



**Classification No.:** 2120.1  
**Approval Date:** 09/09/2004  
**Review Date:** 09/09/2005

---

## **Interim Enterprise Architecture Policy**

---

### **Purpose:**

The purpose of this U.S. Environmental Protection Agency (EPA) Interim Enterprise Architecture Policy is to ensure the Enterprise Architecture Program affords the Agency the opportunity to maximize the business value of EPA's investment in information technology and minimize the amount of unnecessary redundancy resulting from disparate planning and development efforts. More specifically, this policy:

- a. Establishes the governance of EPA's Enterprise Architecture Program;
- b. Sets direction for how the Enterprise Architecture will be developed and maintained;
- c. Establishes how information technology (IT) investments will be made and maintained in compliance with the Enterprise Architecture;
- d. Facilitates alignment of EPA's current business processes, strategic planning, human capital planning, organizational structures, information management programs, and budget and capital investments with the EPA's mission, goals, and objectives;
- e. Supports changes and enhancements to the Agency's business, as directed by Congress or the President, and in response to the Administrator's priorities and program office and regional initiatives;
- f. Supports and enhances information system development and practices to allow EPA and its partners to assess environmental and human health information with a holistic view; and
- g. Promotes public access to environmental information through the effective use of information technology.

---

### **Audience:**

This policy applies to all EPA personnel, agents or others authorized to work or conduct business for EPA. Further, this policy applies to Agency partners, EPA contractors and recipients of EPA financial assistance (e.g., grants, and Interagency Agreements (IAGs)).

---

### **Background:**

The Clinger-Cohen Act requires federal agencies to establish Enterprise Architecture programs and focus on the results achieved through capital investments, while streamlining the federal information technology procurement process.

EPA has implemented an Enterprise Architecture that must be maintained and updated under formal direction and governance, align with the Federal Enterprise Architecture, and support Presidential initiatives and Executive Orders.

In December 2002, EPA published proposed policy for establishing an Enterprise Architecture Practice, Enforcement Function, and Enterprise Architecture Tool Usage (U.S. EPA, *Target Architecture*, December 2002). This Policy further establishes that proposal.

In December 2002, EPA also adopted guiding principles for the Enterprise Architecture. Those principles, and any subsequent revisions to them, will serve as the foundation for this Policy, related procedures, guidance materials, and all future revisions (see Appendix A).

---

**Policy:**

**I. Governance and General Practice**

There is one authoritative Enterprise Architecture for the Agency for which the CIO establishes a governance structure.

The Enterprise Architecture is an authoritative representation of the Agency's strategic direction, organizational programs and projects, lines of business, information technology portfolio (i.e., data, applications, and technologies), security measures, and the inter-relationships among them. It is maintained for the purpose of supporting the Agency's strategic planning, budget formulation and execution, information technology capital planning, information technology acquisition, human capital, and security planning processes.

The Enterprise Architecture serves as a sub-component of the Federal Enterprise Architecture and is therefore maintained in alignment with Federal Enterprise Architecture and e-Government requirements.

This Policy is supplemented with procedures, technical standards, and guidelines as established and published by the CIO or designee. Compliance with the procedures and technical standards is mandatory. Compliance with the guidelines is mandatory unless a senior official in the sponsoring organization has approved an alternate practice that is preferred and beneficial for the particular business concern.

**II. Enterprise Architecture Development and Approval**

All Assistant and Regional Administrators or their designees participate in the development and maintenance of the Enterprise Architecture and its subcomponents.

Security is a primary consideration in the development and implementation of the Enterprise Architecture.

The Enterprise Architecture and any subdivisions are developed utilizing a common framework and methodology that ensures conformance with the Federal Enterprise Architecture.

The Enterprise Architecture is approved by the Chief Information Officer.

### **III. Enterprise Architecture Maintenance and Toolset Usage**

The Enterprise Architecture is updated to align with the Agency's strategic and budgetary plans and the information technology capital planning process.

The Enterprise Architecture is maintained under version and configuration control within the Agency's Enterprise Architecture repository and toolset.

Any subdivisions of the Enterprise Architecture repository and toolset must be interoperable with, and recorded within, Agency's Enterprise Architecture repository and toolset.

### **IV. Enterprise IT Investment Portfolio Compliance**

Compliance with Enterprise Architecture Policy, procedures, technical standards and guidelines is mandatory for all EPA organizations, including contractors that direct, develop, maintain, and operate information technology systems in support of the Agency.

All EPA information management and technology acquisitions must comply with the Enterprise Architecture.

All new and modified information technology development projects must include the development of a Solution Architecture (see Definitions), that ensures adherence to the Enterprise Architecture and the Enterprise Architecture Principles identified in Appendix A. Solution Architectures must be approved by the Chief Architect prior to project development.

All IT systems, applications, data, and metadata, must be recorded within an authoritative inventory.

---

#### **Roles and Responsibilities:**

**EPA Administrator:** The Administrator is the champion of Enterprise Architecture, responsible for communicating its value as an enterprise management tool.

**Assistant Administrators and Regional Administrators:** The Assistant Administrators and Regional Administrators ensure that their organizations actively participate with the Chief Architect and comply with the target architecture. They may also develop Component Architectures in alignment with the Enterprise Architecture.

**Chief Information Officer (CIO):** The CIO has the responsibility and authority for the Enterprise Architecture Program, providing strategic direction, and enforcing its requirements. The CIO establishes, maintains, and approves the Enterprise Architecture. The CIO, or designee, supplements this Policy by approving procedures, technical standards, and guidelines.

**Chief Financial Officer (CFO):** The CFO is the responsible authority for: (a) all architectural considerations required under the Chief Financial Officers Act of 1990 (the CFO Act) and (b) ensuring the Enterprise Architecture and the Capital Planning and Investment Control processes are integrated with strategic and budget planning.

**Chief Technology Officer (CTO):** The CTO is responsible for procedures, technical standards and guidelines associated with the technology and security architectural components.

**Chief Acquisition Officer (CAO):** The CAO ensures information technology services contracts contain requirements for compliance with the Target Architecture through the EPA Acquisition Regulation.

**Chief Architect (CA):** The CA is responsible for providing direction to the Enterprise Architecture development and maintenance, and ensuring its coordination with the Federal Enterprise Architecture and EPA's IT collaborations with state, local, and tribal partners.

---

**Authorities:** See Appendix B

---

**Related Documents:** See Appendix C

---

**Recertification Date:** 09/09/2005

---

**Additional Information:** For further information about this Policy, see [www.intranet.epa.gov/architec](http://www.intranet.epa.gov/architec), or contact the Chief Architect in the EPA Office of Environmental Information, Office of Technology Operations and Planning, Information Technology Policy and Planning Division.

## **Appendix A**

### **Enterprise Architecture Principles**

The following Enterprise Architecture Principles, published in the *U.S. EPA Target Architecture*, December 2002, provide the conceptual foundation of the EPA Enterprise Architecture Policy.

#### **General Principles**

- a. Information resource management activities comply with applicable laws, regulations, policies, procedures, and standards.
- b. Interoperability is a goal of infrastructure, data management, and applications development.
- c. Enterprise-wide access to information, based on users' business need for, and rights to, that information, is the rule rather than the exception.
- d. Individual system development or implementation efforts must not dictate enterprise architecture, enterprise data models, enterprise object models, enterprise business process models or enterprise business rules without an independent review from an enterprise level.

#### **Business Architecture Principles**

- a. Business objectives must be well-defined before information technology solutions are initiated. Business processes (along with security requirements) drive the data architecture, applications architecture, and technical architecture.
- b. Maximizing value is the main objective when making information technology decisions.

#### **Data Architecture Principles**

- a. Information is not only an organizational asset but also a national asset for which our employees are the stewards.
- b. All enterprise-level data have a shared enterprise-wide definition and are accessible to all organizations in the enterprise. Enterprise-level data are data that are collected or compiled by the Agency and which support its mission to protect human health and the environment.
- c. Data is captured once and validated at the source or as close to the source as possible. Data will not be gathered multiple times from the same source.
- d. Data names will be standardized between applications and across database platforms.
- e. Data access is to be independent of physical data location.

## **Application Architecture Principles**

- a. Cross-functional applications are highly encouraged where appropriate.
- b. Business and information requirements should be met using commercial off-the-shelf (COTS) technology rather than customized or in-house solutions, whenever practical.
- c. Applications are designed to be highly granular and loosely coupled. In other words, applications should be flexible to allow for the possibility of future re-partitioning and/or reuse of different application components to adapt to changing business needs and requirements.
- d. The integration of information must adhere to good business practices:
  - Applications should derive from established needs of internal and external customers and be able to effectively respond to emerging needs.
  - Applications should minimize data collection burden and use resources efficiently.
  - Applications should provide effective and economical access to EPA and other data.
  - Applications should authenticate the sources of information.
- e. All applications will incorporate approved data standards by the recommended date.
- f. The applications architecture should support effective data exchange between data partners of widely varying resources.
- g. Applications should be robust enough to handle changing business needs.
- h. Applications should be deployed across an N-Tier, distributed computing environment.
- i. Flexibility should be designed into the architecture to accommodate continuing business changes and improvements in technology.
- j. Established industry vendors, best practices, technology standards and products should be invested in being at the forefront of current trends.

## **Technology/Security Architecture Principles**

- a. The technology architecture's ability to adapt to user needs is paramount.
- b. The technology architecture is based on open technology and should rely on reusable components.
- c. Security is designed into all architectural components, balancing accessibility, availability and ease of use with protection of the integrity of the data and, where appropriate, protection of the confidentiality of the data.
- d. A level of security should be applied to resources commensurate to their value to the organization and sufficient to contain risk at an acceptable level.
- e. External systems are assumed to be insecure and internal security features should be planned accordingly.
- f. Application security should be based on open standards and use security features and services consistent with open standards where possible.

- g. Layered protections should be applied to mitigate vulnerabilities in COTS products, isolate system components and limit or contain vulnerabilities.
- h. Information security is primarily an issue of governance and process, not technology; the applicable organizational goals and policy must therefore serve as the framework on which the remainder of the security architecture is built. Effective change management is key to maintaining a secure environment.
- i. Proactive identification of vulnerabilities and assessment of the associated risks is essential.
- j. Audit and monitoring mechanisms should be used to secure information resources.
- k. Public access systems should be isolated from mission critical resources.

## **Appendix B**

### **Authorities**

- a. The Clinger-Cohen Act of 1996 (also known as the Information Technology Management Reform Act of 1996) (Pub. L. 104-106, Division E);
- b. The Government Performance and Results Act of 1993 (GPRA) (Pub. L. 103-62);
- c. The Chief Financial Officers Act of 1990 (31 U.S.C. 3512 et seq.);
- d. The Federal Information Security Management Act of 2002 (which amends the Computer Security Act of 1987 (Pub. L. 100-235));
- e. The Paperwork Reduction Act of 1995 (Pub. L. 104-13);
- f. The Government Paperwork Elimination Act of 1998 (Pub. L. 105-277, Title XVII);
- g. The E-Government Act of 2002 (Pub. L. 107-347);
- h. The Rehabilitation Act of 1998 (Pub. L. 105-220);
- i. The Federal Managers Financial Integrity Act (FMFIA) of 1989 (Pub. L. 97-255);
- j. The Federal Financial Management Improvement Act (FFMIA) of 1996 (Pub. L. 104-208);
- k. The Privacy Act, as amended (5 U.S.C. 552a);
- l. The Budget and Accounting Act, as amended (31 U.S.C. Chapter 11);
- m. The Federal Acquisition Streamlining Act (FASA) of 1994;
- n. The President's Management Agenda, Office of Management and Budget, Fiscal Year 2002;
- o. Executive Order 13011, Federal Information Technology, FR 61-140, July 19, 1996;
- p. OMB Circular A-11, Preparation, Submission and Execution of the Budget, revised July 25, 2003;
- q. OMB Circular A-94, Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs, revised January 22, 2002;
- r. OMB Circular A-123, Management Accountability and Control, dated June 21, 1995;
- s. OMB Circular A-127, Financial Management Systems, dated July 23, 1993;
- t. OMB Circular A-130, Management of Information Resources, dated November 28, 2003.

## **Appendix C**

### **Related Documents**

- a. U.S. Environmental Protection Agency: *2003 Strategic Plan*, September 30, 2003;
- b. U.S. Environmental Protection Agency: *Human Capital Strategic Plan*, December 2003;
- c. U.S. Environmental Protection Agency: *Baseline Architecture*, September 2002;
- d. U.S. Environmental Protection Agency: *Target Architecture*, December 2002;
- e. U.S. Environmental Protection Agency: *Enterprise Architecture Status Report 2003*, September 2003;
- f. *Performance Reference Model (PRM) Version 1.0, Vols. I & II*, Federal Enterprise Architecture Program Management Office, September 2003;
- g. *Business Reference Model (BRM) Version 2.0*, Federal Enterprise Architecture Program Management Office, June 2003;
- h. Data Reference Model (undated draft);
- i. *Service Component Reference Model (SRM) Version 1.0*, Federal Enterprise Architecture Program Management Office, June 2003;
- j. *Technical Reference Model (TRM) Version 1.1*, Federal Enterprise Architecture Program Management Office, August 2003;
- k. *U.S. EPA IT Roadmap and Standards Profile*;
- l. *Information Resources Management Policy Manual*, EPA Directive 2100B8;
- m. *Interim System Life Cycle (SLC) Policy*, Directive 2100.4;
- n. *Interim System Life Cycle (SLC) Procedure*, Directive;
- o. *Data Standards Policy*;
- p. EPA Acquisition Regulation, Information Resources Management clause;
- q. *Capital Planning and Investment Control (CPIC) Policy*, Directive 2100.2a1
- r. *Procedure: Obtaining a Waiver from an EPA IT Requirement* (in draft).