Memoranda 97-16 (Information Technology Architectures)

June 18, 1997

M-97-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Franklin D. Raines
              Director

SUBJECT: Information Technology Architectures

This memorandum transmits guidance to Federal agencies on the development and implementation of Information Technology Architectures. The Information Technology Architecture (ITA) describes the relationships among the work the agency does, the information the agency uses, and the information technology that the agency needs. It includes standards that guide the design of new systems. An ITA makes it easier to share information internally (e.g., agency-wide e-mail) and to reduce the number of information systems that perform similar functions. The ITA provides the technology vision to guide resource decisions that reduce costs and improve mission performance.

OMB Memorandum 97-02, "Funding Information Systems Investments," (October 25, 1996), requires that agency investments in major information systems should be consistent with Federal, agency, and bureau ITAs. The Clinger-Cohen Act of 1996 (Public Law 104-106) assigns the Chief Information Officer the responsibility of developing, maintaining, and facilitating the implementation of the information technology architecture.

As described in the attachment, a complete ITA is the documentation of the relationships among business and management processes and information technology that ensure:

- alignment of the requirements for agency-sponsored information systems (as defined in OMB Circular A-130) with the processes that support the agency's missions and goals;
- adequate interoperability, redundancy, and security of information systems; and,
- the application and maintenance of a collection of standards by which the agency evaluates and acquires new systems.

Agencies should be prepared to indicate the status of the development, implementation, and maintenance of the agency ITA during the formulation of the FY 1999 President's budget.

Attachment

Development, Maintenance, and Implementation of
Agency Information Technology Architectures

Table of Contents

Purpose

The purpose of this paper is to establish minimum criteria for an agency information technology architecture (ITA) required in the Clinger-Cohen Act of 1996 (Public Law 104-106).

Background

The Clinger-Cohen Act assigns the Chief Information Officers (CIO) the responsibility of "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture." (Section 5125 (b) (2)) The Act defines the ITA as:

an *integrated framework* for evolving or maintaining existing information technology and acquiring new information technology *to achieve the agency's strategic goals* and information resources management goals. (Section 5125 (d)) (Emphasis added.)

OMB's memorandum 97-02, "Funding Information Systems Investments," dated October 25. 1996, states,

Investments in major information systems proposed for funding in the President's budget should be consistent with Federal, agency, and bureau information architectures which: integrate agency work processes and information flows with technology to achieve the agency's strategic goals; and specify standards that enable information exchange and resource sharing.

These references highlight three important characteristics of the ITA as agencies plan for investments in information technology (IT) assets:

- CIOs are responsible for the architecture;
- the architecture must integrate the business processes and goals of the agency with IT acquisitions; and,
- the architecture focuses on work processes, information flows, and standards.

Agencies may address the topics and elements set out herein in a manner appropriate to the agency. Each element identified need not have specific or "stand-alone" documentation.

Information Technology Architecture Defined

For the purpose of conforming to the requirements of Clinger-Cohen Act, a complete ITA is the documentation of the relationships among business and management processes and information technology that ensure:

- alignment of the requirements for information systems (as defined in OMB Circular A-130) with the processes that support the agency's missions;
- adequate interoperability, redundancy, and security of information systems; and,

- the application and maintenance of a collection of standards (including technical standards) by which the agency evaluates and acquires new systems.

Developing the ITA

The ITA is broad in scope and includes processes and products. An architecture in compliance with the Clinger-Cohen Act and OMB guidance will contain two elements:

- the Enterprise Architecture,
- a Technical Reference Model and Standards Profiles.

In developing their ITAs, agencies are *not* required to use the terminology contained in this guidance. Examples of various agency architectures may be found in Appendix I.

A variety of nomenclatures are available to address these elements. Agencies may address the elements of an ITA in different ways and at various levels of granularity as appropriate, combining or reorganizing the parts to create a model that suits the agency's organizational needs. Various aspects of the ITA can be developed at the agency or sub-agency level. However, self-contained sub-agency level architectures should be integrated and consistent with an agency-wide ITA.

The Enterprise Architecture

The Enterprise Architecture is the explicit description of the current and desired relationships among business and management process and information technology. It describes the "target" situation which the agency wishes to create and maintain by managing its IT portfolio.

The documentation of the Enterprise Architecture should include a discussion of principles and goals.[1] For example, the agency's overall management environment, including the balance between centralization and decentralization and the pace of change within the agency, should be clearly understood when developing the Enterprise Architecture. Within that environment, principles and goals set direction on such issues as the promotion of interoperability, open systems, public access, end-user satisfaction, and security.

This guidance adapts a five component model used in the National Institute of Standards and Technology (NIST) Special Publication 500-167, "Information Management Directions: The Integration Challenge." Agencies are permitted to identify different components as appropriate and to specify the organizational level at which specific aspects of the components will be implemented. Although the substance of these components, sometimes called "architectures" or "sub-architectures,"[2] must be addressed in every agency's complete Enterprise Architecture, agencies have great flexibility in describing, combining, and renaming the components, which consist of:

- Business Processes
- Information Flows and Relationships
- Applications
- Data Descriptions
- Technology Infrastructure

With the exception of the Business Processes component, the interrelationships among and priorities of these components are not prescribed by this guidance; there is no hierarchy of relationships implied. Furthermore, agencies should document not only their current environment for each of these components, but also the target environment that is desired.

Business Processes

This component of the Enterprise Architecture describes the core business processes which support the organization's missions. The Business Processes component is a high-level analysis of the work the agency performs to support the organizations's mission, vision, and goals, and is the foundation of the ITA. Analysis of the business processes determine the information needed and processed by the agency. This aspect of the ITA must be developed by senior program managers in conjunction with IT managers. Without a thorough understanding of its business processes and their relation to the agency missions, the agency will not be able to use its ITA effectively.

Business processes can be described by decomposing the processes into derivative business activities. There are a number of methodologies and related tools available to help agencies decompose processes. Irrespective of the tool used, the model should remain at a high enough level to allow a broad agency focus, yet sufficiently detailed to be useful in decision-making as the agency identifies its information needs. Agencies should avoid excessive emphasis on modeling business processes, which can result in a waste of agency resources.[3]

Information Flows and Relationships

This component analyzes the information utilized by the organization in its business processes, identifying the information used and the movement of the information within the agency. The relationships among the various flows of information are described in this component. These information flows indicate where the information is needed and how the information is shared to support mission functions.[4]

Applications

The Applications component identifies, defines, and organizes the activities that capture, manipulate, and manage the business information to support *mission* operations. It also describes the logical dependencies and relationships among business activities.[5]

Data Descriptions and Relationships

This component of the Enterprise Architecture identifies how data is maintained, accessed, and used. At a high level, agencies define the data and and describe the relationships among data elements used in the agency's information systems. The Data Descriptions and Relationships component can include data models that describe the data underlying the business and information needs of the agency. Clearly representing the data and data relationships is important for identifying data that can be shared corporately, for minimizing redundancy, and for supporting new applications.[6]

Technology Infrastructure

The Technology Infrastructure component describes and identifies the physical layer including, the functional characteristics, capabilities, and interconnections of the hardware, software, and communications, including networks, protocols, and nodes. It is the "wiring diagram" of the physical IT infrastructure.[7]

Technical Reference Model and Standards Profiles

The Technical Reference Model (TRM) and Standards Profiles (both technical and security) comprise a cross-cutting element, affecting all components of the Enterprise Architecture. Standards enable interoperability, portability, and scaleability in systems throughout the agency. Although the specificity of the standards may vary by organizational level, the standards must be consistent throughout the agency. Standards are the basis of the development of components of the Enterprise Architecture and ultimately guide and constrain IT asset acquisitions.

Technical Reference Model

The TRM identifies and describes the information services (such as database, communications, and security services) used throughout the agency. For example, Data Interchange Services support the exchange of data and information between applications. This information service would identify the various ways the agency enables the exchange of data, such as plain text, spreadsheets, databases, graphical information over Intranet/Internet, and video.

Standards Profiles

The standards profile defines a set of IT standards that supports the services articulated in the TRM; they are the cornerstone of interoperablity. The profile establishes the minimum criteria needed to

specify technology that achieves the purposes of standardization and supports specific business functions. Standards Profiles are the published sets of standards or the source references for standards that prescribe the interfaces between those services that will be standards-based. A profile may contain specifications that describes the technical standards which enable a service, such as operating systems, network, and data interchange services.

Together with the TRM, the Standards Profiles enable the development and acquisition of standardized systems to cost-effectively meet the business needs of the agency. Agencies are expected to adopt the minimum standards necessary to support all components of the desired Enterprise Architecture. The profiles should address hardware, software, communications, data management, user interfaces, and implementation approaches, and may indicate specific products that implement the standard.[8]

Security Standards Profiles

While security services may be considered part of the TRM and security profiles may be a subset of the standards profiles, the importance of security as a cross-cutting issue warrants special attention. Security standards need not be a separate component of the Enterprise Architecture or of the TRM. Security standards profiles are Standards Profiles specific to the security services specified in the Enterprise Architecture. The profiles cover such services as: identification, authentication, and non-repudiation; audit trail creation and analysis; access controls; cryptography management; virus prevention; fraud prevention, detection and mitigation; and intrusion, prevention and detection. The purpose of the security profiles is to establish information and technology security standards to ensure adequate security for each component of the Enterprise Architecture, and to ensure that information systems conform to agency security policy. The security standards identified in the security standards profiles must be consistent with the requirements of OMB Circular A-130, Appendix III.

Maintaining and Implementing the ITA

While the development of an Enterprise Architecture is important, only its successful implementation meets the goals of the Clinger-Cohen Act. Having established a framework for the ITA, each agency should prioritize areas of high incremental benefits for early implementation. Particular attention should be given to the following:

- Change Management
- Legacy Systems Integration
- IT Personnel Planning
- Compliance, Waivers, and Certification

Change Management

Developing an ITA is an iterative and dynamic process. The ITA should be revised periodically so that it evolves as the agency's business functions evolve. Thus, the ITA itself should be managed with the same change control process that governs other critical documents.

A baseline of the current environment -- how and where IT assets are currently used -- should be part of the initial development of the ITA, and the baseline should be maintained over time. The ITA should reflect the agency's technology research effort. Every agency should have a mechanism for evaluating current technologies and identifying new IT opportunities for the agency. An option for many agencies may be the establishment of an ITA board to act as a steward of the ITA and to perform these ITA development and maintenance activities.

Legacy Systems Integration

A useful ITA must realistically account for the existing infrastructure base, including legacy systems. In this context, "legacy systems" refers to systems currently in use. The architectural strategy for dealing with legacy systems should focus on their interfaces with new systems, permitting the new and the old to interoperate in a cost-effective manner that does not compromise the ability of the new system to conform completely with the target architecture and standards. If the user interface of an older system does not conform to the architecture, a decision whether to change, replace, or terminate will turn on cost, operational, or functional effectiveness criteria.

Information Technology Personnel Planning

The ITA should reflect the training, procedures, and staffing needed to support its successful implementation. Agencies should identify the human resources and technical skills needed and available to develop, maintain, and implement the ITA. Agencies should plan for the remediation of deficiencies, including strategies and plans for hiring, training, and professional development (Clinger-Cohen, Section 5125 (c) (3)).

ITA Compliance, Waivers, and Certification

The ITA itself should guide systems changes for new and operational systems. Conformance to the ITA and compliance with the standards profiles is critical to success. Configuration management and control as well as quality software engineering processes for systems should be implemented to maintain compliance with the architecture. Configuration changes should be tested and validated prior to acceptance for operational use across the architecture.

To migrate from the agency's current environment to the target architecture, new systems will increasingly have to meet the standards of the ITA. The ITA should not be weakened nor should its impact as a tool diluted through the excessive use of waivers. The CIO and other senior managers should require strong business case justifications for exceptions to the ITA. Waivers for non-

conformance should be the exception, not the rule, and waivers should only be granted after a careful, thorough, and well documented analysis which supports the need for the exception.

An ITA should have an established method of evaluating the level of compliance of proposed new systems and of proposed modifications to current systems. This method may be formalized to the point of a certification process. At a minimum, metrics should be established which, if met, permit a proposed system to be termed "ITA compliant."

Appendix I: Published Architecture Model Sources

DEPARTMENT OF AGRICULTURE

The U.S. Department of Agriculture (USDA) has recently developed its first version of the USDA Information Systems Technology Architecture (ISTA). The Architecture is a high level document divided into three components: Business and Data Architecture (Part I), Technical Standards Architecture (Part II), and Telecommunications Architecture (Part III). The Business and Data Architecture identifies core business processes for each of USDA's mission areas and associated common data elements. The Technical Standards Architecture has three tiers: Tier I "Core Technologies," Tier II "General Purpose Productivity Enabling Technologies," and Tier III "Integrating Technologies." The Telecommunications Architecture identifies an enterprise network architecture for USDA.

The three components of the USDA ISTA can be mapped to the NIST model. The Business/Data Architecture aligns with the Business Functions and Data Descriptions layers and the Technical Standards and Telecommunications Architectures align with the Technology Infrastructure layer. The USDA ISTA is a living document and will be continually refreshed to ensure USDA employs established and emerging technology to meet its strategic business goals.

The Office of the Chief Information Officer has also developed a set of criteria to guide the agency's IT investment decisions based on OMB Memorandum 97-02. USDA is establishing the required management mechanisms and tools to ensure successful integration and implementation, assessment, and monitoring of the USDA architecture needs. Additional information and copies of the USDA ISTA may be obtained from Mr. Joseph Ware, Chief, Information Management Division, Office of the Chief Information Officer, USDA; phone: (202) 690-2118; fax: (202) 690-2831; or E-mail: joe.ware@usda.gov.

DEPARTMENT OF DEFENSE

The C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) Architecture Framework, Version 1.0 , prepared by the C4I Integration Support Activity (CISA), serves as guidance to Department of Defense (DoD) organizations that need to develop architectural descriptions for their internal use or to support broader Departmental activities. The objective of the Framework Version 1.0 is to provide guidelines for developing architecture descriptions that are internally consistent within themselves, of practical use to decision makers at all appropriate levels, and will integrate with other architecture descriptions across DoD.

The C4ISR Architecture Framework is organized by the three architecture "views": Operational, Systems and Technical. The framework details products that may be needed in the course of describing an architecture view and also indicates the kinds of information to be captured in each product. While the Operational, Systems, and Technical Architectures frequently are discussed as if they were separate architectures, they are best considered as different views of an architecture -- each focusing on particular aspects. The three architectures views are defined as follows:

1. Operational Architectures containing "descriptions of the tasks, operational elements, and information flows required to accomplish or support a warfighting function." i.e., the pertinent activities, operational elements, and associated information flows.

2. Systems Architectures describing "systems and interconnections which support the warfighting functions," that is, systems (including Automated Information Systems, communications, and weapon platforms) used to satisfy operational needs and the corresponding interconnections.

3. Technical Architectures are "a minimal set of rules governing 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," such as, technical standards, criteria, and reference models that govern the implementation of systems to satisfy the operational needs.

The aforementioned architectures are described by products that are graphical, database and/or textual. For convenience, the products are categorized according to their main view: Operational, Systems, or Technical. However, any given architecture description will consist of the best combination of products to illuminate the issue area, whether they are categorized as Operational, Systems, and/or Technical products. In addition to the view-specific products, Information Infrastructure Products provide support within and/or across the views. These products include entity-relationship models, attributed information models, and an Integrated Data Dictionary.

For more information about the C4ISR Architecture Framework, Version 1.0, please contact Mr. Jim Bain, Director of the Architectures Directorate in the C4I Integration Support Activity, at 703-883-6907 or by E-mail at james.bain@osd.mil.

DEPARTMENT OF ENERGY

The Department of Energy's Information Architecture (IA) is being defined in four volumes, as follows:

Volume I, "The Foundations," issued in March 1995 - Prescribes the IA Principles, the Conceptual IA Model, a high level business case, the current IA baseline, the standards process, a summarized vision, IA policy, and next steps.

Volume II, "The Baseline Analysis," issued in December 1996, is a three part document consisting of the Baseline Analysis Summary (Part 1), the Detailed Baseline Analysis (Part 2), and Baseline Analysis Reference (Part 3). The three parts are founded on an extensive Department-wide analysis using a series of models to assess and extract the significant challenges of the IA. These challenges are described in key areas and are graphically depicted. Findings and conclusions are also presented.

Volume III, "Guidance," targeted for April 1997 (currently in Draft), provides specific guidance to Departmental elements, strongly recommending the formalization of Information Architectures at various levels within DOE (particularly for Programs and sites). The IA principles, conceptual model, minimal design characteristics, IA program, and standards are covered.

Volume IV, "IA Vision," targeted for September 1997, defines the future Departmental Architecture by (subarchitecture) layer, depicting the targeted capabilities and structures envisioned by function. It will give specific examples of business functions and how they are depicted in each layer. It will also relate the standards to each applicable layer.

Other documents available include: "The Standards Service Action Plan," (March 1997), the "DOE IA Standards Profile," the "Standards Process Guide," and the "IA Methodology Guide."

In general, DOE is following the NIST five-layered architectural model, because it ensures that linkages are established from the business functions and processes down though the information, applications and data layers, down to the specific technologies utilized to support the business. The above documents go into detailed explanations regarding what each layer addresses and on other facets of DOE's IA Program.

These documents can be obtained on the DOE IA Web site at HTTP://www-it.hr.doe.gov/iat/, or by contacting Mr. Michael Tiemann, DOE IA Project Manager at michael.tiemann@hq.doe.gov or (202) 586-5461.

DEPARTMENT OF TREASURY

The Treasury Information System Architecture Framework (TISAF) is a model to assist Treasury Bureaus to develop their Enterprise Information System Architectures (EISAs). The TISAF consists of a

list of goals and objectives for planning Treasury information technology, a set of architectural principles for developing information systems, an EISA model for describing distinct views of enterprise information systems, and a set of standards for guiding specific product selection. The EISA model provides four architectural views to organize, plan, and build enterprise information systems, consisting of the Information, Functional, and Work architectures and the Infrastructure.

The Information Architecture is the "what" of information systems which defines and organizes all information needed to perform business operations and describes the relationships among this information. The Functional Architecture is the "how" of information systems which defines and organizes the business functions, processes, or activities that capture, manipulate, and manage the business information to support business operations.

The Work Architecture is the "where" of information systems which depicts the decentralization of the business, the description of the work organizations to business locations, and the communications and coordination between these locations. The Infrastructure is the "enabler" of information systems which describes the supporting services, computing platforms, and internal and external interfaces needed to provide technology environments within which information systems run.

To provide a context for discussing technical standards, a Technical Reference Model (TRM) is developed to organize and depict building blocks of an information system as a set of services categorized by functional areas. For more information and a copy of the TISAF, please contact Mr. Simon Liu at (202) 622-9089, or E-mail at simon.liu@cio.treas.gov.

Appendix II: Additional References

"Application Portability Profile (APP): The U.S. Government's Open System Environment Profile Version 3.0," Computer Systems Technology, NIST, Feb. 1996.

"Architecture Concepts and Design Guidance (TAFIM)," Department of Defense, vol. 3, ver. 2.0, 6/94.

"C4ISR Architecture Framework," C4ISR ITRF, Integrated Architecture Panel, v. 1.0, Department of Defense, CISA-0000-100-96, 6/96.

"Developing the Information Systems Architecture for World-Class Organizations," Lee, Management Decisions, 34/2, 1996, pp. 46-52.

"Enterprise," Department of the Army Technical Architecture, ver. 4.5, 11/12/96.

"Experiences and Examples in Development of Information Systems Architecture," Performance Engineering Corporation, Presentation to the Department of Justice, 4/96.

"How to Align Corporate Goals and Information Technology," Dietrich, Communication News, Vol. 32, No. 10, , 10/1/95.

"Information Architectural Design in Business Process Reengineering," Kettinger, Journal of Information Technology, Vol. 11, pp. 27-37, 1996.

"Information Architecture Volume I: The Foundations," Department of Energy, 3/95.

"Information Architecture Volume II: Baseline Analysis Summary" Department of Energy, 12/96.

"Information Architecture Volume III: Guidance," Department of Energy, 4/97.

"Information Management Directions: The Integration Challenge," Computer Systems Technology, National Institute of Standards and Technology, 9/89.

"Information Systems Technology Architecture Review," Information Technology Resources Board (ITRB), 12/96.

"Joint Technical Architecture," C4ISR, Department of Defense, vol. 1.-0, 8/96.

"Open System Environment (OSE): Architectural Framework for Information Infrastructure," Schulz, NIST Special Publication 500-232, September, 1995.

"Levels of Information System Interoperability," for the C4I Integration Support Activity, Architecture Directorate, MITRE Corporation, 6/96.

"Perspectives," Hurwitz, Computer World, 10/1/95.

"Plan Your Top Priorities," Cash, Information Week, 3/4/96.

"Standards-Based Architecture (SBA) Planning Guide," Defense Information Systems Agency (DISA), 10/93.

"A Systems Engineering Approach to Information Architecture Design," Levis, IFAC Integrated Systems Engineering, 1994, pp. 131-144.

"Technical Architecture Framework for Information Management (TAFIM)," Department of Defense, Vol. 1: Overview, ver. 2.0, 6/94.

"Technology Defiant: Your Ticket To Ride?" Braue, Data Communications, Vol. 24. No. 14, 10/1/95.

"Treasury Information Systems Architecture Framework," Department of Treasury, ver. 1.0, 1/97.

"What is an Information Technology Architecture," IDC Government, 1/96.

*Footnotes
_____

1. Examples of published architectural "frameworks" include the Treasury Information System Architecture Framework (TISAF), the Department of Defense Technical Architecture Framework for Information Management (TAFIM), and the Department of Energy's Information Architecture Volume 1.
2. Examples of agency efforts to develop Enterprise Architectures and how the agencies have named and described these components are found in Appendix I.
3. The Department of Defense includes aspects of the Business Processes element in its Operational Architecture; the Department of Treasury incorporates it into its business view.
4. The Department of Agriculture has incorporated this component into its Business Architecture, while the Department of Defense and Treasury have built it into their Operational Architectures.
5. The Department of Energy incorporates Business Applications into its Applications Subarchitecture, while the Department of Treasury includes them in its Functional Architecture.
6. The Department of Agriculture has included in this element in its Business/Data Architecture, while the Department of Treasury incorporates it in its Information Architecture.
7. The Department of Agriculture has incorporated this architecture into its Technical Standard and Telecommunications Architectures. DoD uses its System Architecture, and Treasury its Infrastrucsture to describe the physical layer.
8. For services not covered by published standards, agencies should identify *de facto* industry standards or specific products that best accommodate an open system environment.