

GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2110.2
November 26, 2008

GSA ORDER

SUBJECT: GSA Enterprise Architecture Policy

1. Purpose. This directive prescribes agency-wide policy, principles, roles and responsibilities for the establishment and implementation of the GSA Enterprise Architecture (EA).
2. Cancellations. This Order cancels GSA Order 2110.1, "One GSA" Enterprise Architecture Policy, dated July 23, 2004.
3. Background. The Clinger-Cohen Act requires the Agency Chief Information Officer (CIO) to oversee the development and maintenance of a sound, and integrated agency-wide information architecture. Office of Management Budget through Circular A-130 has interpreted the information architecture identified in the Clinger-Cohen Act to mean the Agency EA. For GSA, the EA recognizes the federated model under which the organization operates. The GSA EA is intended to guide the GSA-wide business modernization blueprint and maximize the value of related Information Technology (IT) and Business investments within the federated model. The current and target state architectures that comprise the GSA EA are composed of artifacts that specify processes, technology, data, services, and other capabilities necessary to perform GSA's mission. The architectural artifacts are aligned to GSA's business areas.
4. Applicability. This guidance applies to all GSA organizations and persons in positions with responsibility for using information technology to support business and administrative operations in GSA.
5. Policy. The GSA EA is a strategic business asset. As such, the EA is integral to the GSA Performance Management, Capital Planning and Investment Control, Budgeting, and System Development Life Cycle processes. As a tool, the GSA EA supports enterprise and business level planning and decision making.

a. The GSA EA will support the business needs and priorities expressed through GSA Strategic Plan, IT Strategic Plan;

b. Service and Staff Offices (SSOs) will be responsible for resourcing the development of the Office of Management and Budget approved GSA architecture segments in their business lines;

The GSA EA will be used to support alignment of the GSA IT portfolio;

d. With support from the GSA CIO, the SSOs will develop and maintain segment architectures consistent with guidance from the Enterprise Architecture Committee;

e. Architecture development and maintenance will be compliant with the methods and technology baseline established and approved by the Enterprise Architecture Committee;

f. The Enterprise Architecture Committee will establish value and performance measures to assess compliance, completion, and results derived directly and indirectly from the use of the GSA EA;

g. The Enterprise Architecture Committee will be the governance body that provides management oversight of the GSA-wide EA program;

h. SSOs will support the GSA CIO reporting of EA in accordance with the Office of Management and Budget defined criteria.

6. Enterprise Architecture Guiding Principles. The GSA EA guiding principles represent fundamental requirements and practices to be used when developing, using, or maintaining the GSA architecture.

a. General Principles. EA links strategic planning, transformation and modernization of business processes and supporting technology.

(1) Whenever possible, seek commonality across program and business lines, and promote interoperability across GSA. Interoperability and information sharing should be pursued with respect to business processes and supporting infrastructure.

(2) Enterprise-wide access to information based on users' business need for, and rights to, that information is the rule rather than the exception.

(3) The GSA Capital Planning investment portfolio will be underpinned by planning that is informed by the GSA EA.

(4) Flexibility should be designed into the architecture to accommodate continuing business changes and improvements in technology.

(5) Alignment of business and IT to support business agility and effectiveness is a key objective of EA.

(6) Enterprise and business level architectural segment designs and implementations must support approved business processes, services, data, and technology.

(7) The GSA EA is owned by the business.

b. Business Principles. The GSA EA will be business driven.

(1) Business processes, along with security requirements, drive the data architecture, applications architecture, and technical architecture.

(2) Maximizing business value is the primary objective when making IT and investment decisions.

c. Data Principles. Information is a strategic business asset.

Data is an Agency asset and will be shared with all who have a business need.

(2) Data is captured once and validated at the source or as close to the source as possible.

(3) Data will not be gathered multiple times from the same source.

(4) Data names will be standardized between applications and across database platforms.

(5) Data access is to be independent of physical data location.

d. Service Component Architecture Principle.

(1) Reusability of service components (or applications) will be promoted whenever possible.

(2) If commercial off-the-shelf (COTS) technology is not feasible, business and information requirements should be met with standard-based solutions; building customized or in-house solutions is discouraged.

(3) Service components (or applications) should be designed to be highly granular and loosely coupled. Applications should allow for future re-partitioning and/or reuse of application components to adapt to changing business needs and requirements.

(4) The integration of information must adhere to good business practices:

(a) Service components (or applications) should support established business needs and be agile enough to respond to emerging needs.

(b) Service components (or applications) should minimize data collection burdens and use resources efficiently.

(c) Service components (or applications) should provide effective and economical access to GSA and other data.

(d) Service components and services will be discoverable to minimize duplicative efforts.

(e) Service components (or applications) must incorporate approved data standards.

e. Technology/Security Architecture Principles. The technology and security architecture must support the secure conduct of business activities.

(1) The technology architecture will be based on the appropriate set of approved technologies contained in the GSA IT Standards Profile.

(2) The technology architecture's ability to adapt to user needs is paramount.

(3) The technology architecture should be based on open standards and use of security controls and services consistent with business needs, where possible.

(4) Security must be applied to all GSA EA identified resources commensurate to their value and an acceptable level of business risk.

(5) The technology and security architecture must reflect all defined security policies for public access systems and mission critical resources.

(6) The technology architecture must be compliant with the GSA Technology Reference Model.

7. Organizational Roles and Responsibilities. GSA's governance policy addresses the various forums and stakeholder roles and responsibility. The organizational roles and responsibilities listed below are specific to the requirements of the architecture practice within GSA.

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

b. Heads of Service and Staff Offices (HSSOs), and Regional Administrators. The HSSOs and Regional Administrators ensure that their organizations actively participate

with the Chief Architect and comply with the target architecture. They may also develop Segment Architectures in alignment with the Enterprise Architecture.

c. 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.

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

e. Chief Technology Officer (CTO). The CTO is responsible for procedures, technical standards and guidelines associated with the technology. Additionally, the CTO in concert with the CA and SAISO will ensure that information security requirements from FISMA legislation and associated NIST security standards and guidelines are integrated into segment architectures.

f. Senior Agency Information Security Officer (SAISO). Responsible for carrying out Federal Information Security Management Act (FISMA) and agency-wide information security liaison. Additionally, the SAISO in concert with the CTO and CA will ensure appropriate guidance is developed for incorporating security into segment architectures.

g. Chief Acquisition Officer (CAO). The CAO ensures information technology services contracts contain requirements for compliance with an approved Target Architecture through GSA Acquisition Regulation.

h. Chief Architect (CA). The CA is responsible for providing direction for the Enterprise Architecture development and maintenance, and ensuring its coordination with the Federal Enterprise Architecture and collaboration with GSA's partners.

8. References.

- a. The Clinger-Cohen Act of 1996 (Pub. L. 104-106, Division E);
- b. OMB Circular A-11, Preparation, Submission and Execution of the Budget;
- c. OMB Circular A-130, Management of Federal Information Resources;
- d. E-Government Act of 2002;

e. Federal Enterprise Architecture Reference Models;

f. Federal Transition Framework.

CASEY COLEMAN
Chief Information Officer

Printer Friendly Format