDP

Robert Duncan Plaza: Building that WPC is in.

RMS

Resident Engineer Management System: AIS to support resident managers in construction offices.

ROF

See CNSS.

SAN

Storage Area Network: A pool of drive space shared among multiple servers. CEEIS operates a SUN-based SAN, which provides high availability storage capability.

SBU

Sensitive-but-Unclassified: All systems connected to the CEEIS network are SBU for their classification.

SCADA

Supervisory Control and Data Acquisition: Systems that are used for process control (typically for locks and dams) and management.

SIPRNET

Secret Internet Protocol Router Network: Separate network used to pass classified traffic Secret and above.

SMTP

Simple Mail Transfer Protocol: IP protocol used to exchange e-mail. In USACE this protocol is used to get and send external e-mail.

SNMP

Simple Network Management Protocol: Used to get information from network devices.

Spam

Junk e-mail sent to many people at once. It is unsolicited, usually comes from a source you are unfamiliar with, and generally is for commercial purposes.

SPS

Standardized Procurement System: System run at the processing centers in support of contracting and procurement activities.

STAT

Tool provided by Army to scan sites. Vendor of software is HARRIS.

TLA

Top Level Architecture: Army design for security configurations.

TNOSC

Theater Network Operations Security Center: Army term for a network center that operates a theatre network.

U-PASS

User-id Password Administration and Security System: User-id and password management system for access to USACE systems. System is managed by CEEIS.

Virus Hoax

A false warning about a computer virus. Two common popular hoaxes are Good Times and Join the Crew. Innocent users believing they are helping the community by playing “Paul Revere” forward these and other warnings via e-mail.

Virus

A program or piece of code -- generally destructive -- that loads onto your computer without your knowledge and runs against your wishes. It can damage the files on your computer and then automatically spread to other computer users.

VOIP

Voice over Internet Protocol (IP): using an IP network to pass voice call information.

VPN

Virtual Private Network: the creation of encrypted tunnels through a network. For USACE, VPNs are used to allow external systems to connect inside the Corps.

Worm

Not technically a virus, but more of a code that can replicate itself and use memory, but cannot attach itself to other programs. Usually spreads via e-mail or IRC (Internet Relay Chat).

WPC

Western Processing Center, located in the Robert Duncan Plaza in Portland, OR.

To incorporate additions, contact Tracey Pruitt, CEEIS Document/Suspense Control Officer, at (601) 634-4633 or <mailto:tracey.i.pruitt@usace.army.mil>.

U.3 Glossary Definition Sources:

1. United States General Accounting Office (GAO) Accounting and Information Management Division, May 2000, Version 1, Information Technology Investment Management - A Framework for Assessing and Improving Process Maturity - Exposure Draft, GAO/AIMD-10.1.23, Available, <http://www.cio.gov/documents/ai10123.pdf>

2. THE BUSINESS REFERENCE MODEL, VERSION 1.0 - A Foundation for Government-wide Improvement, July 2002, Available:
http://www.cio.gov/documents/fea_brm_release_document_rev_1.pdf
3. H. R. 2458, E-Government Act of 2002, Available,
http://www.cio.gov/documents/e_gov_act_2002.pdf
4. Information Technology Management Reform Act of 1996, Available:
http://www.cio.gov/documents/it_management_reform_act_feb_1996.html
5. OMB Circular No. A-11 (2003) Section 53, Available:

U.4 Related GAO Documents

Information Security Risk Assessment: Practices of Leading Organizations (GAO/AIMD-00-33, November 1, 1999).

Executive Guide: Creating Value Through World-class Financial Management (GAO/AIMD-99-45, Exposure Draft, August 1999).

Executive Guide: Leading Practices in Capital Decision-Making (GAO/AIMD-99-32, December 1998).

Executive Guide: Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, April 1998).

The Results Act: An Evaluator's Guide to Assessing Agency Annual Performance Plans (GAO/GGD-10.1.20, Version 1, April 1998).

Executive Guide: Measuring Performance and Demonstrating Results of Information Technology Investments (GAO/AIMD-98-89, March 1998).

Agencies' Annual Performance Plans Under the Results Act: An Assessment Guide to Facilitate Congressional Decision Making (GAO/GGD/AIMD-10.1.18, Version 1, February 1998).

Business Process Reengineering Assessment Guide (GAO/AIMD 10.1.15, Version 3, May 1997).

Agencies' Strategic Plans Under GPRA: Key Questions to Facilitate Congressional Review (GAO/GGD-10.1.16, Version 1, May 1997).

Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making (GAO/AIMD-10.1.13, Version 1, February 1997).

Executive Guide: Effectively Implementing the Government Performance and Results Act (GAO/GGD-96-118, June 1996).

Strategic Information Management (SIM) Self-Assessment Toolkit (Exposure Draft, Version 1.0, October 28, 1994).

Executive Guide: Improving Mission Performance Through Strategic Information Management and Technology (GAO/AIMD-94-115, May 1994).

U.5 Additional Resources

U.5.1 Professional Organizations

Association for Federal Information Resources Management: www.affirm.org

Chief Financial Officers Council: www.financenet.gov

Federal Chief Information Officers Council: www.cio.gov

Government Information Technology Services Board: www.gits.gov

Industry Advisory Council: www.iaconline.org

Information Systems Audit and Control Association and Foundation: www.iasca.org

Information Technology Association of America: www.ita.org

Information Technology Resources Board: www.itrb.gov

International Federation of Accountants: www.ifac.org

National Association of State Information Resource Executives: www.nasire.org

Society for Information Management: www.simnet.org

U.5.2 Publications

Beyond Computing: www.beyondcomputingmag.com

CIO Magazine: www.cio.com

Federal Computer Week: www.fcw.com

Government Computer News: www.gcn.com

Government Executive: www.govexec.com

InformationWeek: www.informationweek.com

International Data Group: www.idg.com

Sloan Management Review: www.mitsloan.mit.edu/smr/index.html

GAO-01-376G CIO Executive Guide Page 61

U.5.3 Research Organizations

Forrester Research, Inc.: www.forrester.com

Foundation for Performance Measurement: www.fpm.com

Gartner Group: www.gartner.com

GIGA Information Group: www.gigaweb.com

International Data Corporation: www.idc.com

IT Governance Institute: www.itgovernance.org/itgi

META Group Inc.: www.metagroup.com

Yankee Group: www.yankeegroup.com

U.5.4 Federal Resources

Federal Acquisition Regulation: www.ARNet.gov/far/

Critical Infrastructure Assurance Office: www.caio.gov

Federal Computer Incident Response Capability: www.fedcirc.gov

Federal Information Processing Standards: www.itl.nist.gov

General Accounting Office: <http://www.gao.gov/>

GSA's Policyworks: www.policyworks.gov

IT Policy On-Ramp: www.itpolicy.gsa.gov

National Partnership for Reinventing Government: www.npr.gov

Office of Management and Budget Homepage: www.whitehouse.gov/omb

U.5.5 Selected Books and Articles

Boar, Bernard H., Practical Steps for Aligning Information Technology with Business Strategies: How to Achieve a Competitive Advantage (John Wiley & Sons, Inc., New York, New York, 1994).

Boar, Bernard H., Strategic Thinking for Information Technology (John Wiley & Sons, Inc., New York, New York, 1996).

Bryson, John M., *Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement* (Jossey-Bass Publishers, San Francisco, California, 1991).

Camp, Robert C., *Benchmarking: The Search for Industry Best Practices That Lead to Superior Performance* (ASQC Quality Press, New York, New York, 1989).

Cortada, James W., *Best Practices in Information Technology* (Prentice Hall PTR, Upper Saddle River, New Jersey, 1998).

Earl, Michael J., and Feeny, David F., *Does the CIO Add Value?* *Informationweek*, May 30, 1994.

Ferris, Nancy, *CIOs on the Go*, *Government Executive*, March 1999.

Government Executive Magazine/Price Waterhouse, The Manager's Edge (National Journal Group, Washington, D.C., 1998).

Hubbard, Douglas, *The IT Measurement Inversion*, *CIO Enterprise*, April 15, 1999.

Mayor, Tracy, *Making a Federal Case of IT*, *CIO Magazine*, July 1, 1999.

Morin, Therese; Devansky, Ken; Little, Gard; and Petrun, Craig, *Information Leadership: A Guide for Government Executives* (PricewaterhouseCoopers, LLP, 1999).

Stephens, Charlotte S., *The Nature of Information Technology Managerial Work: The Work Life of Five Chief Information Officers* (Quorum Books, Westport, Connecticut, 1995).

Stuart, Anne, *The CIO Role: The New IS Role Models*, *CIO Magazine*, May 15, 1995.

Tapscott, Don and Caston, Art, *Paradigm Shift – The New Promise of Information Technology* (McGraw-Hill, Inc., New York, New York, 1993).

GAO-01-376G *CIO Executive Guide* Page 63

Wakin, Dr. Edward, *The Multifaceted CIO*, *Beyond Computing*, May 1995.

Wang, Charles B., *Techno Vision II: Every Executive's Guide to Understanding and Mastering Technology and the Internet* (McGraw-Hill, Inc., New York, New York, 1997).

Weill, Peter, and Broadbent, Marianne, *Leveraging the New Infrastructure: How Market Leaders Capitalize on Information Technology* (Harvard Business School Press, Boston, Massachusetts, 1998).

Woldring, Roelf, *Choosing the Right CIO*, *Business Quarterly*, Spring 1996.

Wreden, Nick, Executive Forum: Proving the Value of Technology, Beyond Computing, July/August 1998.

Page 64 GAO-01-376G CIO Executive Guide

U.5.6 Selected Information Management Reports and Guidance

An Analytical Framework for Capital Planning and Investment Control for Information Technology, U.S. General Services Administration, Office of Policy, Planning and Evaluation, Office of Information Technology, May 1996.

Best IT Practices in the Federal Government, CIO Council and IAC, October 1997.

Capital Programming Guide, Version 1.0, Supplement to Office of Management and Budget Circular A-11, Part 3: Planning, Budgeting, and Acquisition of Capital Assets, July 1997.

Evaluating Information Technology Investments: A Practical Guide, Version 1.0, Office of Information and Regulatory Affairs, Information Policy and Technology Branch, Office of Management and Budget, November 1, 1995.

Federal Enterprise Architecture Framework, Version 1.1, Federal CIO Council, September 1999.

Federal Information Technology, Executive Order on ITMRA, The White House, July 17, 1996.

Federal IRM Training Roadmap: A Guide for Federal CIOs, (Draft), Federal CIO Council, Education and Training Committee, January 1999.

Funding Information Systems Investments, M-97-02, Office of Management and Budget, October 25, 1996.

IAC / CIO Task Force Draft Report, Industry Advisory Council, July 9, 1996.

Implementing Best Practices: Strategies at Work, Federal CIO Council, Capital Planning and IT Investment Committee, June 1998.

Implementing Capital Planning and Information Technology Investment Processes: An Assessment, Federal CIO Council, Capital Planning and IT Investment Committee, Best Practices Subcommittee, May 29, 1998.

Major System Acquisitions, Circular No. A-109, Office of Management and Budget, April 5, 1976.

Management of Federal Information Resources, Circular No. A-130, Revised, Office of Management and Budget, February 8, 1996.

Meeting the Federal IT Workforce Challenge, Federal CIO Council, Education and Training Committee, June 1999.

Preparation and Submission of Budget Estimates, Circular No. A-11, Revised, Office of Management and Budget, June 23, 1997.

GAO-01-376G CIO Executive Guide Page 65

ROI and the Value Puzzle, Federal CIO Council, Capital Planning and IT Investment Committee, April 1999.

Strategic Plan, Federal CIO Council, Fiscal Year 2000.

The Federal Chief Information Officer: Fourth Annual Top Ten Challenges Survey, Association for Federal Information Resources Management, December 1999.

The Impact of Change: Clinger-Cohen Act Implementation, Laying the Foundation for Year 2000 and Beyond, Eighth Annual ITAA Survey of Federal CIOs, December 1997.

Meeting the Federal IT Workforce Challenge, Federal CIO Council, Education and Training Committee, June 1999.

Preparation and Submission of Budget Estimates, Circular No. A-11, Revised, Office of Management and Budget, June 23, 1997.

GAO-01-376G CIO Executive Guide Page 65

ROI and the Value Puzzle, Federal CIO Council, Capital Planning and IT Investment Committee, April 1999.

Strategic Plan, Federal CIO Council, Fiscal Year 2000.

The Federal Chief Information Officer: Fourth Annual Top Ten Challenges Survey, Association for Federal Information Resources Management, December 1999.

The Impact of Change: Clinger-Cohen Act Implementation, Laying the Foundation for Year 2000 and Beyond, Eighth Annual ITAA Survey of Federal CIOs, December 1997.