THE COMMON APPROACH TO FEDERAL ENTERPRISE ARCHITECTURE

May 2, 2012

Table of Contents

INTRODUCTION

This document provides guidance for a common approach to the practice of Enterprise Architecture (EA) throughout the Executive Branch of the U.S. Federal Government. Federal law and policy require Agency Heads to develop and maintain an agency-wide enterprise architecture that integrates strategic drivers, business requirements, and technology solutions.[1] [2] The *Common Approach to Federal Enterprise Architecture* promotes increased levels of mission effectiveness by standardizing the development and use of architectures within and between Federal Agencies.[3] [4] This includes principles for using EA to help agencies eliminate waste and duplication, increase shared services, close performance gaps, and promote engagement among government, industry, and citizens.

The target audience for this document is Federal Government employees who plan, approve, and execute Agency programs, and those in industry who support those activities.

Within the Federal Government there are over 300 organizational entities of differing size, scope, and complexity which include departments, administrations, bureaus, commissions, agencies, and boards. These entities employ more than 2.6 million people and spend over $3.4 trillion each year to perform their mission functions, often through services that are directed to customer groups that include citizens, industry, academia, non-profits, and other government agencies in the U.S. and abroad. Over $80 billion of annual federal spending is devoted to various forms of information technology (IT) that enable thousands of mission and support services across the Executive Branch and with external groups.

During the past several years many Agency budgets have gone from flat to declining, yet the public's expectations of government continue to rise. In response, there has been a widespread call from Congress, the Administration, citizens, and industry for more cost-efficient Agency operating models and more transparency in tracking the performance of federal programs. Shrinking budgets increase the urgency for accomplishing these changes so that scarce resources can be directed to areas of the Agency that will contribute the most value. The *Common Approach to Federal Enterprise Architecture* accelerates Agency business transformation and new technology enablement by providing standardization, design principles, scalability, an enterprise roadmap, and a repeatable architecture project method that is more agile and useful and will produce more authoritative information for intra- and inter-Agency planning, decision-making, and management.

---

[1] Congressional mandates for IT architecture are contained in the Clinger-Cohen Act of 1996 (P.L. 104-106) which was updated and revised by the E-Government Act of 2002 (P.L. 107-347) to reflect enterprise architecture.

[2] Related implementation guidance from the Office of Management and Budget is contained in various documents, including Circulars A-11, A-130, Memoranda 97-16, 00-10, 05-22, 11-29, 12-10, and the *Digital Government Strategy*.

[3] This document replaces document: "*A Practical Guide to Federal Enterprise Architecture*", February 2001.

[4] The Government Performance and Results Modernization Act of 2010 (P.L. 111-352) addresses agency strategic plans / priority goals.

The Common Approach supports the Office of Management and Budget's IT Shared Services Strategy, Digital Strategy, and implementation of the Portfolio Stat process.

OVERALL CONCEPT

This document's common approach to Federal EA provides principles and standards for how business, information, and technology architectures should be developed across the Federal Government so they can be used consistently at various levels of scope within and between agencies, as well as with external stakeholders. The common approach provides integration points with other governance areas including strategic planning, capital planning, program management, human capital management, and cyber security. The meta-model for *The Common Approach to Federal EA* is depicted in Figure 1 below:

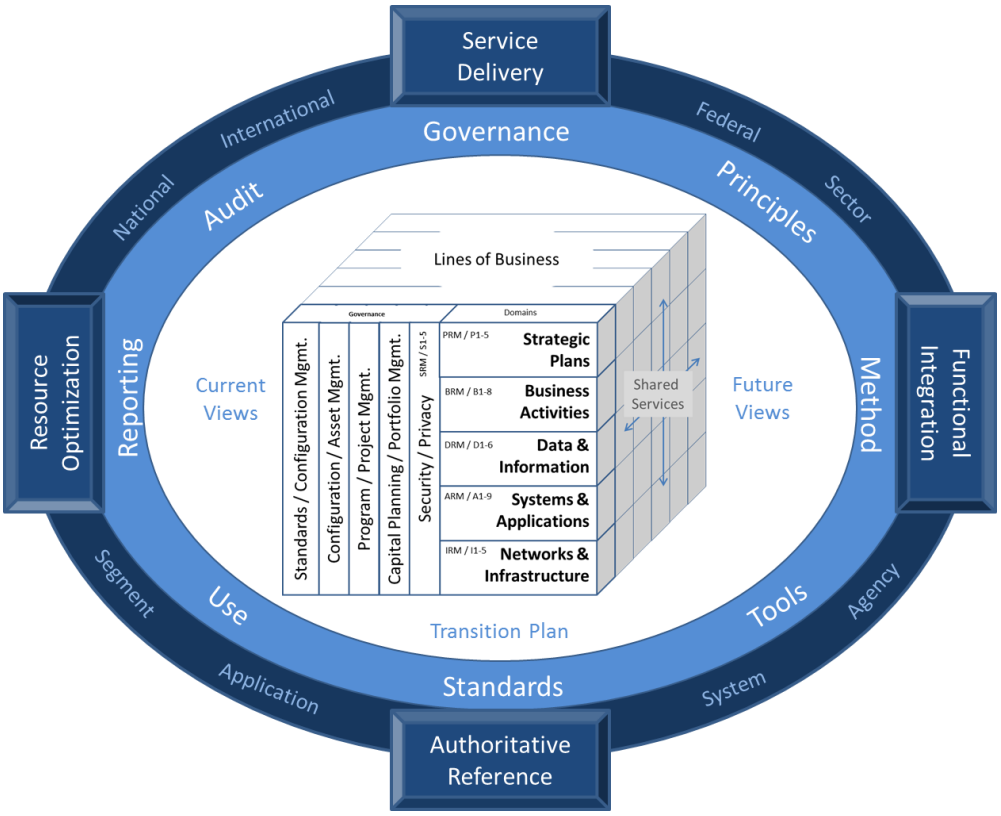


Figure 1. The Common Approach to Federal EA

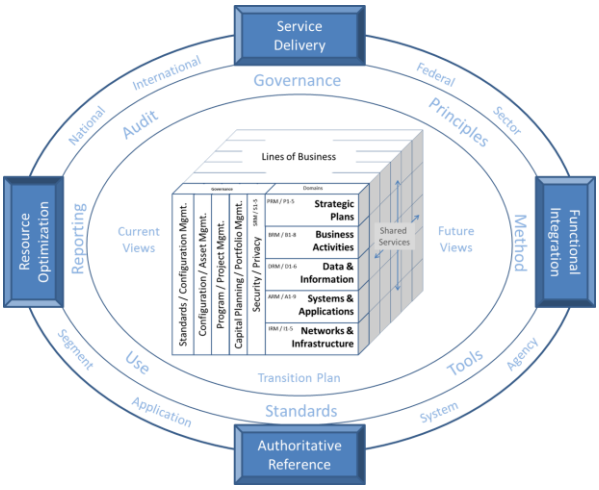
Standardization in the *Common Approach to Federal EA* is based on the following items: primary outcomes, levels of scope, basic elements, sub-architecture domains, reference models, current and future views, transition plans, and a roadmap. When implemented, this standardization promotes comparable architectures across the Federal Government

that will be more useful in managing change and enabling mission success with a lower total cost of ownership, faster time to market, and reduced duplication.

PRIMARY OUTCOMES

There are four primary outcomes that are enabled by the common approach to federal EA:

- Service Delivery
- Functional Integration
- Resource Optimization
- Authoritative Reference



While there are many positive outcomes that EA contributes to, these four outcomes are "primary" in that they represent areas of direct, positive impact that architectures can make within and between agencies and with customers and partners external to government.

EA is uniquely positioned as the management best practice which can provide a consistent view across all program and service areas to support planning and decision-making. EA standards also promote mission success by serving as an authoritative reference, and by promoting functional integration and resource optimization with both internal and external service partners.

Service Delivery

Federal Agencies[5] exist to perform a wide spectrum of missions that meet our Nation's ongoing needs through a variety of programs and services. These missions, programs, and services are provided in law, Administration policy, and Agency policy. Increasingly, these mission and support programs/services/systems require joint management and execution by multiple Agencies that are enabled through an IT shared service strategy and various embedded information-related technologies.

[5] This document's use of the term "Federal Agency" includes Departments, Agencies, Commissions, Bureaus, and Boards and other types of organizations in the Executive Branch of the U.S. Federal Government.

Success in accomplishing an Agency's mission and optimizing resources requires a coherent and consistent understanding of program and service performance, and agile planning and development processes. This coherent view and agility becomes more important in resource-constrained operating environments. EA ensures that IT enables the business and mission functions to achieve optimum performance.

Functional Integration

Functional integration means interoperability between programs, systems, and services, which requires a meta-context and standards to be successful. EA can provide both a meta-context across all functional domains (strategic, business, and technology) as well as related standards for the full lifecycle of activities in each domain.

Program, systems, and services interoperability is foundational for Federal Government organizations to be able to successfully partner in new shared service models that may involve outside providers and new roles for participation (e.g., consumer, developer, or provider). The EA should provide context and be the source of standards for all levels of interoperability.

Resource Optimization

As custodians of public funds, federal sector organizations have a special responsibility to optimize their use of resources. Additionally, because of a variety of factors that cannot be anticipated or controlled (e.g., new laws, policies, and regulations; growing/evolving customer needs, new technologies, natural disasters, etc.) federal organizations must often accomplish their mission with less resources than anticipated.

The organization's enterprise-wide architecture should and must continuously evolve over time to document the discovery of an increasingly harmonized set of views as measured by their degree of completeness of the scope of the variables being depicted, the consistency across the views, and how coherently they reflect the problem being solved. As an authoritative reference for the organization, these views allow for more informed planning and decision-making each year for capital planning and the investment portfolio. Asset management (e.g., hardware inventory and software licenses) and configuration management (maintaining and monitoring a documented baseline of users, processes, hardware, and software) are important elements of resource optimization that EA also enables.

EA is important to the successful introduction of new technologies and operating paradigms that promote resource optimization, such as cloud computing, virtualization, the semantic web, mobile technologies, business intelligence, and social media.

Authoritative Reference

Just as the blueprints of a building are the authoritative reference for how the structure will function, the organization's enterprise-wide architecture provides an integrated, consistent view of strategic goals, mission and support services, data, and enabling technologies across the entire organization, including programs, services, and systems.

When the EA is recognized as the authoritative reference for the design and documentation of systems and services, issues of ownership, management, resourcing, and performance goals can be resolved in a more consistent and effective manner.

EA also serves as a reference to promote the achievement and maintenance of desired levels of security and trust in an Agency's business and technology operating environment. EA's contribution to security protection is accomplished through the integrated use of federal methods[6] [7] during process or resource design activities to identify and implement controls to address potential vulnerabilities with users, processes, systems, applications, and networks.[8]

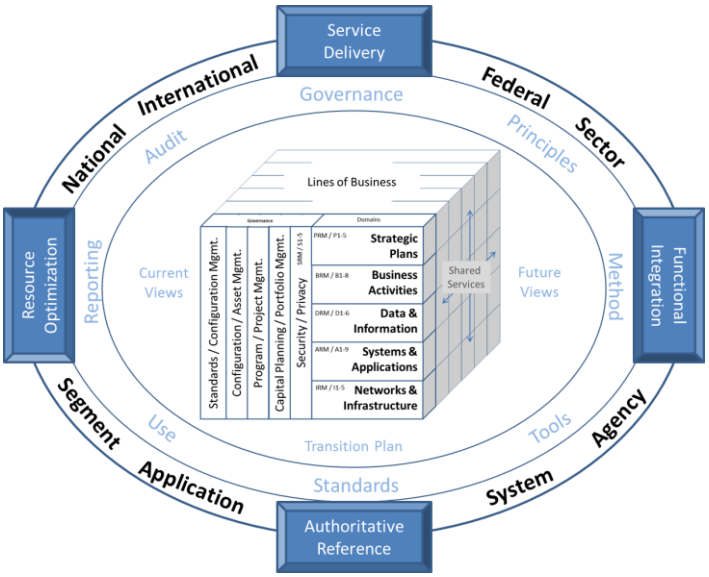
Configuration management is an important part of successful, secure business and technology operations. EA contributes to effective configuration management practices by providing authoritative reference information that reflects the hardware, software, and process designs that have been approved and include risk-adjusted security and privacy controls. This approach to maintaining a "verified configuration" should be applied on an ongoing basis to infrastructure, host environments, systems, applications, and workflow, in combination with intrusion detection capabilities, to enable effective continuous monitoring.[6] Continuous monitoring of verified configurations in clouds and non-cloud based host environments is essential to maintaining effective levels of security and privacy, and as such, is an important consideration in all EA projects.

[6] National Institute of Science and Technology (NIST) Special Publications 800-37, 39, 47, 53 (Revision 3), 53A, and 144.
[7] Federal Information Processing Standards 199 and 200.
[8] Federal Enterprise Architecture's Security Reference Model v1.0 (release date is scheduled for March 2012).

LEVELS OF SCOPE

There are eight levels of scope for implementing an architecture using the common approach:

- International
- National
- Federal
- Sector
- Agency
- Segment
- System
- Application



These levels of scope promote consistency in architecture methods to promote comparability and support varying levels of complexity.

The scope of a particular architecture ranges from high level views of one or more organizations, to detailed views of a single segment, system, or application. Due to the nature of how the U.S. Federal Government functions, multiple levels of scope are needed to develop effective architectures that support mission and support objectives within and between agencies.

It should be noted that an enterprise-wide architecture for a Federal Agency will include strategic, business, and technology views that derive from documentation and analyses that are produced through architecture projects at the applicable levels of scope described herein. The standardized approach for federal agencies to use in creating and updating architectures involves a five-step method, design principles, and a set of core and elective artifacts in each of the six sub-architecture domains. These methods, principles, and artifacts are described in subsequent sections of this document.

Architecture at Various Levels of Scope

International: This level of architecture focuses on international partnerships of the U.S. Federal Government with other governments, global industry, non-profits, and other groups. These international-level architectures often center on the enablement of shared services, wherein the roles of provider and consumer need to be detailed and a comprehensive business model for the service provides the requirements for the architecture.

National: This level of architecture includes all Federal, State, Tribal, and Local government agencies within the U.S. and its territories. These architectures are very important to the coordination of nation-wide capabilities, such as first-responder coordination, disaster notification, telecommunications, and transportation infrastructure.

Federal: This level of architecture focuses on services (and associated systems) that serve the entire Executive Branch of the U.S. Federal Government. These Federal-wide mission and support services are channeled through OMB-designated "Line of Business" providers, wherein the roles of provider and consumer are detailed and a comprehensive business model for each Federal-wide service generate requirements for that architecture.

Sector: This level of architecture focuses on a system or service in one particular mission sector of the Executive Branch of the U.S. Federal Government. These inter-agency architectures often include the enablement of mission and/or support shared services, wherein the roles of provider and consumer need to be detailed and a comprehensive business model for the service provides the requirements for the architecture. These architectures may also include private sector participants.

Agency: This level of architecture provides an overview of the entire department/agency and consistent, decomposable views of all sub-agencies/bureaus, business units, programs, systems, networks, and mission or support services. The depth of documentation in any particular area of an agency's architecture is determined by the need to support planning and decision-making, prioritized in the context of the agency's strategic goals and business operating plans. Drill-down is accomplished through the completion of segment, system, and application-level architectures, as described below.

Segment: This level of architecture focuses on a particular service area or business unit within an agency or between agencies that is not Federal-, Sector-, or Agency-wide. Each segment is defined either organizationally (e.g., as a business unit and per the organization chart) or functionally (as a vertical or crosscutting mission or support service).

System: This level of architecture focuses on one particular information technology system, which supports the delivery of one or more services within or between segments and agencies. All aspects of a system's functionality and configuration should be documented, including strategic drivers, business requirements, applicable standards, workflow processes, information exchanges, software applications, host infrastructure, remote access, and security/privacy controls.

Application: This level of architecture focuses on the development, update, or integration of one or more software applications that are part of one or more system(s)/service(s) in one or more organization(s). This includes websites, databases, email, and other mission or support applications.

Figure 2 shows the relationship between these levels of architectural scope, and the concept that the level of detail and scope for analysis and documentation will vary according to the requirements and planned usage for each architecture.

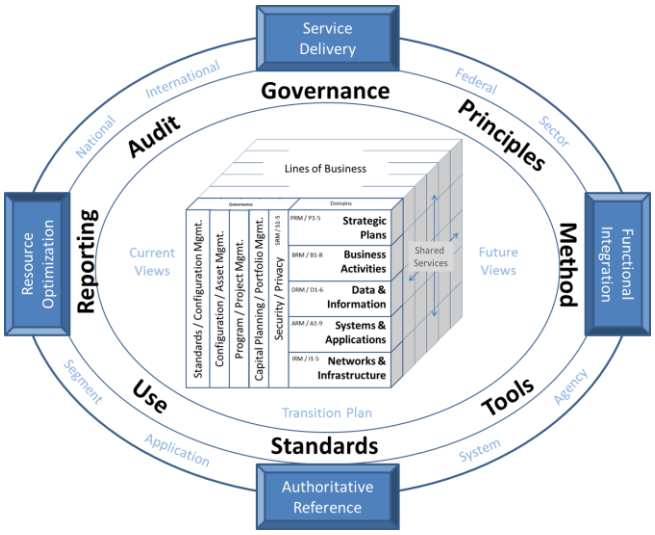
Architectural Level	Scope	Mission Impact	Planning Detail	Audience
International	U.S. & Other Governments	Global Outcomes	Low	All Stakeholders
National	U.S. - Wide	National Outcomes		
Federal	Executive Branch	Government Outcomes		
Sector	Multiple Agencies	Mission Outcomes	Medium	Business Owners
Agency	One Agency Organization	Mission Outcomes		
Segment	One or More Business Units	Business Outcomes		
System	One or More Systems	Functionality	High	Users and Developers
Application	One or More Applications	Functionality		

Figure 2. Levels of Architectural Scope and Impact

BASIC ELEMENTS OF FEDERAL ENTERPRISE ARCHITECTURE

There are eight basic elements that must be present and be designed to work together in each agency EA program:

- Governance
- Principles
- Method
- Tools
- Standards
- Use
- Reporting
- Audit



These elements ensure that agency EA programs are complete and can be effective in developing solutions that support planning and decision-making.

EA Basic Element #1: Governance

The first basic element is "Governance" which identifies the planning, decision-making, and oversight processes and groups that will determine how the EA is developed, verified, versioned, used, and sustained over time with respect to measures of completeness, consistency, coherence, and accuracy from the perspectives of all stakeholders.

Figure 3 on the next page provides a view of the interrelationships between federal guidance, agency governance processes, and the programs that implement that guidance in an integrated manner. This governance model begins in the upper left quadrant with law and policy; moves to the upper right quadrant where high-level agency directives are represented; moves down to the lower right where operations and planning/management functions are reflected, and finally to the lower left quadrant where architecture and standards are reflected. The model finishes in the center where portfolio and investment management occurs through a number of planning and decision-making bodies. The harmonizing/standards role of EA is depicted as being driven by law and policy and delivering authoritative reference information and design alternatives for the capital planning process in the center.

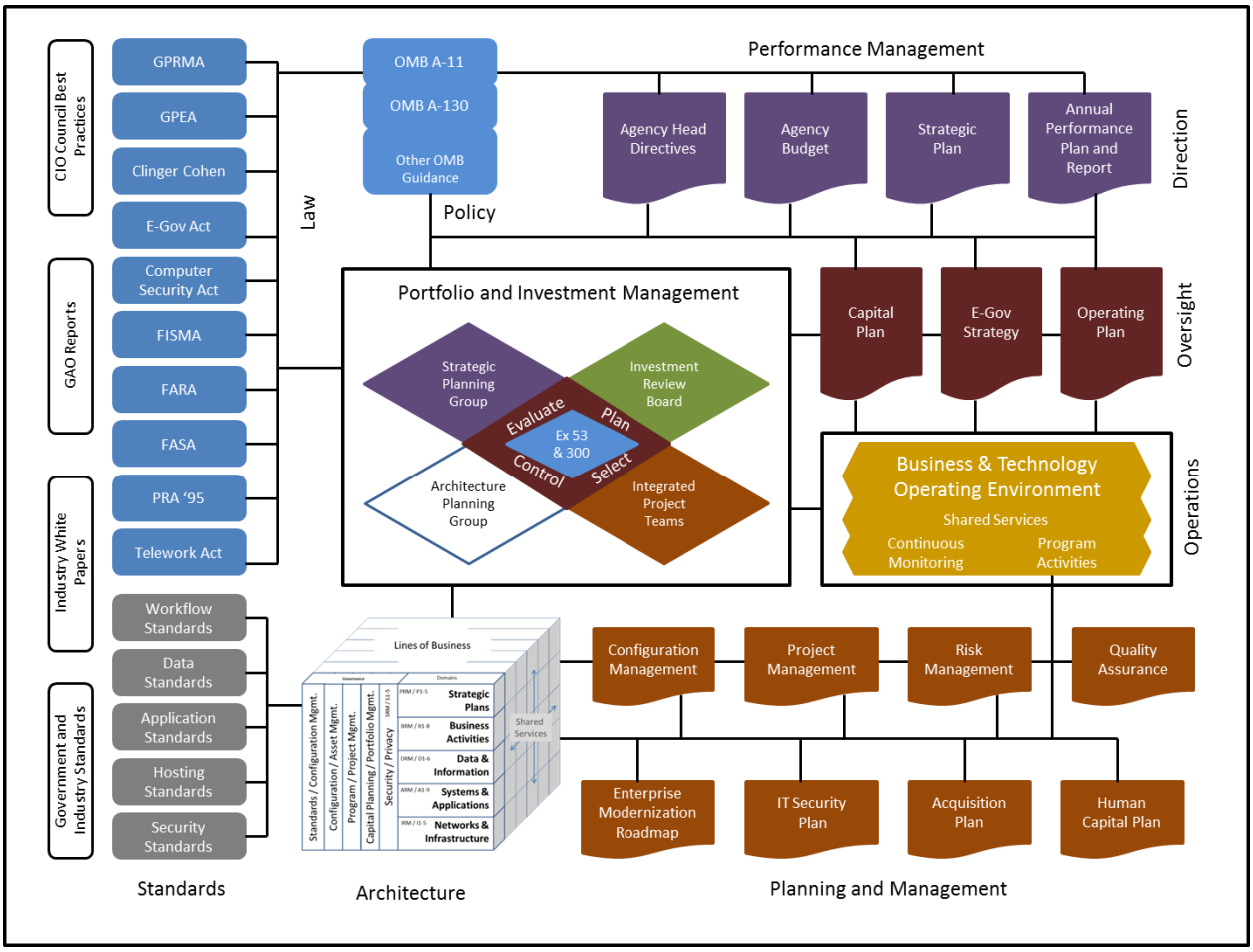


Figure 3. Integrated Governance

Figure 4 below provides an example of integrated governance structures from a program-centric perspective wherein an Agency's Program Manager (PM) is the accountable entity and subject matter experts from the business and technology areas are supporting the PM. Here we are referring to PMs for mission or support programs, not the EA program.

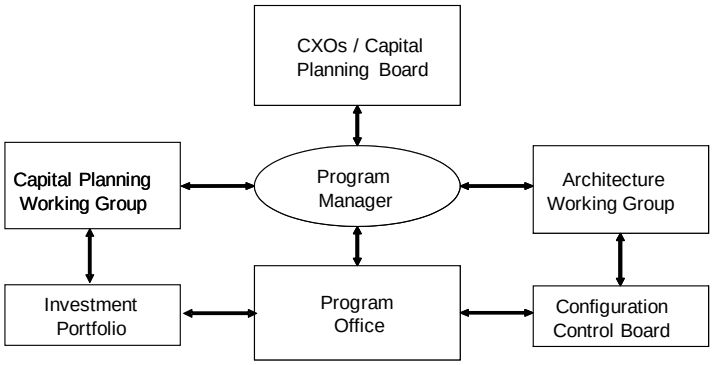


Figure 4. Program Governance

EA Basic Element #2: Principles

General Principles

The following are general principles for the *Common Approach to Federal EA* and represent the criteria against which potential investment and architectural decisions are weighed.

Future-Ready. EA helps the Federal Government to be successful in completing the many missions that the Nation depends on. Mission requirements continually change, and resources are often limited – EA is the key business and technology best practice that enables Agencies to evolve their capabilities to effectively deliver needed services.

Investment Support. EA supports intra- and inter-agency investment decision-making through an "architect – invest – implement" sequence of activities. Agencies must ensure that investment decisions are based on architectural solutions that result in the achievement of strategic and/or tactical outcomes by employing technology and other resources in an effective manner.

Shared Services. Agencies should select reusable and sharable services and products to obtain mission or support functionality. Increasingly, the Federal Government is becoming a coordinator and consumer as opposed to the producer of products and services. Standardization on common functions and customers will help Federal Agencies implement change in a timely manner.

Interoperability Standards: Federal EA promotes intra- and inter-agency standards for aligning strategic direction with business activities and technology enablement. Agencies should ensure that EA solutions conform to Federal-wide standards whenever possible.

Information Access. EA supports Federal Government transparency and service delivery through solutions that promote citizen, business, agency, and other stakeholder access to Federal information and data, balanced by needs for Government security and individual privacy. EA solutions should support a diversity of public and private access methods for Government public information, including multiple access points, the separation of transactional from analytical data, and data warehousing architecture. Accessibility involves the ease with which users obtain information. Information access and display must be sufficiently adaptable to a wide range of users and access methods, including formats

accessible to those with sensory disabilities. Data standardization, including a common vocabulary and data definitions are critical.

Security and Privacy: EA helps to secure Federal information against unauthorized access. The Federal Government must be aware of security breaches and data compromise and the impact of these events. Appropriate security monitoring and planning, including an analysis of risks and contingencies and the implementation of appropriate contingency plans, must be completed to prevent unauthorized access to Federal information. Additionally, EA helps Agencies apply the principles of the Privacy Act of 1974 and incorporate them into architecture designs.

Technology Adoption. EA helps Agencies to select and implement proven market technologies. Systems should be decoupled to allow maximum flexibility. Incorporating new or proven technologies in a timely manner will help Agencies to cope with change.

Design and Analysis Principles

EA is most effectively practiced in a common way at all levels of scope when it is based on principles that guide the actual design and analysis work that goes into architecture projects. The *Common Approach to Federal Enterprise Architecture* promotes the following design and analysis principles in each of the three primary domains (strategy, business, and technology) that serve as a guide for EA programs and architecture projects:

Strategic Principles:

- Agency IT Strategy and Enterprise Roadmap should be developed in close coordination with broader agency strategic planning efforts to ensure alignment of automated information management processes and investments with overall organization priority
- The structure of Agency IT strategic plans should follow the same fundamental structure as Agency strategic plans and performance documents. Agency IT strategic planning documents should focus on achievement of overall Agency strategic outcomes rather than the optimization of internal CIO processes
- Internal CIO process optimization performance measurement should be managed through lower level planning processes
- The Enterprise Architecture is "the" authoritative reference for planning IT support for optimum business performance
- Agency-wide information sharing and protection policies are specified
- Security and privacy requirement must be identified and addressed

Business Principles:

- Agency business activities exist to meet strategic objectives
- Services should be standardized within and between agencies where possible

- Services should be web-enabled whenever possible
- Security controls must be designed into IT support of every business process

Technology Principles:

- Data and information exchange should be based on open standards
- Privacy considerations must be designed into every data solution
- Use well documented interfaces built on non-proprietary open platforms using standard platform independent data protocols (such as XML)
- Application platforms should be virtualized whenever possible
- Open-source software solutions should be included in alternatives analyses
- Use cloud-based application, platform, and infrastructure hosting designs whenever possible to promote scalability, cost-efficiency, and metering
- Convergence in voice, data, video, and mobile technologies supports infrastructure consolidation, which should be pursued wherever possible
- Host solutions must be compliant with federal policy and standards (e.g., Trusted Internet Connection, IPv6 routing, and PIV authentication)
- Desktop/mobile solutions must be compliant with the latest US Government Configuration Baseline standard
- Security controls must be designed into every technology solution

EA Basic Element #3: Method

In its most successful form, EA is used by organizations to enable consistent planning and decision making, and not simply relegated to use within a single branch of an Information Resource Management Office. In today's agency operating environment, which demands more efficient government through the reuse of solutions and the use of services, organizations now need an EA community of practice and standard methods that support efforts to leverage other Federal, state, local, tribal, and international experiences and results as a means to most efficiently solve priority needs.

The role of an enterprise architect is to help facilitate and support a common understanding of needs, help formulate recommendations to meet those needs, and facilitate the development of a plan of action that is grounded in an integrated view of not just technology planning, but the full spectrum of planning disciplines to include mission/business planning, capital planning, security planning, infrastructure planning, human capital planning, performance planning, and records planning. Enterprise architects provide facilitation and integration to enable this collaborative planning discipline, and work with specialists and subject matter experts from these planning groups in order to formulate a plan of action that not only meets needs but is also implementable within financial, political, and organizational constraints. In addition, enterprise architects have an important role to play in the investment, implementation, and performance measurement activities and decisions that result from this integrated planning.

The Collaborative Planning Methodology (CPM), shown in Figure 5, is a simple, repeatable process that consists of integrated, multi-disciplinary analysis that results in recommendations formed in collaboration with leaders, stakeholders, planners, and implementers. The first release of the CPM includes the master steps and detailed guidance for planners to use throughout the planning process. EA is but one planning discipline included in this methodology. Over time the methods and approaches of other planning disciplines will be interwoven into this common methodology to provide a single, collaborative approach for organizations to use. The CPM is intended as a full planning and implementation lifecycle for use at all levels of scope described earlier in the common approach (International, National, Federal, Sector, Agency, Segment, System, and Application).

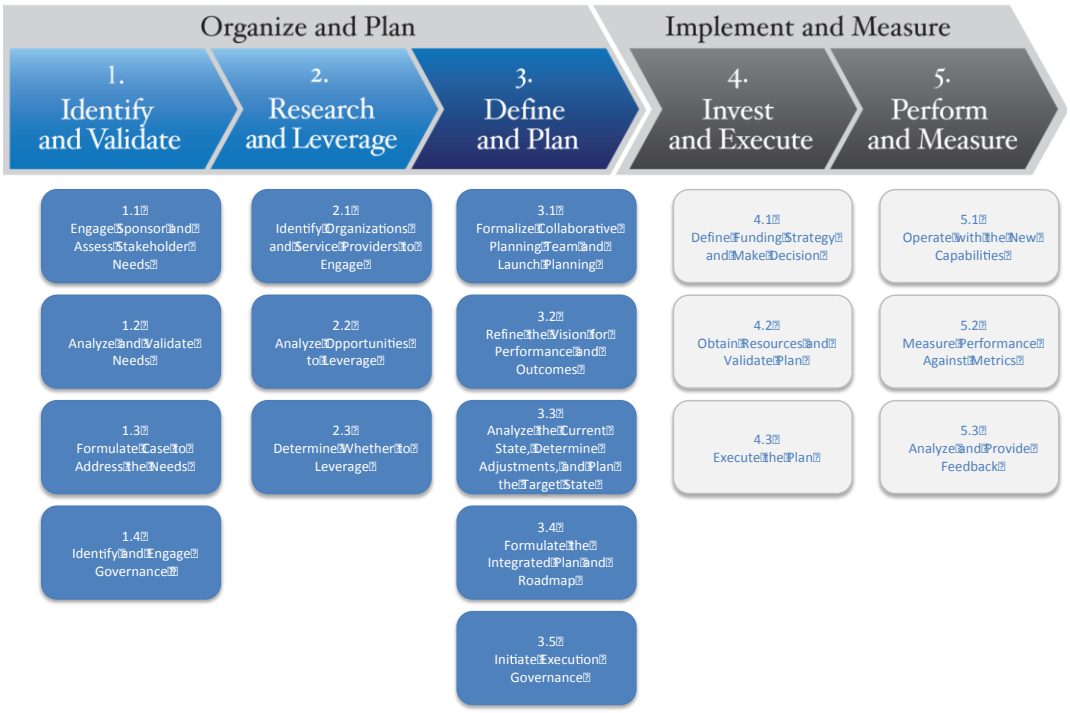


Figure 5. Collaborative Planning Methodology

The CPM consists of two phases: (1) Organize and Plan and (2) Implement and Measure. Although the phases are shown as sequential, in fact there are frequent and important iterations within and between the phases. In the first phase, the architect serves a key role facilitating the collaboration between leadership and various stakeholders to clearly identify and prioritize needs, researches other organizations facing similar needs, and formulates the integrated set of plans to define the roadmap of changes that will address the stated needs. In the second phase, the architect shifts into a participatory role, supporting other key personnel working to implement and monitor change related

activities. As part of the second phase of the methodology, the architect specifically supports investment, procurement, implementation, and performance measurement actions and decisions.

The CPM is stakeholder-centered with a focus on understanding and validating needs from leadership and stakeholder perspectives, planning for those needs, and ensuring that what is planned ultimately results in the intended outcomes (Step 1). Additionally, the CPM is structured to embrace the principles of leverage and reuse by assisting planners in determining whether there are other organizations that have previously addressed similar needs, and whether their business model, experiences and work products can be leveraged to expedite improvement (Step 2).

Ultimately, the CPM helps planners work with leadership and stakeholders to clearly articulate a roadmap that defines needs, what will be done to address those needs, when actions will be taken, how much it will cost, what benefits will be achieved, when those benefits will be achieved, and how those benefits will be measured (Step 3). The methodology also helps planners support leadership and stakeholders as they make decisions regarding which courses of action are appropriate for the mission, including specific investment and implementation decisions (Step 4). Finally and perhaps most importantly, the methodology provides planners with guidance in their support of measuring the actual performance changes that have resulted from the recommendations, and in turn, using these results in future planning activities (Step 5).

The five steps of the CPM are detailed as follows:

Step 1: Identify and Validate

Purpose: The purpose of this step is to identify and assess what needs to be achieved, understand the major drivers for change, and then define, validate, and prioritize the operational realities of the mission and goals with leadership, stakeholders, and operational staff. During this step, the leadership, stakeholder, and customer needs and the operational requirements are validated so that ultimately, all stakeholder groups are working towards the same, well understood, validated outcome. Initial performance metrics are created to begin focusing the measurement of success to be consistent across stakeholder groups. In this step, "leadership" can range in levels of scope from an executive leader over an international challenge to a functional leader who has identified steady state improvements that may include services, systems, or infrastructure. An additional purpose of this step is to identify and engage appropriate governance.

Architect's Role: In this step, architects facilitate a direct collaboration between leadership and stakeholders as they work together to define, validate, and prioritize

their needs, and build a shared vision and understanding. In doing so, the architects analyze stated needs in the context of overarching drivers to help aid decision makers in their assessment of whether stated needs are feasible and realistic. Since these needs shape the scope and strategic intent for planning, it is imperative that leadership and stakeholders agree on the needs before work begins on subsequent planning steps.

In addition to identifying needs, architects work with leadership and stakeholders to establish target performance metrics that will ultimately be used to determine if the planned performance has been achieved. Once needs are identified and validated, architects support leadership in identifying and initiating appropriate governance. Who makes the decisions and when those decisions will be made is important to the timing and buy-in of recommendations for change.

Outcome: At the end of Step 1, the key outcomes are (1) identified and validated needs, (2) an overarching set of performance metrics, and (3) a determination of who (governance) will ultimately oversee and approve recommended changes to meet those needs.

Step 2: Research and Leverage

Purpose: The purpose of this step is to identify external organizations and service providers that may have already met, or are currently facing needs similar to the ones identified in Step 1, and then to analyze their experiences and results to determine if they can be applied and leveraged or if a partnership can be formed to address the needs together. In alignment with "Shared First" principle, it is at this point that the planners consult both internal and external service catalogs for pre-existing services that are relevant to the current needs. In some instances, an entire business model, policy, technology solution, or service may be reusable to address the needs defined in Step 1 – an important benefit in these cost-constrained, quickly evolving times. Based on this analysis, leadership and stakeholders determine whether or not they will be able to leverage the experiences and results from other organizations.

Architect's Role: Architects facilitate the research of other organizations and service providers to assess whether they have similar needs and whether these organizations have already met these needs or are currently planning to meet these needs. The architects lead the assessment of the applicability of the other organizations' experiences and results and help to determine whether there are opportunities to leverage or work together to plan. Once these organizations and their needs and experiences have been identified and assessed, the architect formulates a set of findings and recommendations detailing the applicability and opportunity for leverage. These findings and

recommendations are submitted to leadership who engages governance with this information as appropriate.

Outcome: At the conclusion of Step 2, the architects, leadership, and stakeholders have a clear grasp on the experiences and results of other organizations, and the leadership and / or governance have determined whether or not they can leverage these experiences for their own needs. In some instances, another organization may be currently planning for similar needs and a partnership can be formed to collectively plan for these needs. The decision to leverage or not leverage has a significant impact on the planning activities in Step 3. For instance, if the organization determines that its can leverage policies and systems from another organization in order to meet its own needs, these policies and systems become a critical input to planning in Step 3.

Step 3: Define and Plan

Purpose: The purpose of this step is to develop the integrated plan for the adjustments necessary to meet the needs identified in Step 1. Recommended adjustments could be within any or all of the architecture domains: strategy, business, data, applications, infrastructure, and security. The integrated plan defines what will be done, when it will be done, how much it will cost, how to measure success, and the significant risks to be considered. Additionally, the integrated plan includes a timeline highlighting what benefits will be achieved, when their completion can be expected, and how the benefits will be measured. It is during this step that analysis of current capabilities and environments results in recommended adjustments to meet the needs identified in Step 1. Also during this step, the formal design and planning of the target capabilities and environment is performed. In addition to the integrated plan, the full complement of architecture, capital planning, security, records, budget, human capital, and performance compliance documents is developed based on the analysis performed in Step 3. The end outcome is an integrated set of plans that can be considered and approved by leadership and governance.

Architect's Role: Architects lead the development of the architecture by applying a series of analysis and planning methods and techniques. Through this process, the architects plan for each of the architecture domains (strategy, business, data, applications, infrastructure, and security) and produce data as well as artifacts to capture, analyze, and visualize the plans for change. Most important is the architect's efforts to synthesize the planning into recommendations that can be considered and approved by leadership and governance. During the creation of the architecture, architects facilitate interaction with other planning disciplines (e.g. budget, CPIC, security) so that each discipline's set of plans is integrated into a cohesive set of recommendations to meet the needs stated in Step 1. Throughout these efforts,

architects maintain the integrated plan and roadmap to reflect the course of action that has been determined through these planning activities.

Outcome: At the end of Step 3, leadership and stakeholders will possess an integrated set of plans and artifacts defining what will be done, when it will be done, what benefits will be achieved and when, and an estimate of cost. This set of plans should be synthesized into discrete decision-making packages for leadership and governance that are appropriate given financial, political, and organizational constraints.

Step 4: Invest and Execute

Purpose: The purpose of this step is to make the investment decision and implement the changes as defined in the integrated plan. Many groups participate in this step, however, it is important to note that these groups will need to work as a coordinated and collaborative team to achieve the primary purpose of this step: to successfully implement the planned changes.

Architect's Role: In this step the architect is in a support role, assisting in investment and implementation activities by providing information to aid in decisions, and to support interpretation and revision of plans from Step 3. The architects may be required to continue research and analysis into other organizations and their experiences (Step 2), update plans (Step 3), or re-engage stakeholders for feedback (Step 1). The architects have a continuing support role (e.g. interpreting the plans, making changes to the plans, supporting decision making) throughout investment and implementation. The involvement of architects does not cease at the conclusion of planning in Step 3.

Outcome: During Step 4, a decision is made concerning the investment in the changes that were planned in Step 3. At the end of Step 4 the recommendations for addressing the defined needs have been implemented. If the investment is not approved, the architect, leadership, and stakeholders return to previous steps to alter the recommendations and plans for future leadership consideration. It is important to reiterate that the integrated plans (Step 3) and the implementation (Step 4) could consist of a variety of changes to include, but not limited to, policy changes, organizational changes, technology changes, process changes, and skills changes.

Step 5: Perform and Measure

Purpose: During Step 5 the mission is operated with the new capabilities planned in Step 3 and implemented in Step 4. The purpose of Step 5 is to operate the mission and measure performance outcomes against identified metrics.

Architect's Role: The architects may not be the keeper of the actual performance data, but they need to leverage available performance data to assess whether the implemented capabilities achieve planned performance metrics. Feedback from this step can feed into future planning efforts as well as immediate planning and implementation adjustments as necessary. Feedback may also necessitate more immediate changes in plans that may need to be considered by governance, including configuration management.

Outcome: At the end of Step 5, the new capabilities as planned in Step 3 and implemented in Step 4 will be operational. The key outcome of this step is measured performance outcomes against identified metrics.

Sub-Architecture Domains

Each solution produces a tangible capability (e.g., system, network, service) that spans six sub-architectural domains in the overall EA: strategy, business, data, applications, infrastructure, and security. These domains are hierarchical (except security, which is a "thread" or cross cutting concern involving all domains) in that strategic goals drive business activities, which are the source of requirements for services, data flows, and technology enablement. Security controls pervade all of the other domains by providing risk-adjusted control elements in the form of hardware, software, policy, process, and physical solutions.

Using the Architected Solution

The value of having an EA and being able to implement an architected solution is that it produces one or more design alternatives and authoritative information to support planning and decision-making for mission and support requirements. EA provides standards, methodologies, and guidelines that architects can re-use for their designs and plans.

Importance of the Framework

An EA framework defines the scope of the architecture and the relationship of sub-architecture views to enable analysis, design, documentation, and reporting. There are a number of EA frameworks in use in the public and private sectors, and this guidance does not seek to require only one type, but there are characteristics that a framework should possess to be selected for use in the federal sector:

- Comprehensive: Covers all aspects of an agency through current and future views of the strategic, business, and technology areas at whatever level of scope is selected;
- Integrated: Shows the relationship between sub-architecture domains for strategy, business, data, applications, infrastructure, and security; and
- Scalable: Supports architecture practices at various levels of scope

The Federal EA Framework, version 2.0 (FEAF-II) meets these criteria, an example of which is provided in Figure 6 on the next page. The geometry of the FEAF-II shows the hierarchical relationship of the major areas of the architecture, which serves to emphasize that strategic goals drive business services, which in turn provide the requirements for enabling technologies. This framework also shows the relationship of sub-architecture domains, how the architecture can be decomposed into segments (that follow structural or functional lines in the organization) and how shared services would be positioned. Finally, FEAF-II correlates the other areas of governance (capital planning, program management, and human capital management); documentation via an enterprise-wide modernization roadmap, a standard set of core / elective artifacts and reporting via standard reference model taxonomies in each sub-architecture domain.

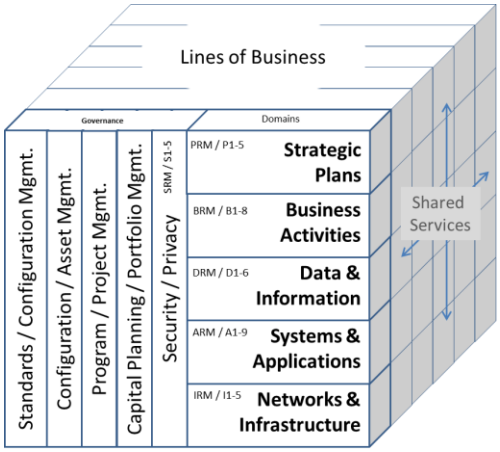


Figure 6. Federal Enterprise Architecture Framework v2 (FEAF-II)

EA Basic Element #4: Tools

Various types of software applications (tools) are required to support EA documentation and analysis activities, including:

- Repository website and content to create a visual representation of architecture
- Decomposable views of the overall architecture and specific architectures
- Over-arching "management views" of the architecture
- Strategic planning products and performance measures
- Business process documentation to answer key questions and solve problems
- Physical and logical design of data entities, objects, applications, and systems
- Physical and logical design of networks & cloud computing environments
- Links to applications and databases for analysis and reporting
- Links to the portfolio of investments and asset inventory
- Configuration management and quality standards
- Security and risk solutions for physical, information, personnel and operational needs

The tools that an agency selects for use with an EA program should not only develop and store documentation, but must be data centric and meet stakeholder needs for information to support planning and decision-making.

In using architecture information to support planning and decision-making, the EA repository is intended to provide a single place for the storage and retrieval of architecture artifacts. Some of the artifacts are created using tools and some are custom developed for particular uses (e.g., composite management views). A repository works best if it is easy to access and use. For this reason, a web-based EA repository is recommended. A repository should be located on the internal network to provide security for the information while still supporting access by executives, managers, and staff.

EA Basic Element #5: Standards

Architectural standards apply to all areas of EA practice and are essential to achieving interoperability and resource optimization through common methods for analysis, design, documentation, and reporting. Standards are included in the common approach to federal EA from a number of authoritative sources that are non-proprietary and support the ability to develop and use architectures within and between federal organizations, at the state, tribal, local and international levels, and with industry partners. Without standards, EA models and analyses will be done differently and "likewise comparisons" will not be possible between systems, services, lines of business, and organizations. Selected standards should include those from leading bodies nationally and throughout the world, including the National Institute of Science and Technology (NIST), the Institute of Electrical and Electronics Engineers (IEEE), the International Enterprise for Standardization (ISO), and the European Committee on Standardization (CEN).

EA artifacts are important standardization elements. An artifact is a type of model or documentation that describes part or all of an architecture. Types of artifacts include reports, diagrams, charts, tables, matrices, and spreadsheets. The format for high-level EA artifacts is often succinct text documents or diagrams that describe overall strategies, programs, and desired outcomes. Mid-level EA artifacts are documents, diagrams, charts, spreadsheets, and presentation slides that describe organizational processes, services, supply chains, systems, information flows, networks, and web sites. Low-level EA artifacts describe specific system and application resources, interface specifications, data dictionaries, technical standards, network hardware, and security controls. When these EA artifacts are harmonized and integrated to the greatest extent possible through the organizing taxonomy of the EA framework, new and more useful views of the architecture are generated. This is one of the greatest values of EA as a documentation process…

creation of the ability to see a hierarchy of views of the organization and/or lines of business that can be examined from several perspectives.

A "Reference Architecture" is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions. Reference Architectures solve a specific (recurring) problem in a problem space; explain context, goals, purpose, and problem being solved including when and how Reference Architecture should be used; and provide concepts, elements and their relationships that are used to direct/guide and constrain the instantiation of repeated concrete solutions and architectures. Reference Architecture serves as a reference foundation for architectures and solutions and may also be used for comparison and alignment purposes. There may be multiple Reference Architectures within a subject area where each represents a different emphasis or viewpoint of that area. A Reference Architecture for one subject area can be a specialization of a more general Reference Architecture in another subject area. The level of abstraction provided in a Reference Architecture is a function of its intended usage.

In this guidance for the *Common Approach to Federal EA*, there is one core documentation artifact for each of the six sub-architecture views, which serves to promote consistent views within and between architecture as well as promoting interoperability within and between government organizations. Additional details are provided in the "Documentation" section.

EA Basic Element #6: Use

The value of EA is in both the process and the products. Doing an architecture project provides a focus on a mission or support area of the organization and the resulting analysis and design activities, if done correctly, support improvements in that area. Only an enterprise-wide architecture can provide an integrated view of strategic, business, and technology domains across all lines of business, services, and systems – which is key to optimizing mission capabilities and resource utilization. At present, there is no other management best practice, other than EA, that can serve as a context for enterprise-wide planning and decision making. When an EA is viewed as authoritative by agency leadership, then it becomes a catalyst for consistent methods of analysis and design, which are needed for the organization to remain agile and effective with limited resources.

EA Basic Element #7: Reporting

The reporting function of an EA program is important in maintaining an understanding of current capabilities and future options. Providing a repository of architecture artifacts, plans, solutions, and other information is not enough (a "pull" model). What is also needed is regular reporting on capabilities and options through the lens of the architecture, delivered in a standardized way and from dash-boards for overall progress and health (a "push" model). The primary products for this type of standardized reporting are two-fold: (1) an annual EA Plan, and (2) a set of reference models that contain taxonomies to categorize information consistently in each sub-architecture view, as well as for the overall architecture. These plans and reference models do not contain artifacts. They contain information about what is in an architecture to support consistent reporting as well as supporting planning, decision-making, and analysis activities.

EA Basic Element #8: Audit

Auditing architectures and EA programs is important to ensuring quality work, consistent methods, and increasing levels of capability and maturity. As with any management or technology program, periodic audits are needed by internal and external experts to ensure that proper methods are being followed, information is accurate, and value is being produced for the organization. Add audits and recommendations should be presented to the Agency CIO for review and action.

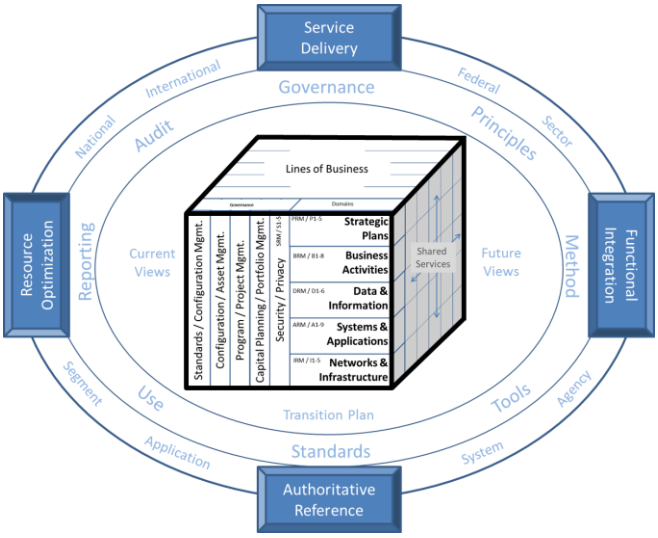
EA program and project auditing methods should be consistent with this common approach to federal EA and should also support the use of the EA Maturity Management Framework (EAMMF) Version 2.0 as a tool to evaluate maturity and promote the capability of EA programs.[9] The EAMMF v2.0 consists of four critical success attributes for managing EA programs; 7 maturity stages; and 59 elements of EA management that are at the core of an EA program.

[9] Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management, v2.0. U.S. Government Accountability Office, 10-846G, August 2010.

DOCUMENTATION

EA supports planning and decision-making through documentation and information that provides an abstracted view of an enterprise at various levels of scope and detail. There are six sub-architecture domains in the common approach to Federal EA:

- Strategic
- Business Services
- Data and Information
- Enabling Applications
- Host Infrastructure
- Security



These six sub-architecture domains delineate the types of analysis and modeling that is necessary for an architecture to meet stakeholder requirements.

Based on EA best practices, the following set of documentation associated with each sub-domain represents a minimum set of "core" artifacts that need to be considered and/or tailored to support a robust set of EA artifacts for the organization adopting the principles in this guide. To ensure interoperability and share-ability of services that will be developed as part of a cross-organization extended Service Oriented Architecture (SOA), a detailed meta-model of data in these artifacts will be required to sufficiently described and specify the attributes of components in the EA.

Each sub-architecture domain represents a specific area of the overall framework. The type and depth of documentation should be guided by the need for detail and answers to questions about requirements, applicable standards, timeframes, and available resources. In this guidance for the *Common Approach to Federal EA*, there is one required core documentation artifact for each of the six sub-architecture views, which serves to promote consistent views within and between architecture as well as promoting interoperability within and between government organizations. There are also several dozen elective artifacts to support additional analysis if that is needed. Table A provides a list of each of the required core artifacts in this common approach.

Sub-Architecture Domain	Required Core Artifact
Strategy	Concept Overview Diagram
Business	High-Level Process Diagram
Data	High-Level Logical Data Model
Applications	Application Interface Diagram
Infrastructure	High-Level Network Diagram
Security	Control List

Table A. Required Core Artifact List

Strategy Sub-Architecture Domain

The strategic sub-architecture domain identifies the mission, vision, and goals of the enterprise being documented. The primary documentation of this domain, is accomplished through a concept overview diagram and the identification of strategic drivers and goals, as should be specified in the Agency's Strategic Plan. The questions that should be asked for this domain begin with "for what purpose does the enterprise exist" (usually expressed in the mission statement) and "what does the enterprise want to do and be known for" (often given in the vision statement). Include artifact – mapping of initiative to appropriate performance goals or objectives. The questions then move to "what are the primary goals (strategic goals) of the enterprise" and "what then are the strategic initiatives (ongoing programs or new projects) that will enable the enterprise to achieve those goals", and "what are the measures of success (outcome measures) in each initiative area."

Table B provides core and elective artifacts in the strategy sub-architecture domain:

	Strategy Sub-Architecture Domain
S-1	Concept Overview Diagram (core)
S-2	Strategic Plan
S-3	Concept of Operations Scenarios
S-4	SWOT Analysis
S-5	Performance Measures Scorecard

Table B. Strategy Domain Artifacts

Business Sub-Architecture Domain

The questions to ask in the business sub-architecture domain begin with "what is the business plan (operating plan) and "how does this relate to the strategic plan's goals and metrics." Then, "what are the business units" (usually depicted in the organization chart) and "what are the mission and support services within and between the business units."

This follows with "how do we measure the effectiveness and efficiency of the line of business processes" (input/output measures) and their contribution to strategic goals (outcome measures) and "do any of these business services or manufacturing processes need to be reengineered/improved before they are made to be part of the future architecture"? Finally, "what are the workforce, standards, and security issues in this sub-architecture domain?" Table C provides core and elective artifacts for the business domain:

	Business Sub-Architecture Domain
B-1	Business Process Diagram (core)
B-2	Business Operating Plan
B-3	Business Service Catalog
B-4	Organization Chart
B-5	Use Case Narrative and Diagram
B-6	Business Case / Alternatives Analysis

Table C. Business Domain Artifacts

Data Sub-Architecture Domain

In the data sub-architecture domain of the EA framework, after the lines of business and specific business services have been identified, it is important to ask "what are the flows of information that will be required within and between service areas in order to make them successful" and "how can these flows of information be harmonized, standardized, and protected to promote sharing that is efficient, accurate, and secure", as well as "how will the data underlying the information flows be formatted, generated, shared, and stored?" Also, "what are the workforce, standards, and security issues in this domain?" Table D provides core and elective artifacts in the data sub-architecture domain:

	Data Sub-Architecture Domain
D-1	Logical Data Model (core)
D-2	Knowledge Management Plan
D-3	Data Quality Plan
D-4	Data Flow Diagram
D-5	Physical Data Model
D-6	CRUD Matrix
D-7	State-Transition Diagram
D-8	Event Sequence Diagram
D-9	Data Dictionary
D-10	Object Library

Table D. Data Domain Artifacts

Applications Sub-Architecture Domain

In the applications sub-architecture domain of the EA framework it is important to ask "which systems and applications will be needed to generate, share, and store the data, information, and knowledge that the business services need" and "how can multiple types of IT systems, services, applications, databases, and web sites be made to work together where needed?" Also, "how can configuration management help to create a cost-effective and operationally efficient common operating environment (COE) for systems and applications? Additionally, "what are the workforce, standards, and security issues in this sub-architecture view?" Finally, "what are the workforce, standards, and security issues in this domain?" Table E provides core and elective artifacts in the applications sub-architecture domain:

	Application Sub-Architecture Domain
A-1	Application Interface Diagram (core)
A-2	Application Communication Diagram
A-3	Application Interface Matrix
A-4	Application Data Exchange Matrix
A-5	Application Service Matrix
A-6	Application Performance Matrix
A-7	System/Application Evolution Diagram
A-8	Enterprise Service Bus Diagram
A-9	Application Maintenance Procedure
A-10	Application Inventory
A-11	Software License Inventory

Table E. Application Domain Artifacts

Infrastructure Sub-Architecture Domain

In the infrastructure sub-architecture domain of the EA framework it is important to ask "what types of voice, data, mobile, and video networks will be required to host the IT systems/applications and to transport associate, data, images, and conversations", as well as "what type of physical infrastructure is needed to support the networks" (e.g. buildings, server rooms, points of presence, and other equipment). It is also important to ask "will highly scalable cloud computing environments be needed and if so will the organization be a provider or consumer" and "how can these networks be integrated to create a cost-effective and operationally efficient hosting environment" as well as "will these networks extend beyond the enterprise" and "what are the physical space and utility support requirements for the networks." Will cloud-based concepts be used (virtualization, scaling, metering)? Finally, "what are the workforce, standards, and security issues in this sub-architecture domain?"

Table F provides core and elective artifacts in the infrastructure sub-architecture domain:

	Infrastructure Sub-Architecture Domain
I-1	Network Diagram (core)
I-2	Hosting Concept of Operations
I-3	Technical Standards Profile
I-4	Technology Forecast
I-5	Cable Plant Diagram
I-6	Wireless Connectivity Diagram
I-7	Rack Elevation Diagrams (front and back)
I-8	Data Center/Server Room Diagram
I-9	Wiring Closet Diagram
I-10	Point of Presence Diagram
I-11	Asset Inventory
I-12	Facility Blueprints

Table F. Infrastructure Domain Artifacts

Security Sub-Architecture Domain

The security sub-architecture pervades all of the other five areas of the EA framework because security and privacy controls, to be most effective, need to be "built into" service workflows, data flows, systems, applications, and host networks. This is also true for standards and workforce skills and is why it was the final question in each of the other domain areas. Table G provides core and elective artifacts in the security domain:

	Security Sub-Architecture Domain
SP-1	Security Controls Catalog (core)
SP-2	Security and Privacy Plan
SP-3	Certification & Accreditation Documentation
SP-4	Continuous Monitoring Procedures
SP-5	Disaster Recovery Plan
SP-6	Continuity of Operations Plan

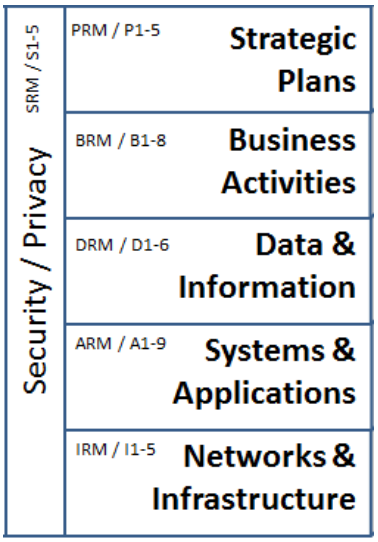
Table G. Security Domain Artifacts

REFERENCE MODELS

There are six reference models in the common approach to Federal EA:

- Performance Reference Model - PRM
- Business Reference Model - BRM
- Data Reference Model - DRM
- Application Reference Model - ARM
- Infrastructure Reference Model - IRM
- Security Reference Model - SRM

These reference models are taxonomies that provide standardized categorization for strategic, business, and technology models and information. This supports analysis and reporting across agency EAs and each of the documentation domains.



Each reference model will have its own taxonomy, methods, touch points, and use cases. The associated meta-model will illustrate the relationship between the reference models, with the use cases providing examples of how each reference model can be applied.

Performance Reference Model

The Performance Reference Model (PRM) supports architectural analysis and reporting in the strategy sub-architecture view of the overall EA. The PRM is both a taxonomy and a standard method for performance measurement as it provides for a common approach to performance and outcome measurements throughout the Executive Branch of the Federal Government, as is required by the Government Performance and Results Modernization Act of 2010 (Public Law 111-352). The PRM allows agencies to better manage the business of government at a strategic level, by providing a means for using the EA to measure the success of investments and their impact on strategic outcomes. The PRM accomplishes these goals by establishing a common language to describe the outputs and measures used to achieve strategic objectives through coupled business services (mission and support). The PRM shows the linkage between internal business components and the achievement of business and customer-centric outputs and outcomes. Most importantly, the PRM helps to support planning and decision-making based on comparative determinations of which programs and services are more efficient and effective. The PRM focuses on three main objectives:

- Produce enhanced performance information to improve strategic and daily decision-making;
- Improve the alignment and better articulate the contribution of inputs to outputs, thereby creating a clear "line of sight" to desired results; and
- Identify performance improvement opportunities that span traditional organizational structures and boundaries.

The PRM structure is designed to clearly express the cause–and-effect relationship between inputs and outputs. This line of sight is articulated through the PRM's hierarchical taxonomy and the use of "Measurement Area", "Category", "Grouping", and "Indicator" information areas, as well as a representation of related organizational units at the Department, Bureau (sub-agency), Line of Business (operating unit), and Program levels.

Business Reference Model

The Business Reference Model (BRM) supports architectural analysis and reporting in the business services sub-architecture view of the overall EA. This updated version of the BRM (v3.0) combines prior versions of the Business Reference Model and the Service Reference Model, so as to now be able to directly map an organization's lines of business and business activities to services within and between Federal Government organizations. The BRM provides a functional view rather than a structural (organization chart) view of Federal Government organizations and their lines of business, including mission and support business services. The BRM describes an organization through a taxonomy of common (shared) mission and support service areas instead of through a stove-piped single organizational view. The BRM therefore promotes intra- and inter-agency collaboration and serves as the underlying foundation for sector and federal-wide shared services strategies.

Data Reference Model

The Data Reference Model (DRM) is the supporting foundation for the overall EA with a focus on two core questions: What information is available for sharing and re-use, and what are the information gaps needing correction? The DRM is designed to provide a flexible common framework for effective sharing of government information across organizational boundaries, increase integration and re-use opportunities, and support semantic interoperability while respecting security, privacy, and appropriate use of that information. It enables agencies to manage information as national assets to better serve the American public and meet mission needs. As a catalyst, the DRM multiplies the value of existing data holdings residing in "silos" through better discovery and understanding of

the meaning of the data, how to access it, and how to work it to support performance results.

The DRM provides a standard means by which data may be described, categorized, and shared. These are reflected within each of the DRM's three standardization areas:

- Data Description: Provides a way to uniformly describe data to convey meaning, thereby supporting its discovery and sharing;
- Data Context: Facilitates discovery of data through an approach to the categorization of data according to taxonomies. Additionally, enables the definition of authoritative data assets within a Common operating environment; and
- Data Sharing: Supports the access and exchange of data where access consists of ad-hoc requests (such as a query of a data asset), and exchange consists of fixed, reoccurring transactions between parties. This is enabled by capabilities provided by both the Data Context and Data Description standardization areas.

Application Reference Model

The Application Reference Model (ARM) supports architectural analysis and reporting in the applications sub-architecture view of the overall EA. The ARM is a component-driven taxonomy that categorizes the system and application related standards and technologies that support and enable the delivery of service components and capabilities. It also unifies existing agency application portfolios and guidance on standard desktop configurations by providing a foundation to advance the reuse and standardization of technology and service components from a Federal Government perspective.

Aligning agency capital investments to the ARM leverages a common, standardized vocabulary, allowing interagency discovery, collaboration, and interoperability. Agencies and the Federal Government will benefit from economies of scale by identifying and reusing the best solutions and technologies for applications that are developed/provided or subscribed to support their business functions, mission, and target architecture.

Infrastructure Reference Model

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

standardization of technology and service components from a Federal Government perspective.

Aligning agency capital investments to the IRM leverages a common, standardized vocabulary, allowing interagency discovery, collaboration, and interoperability. Agencies and the Federal Government will benefit from economies of scale by identifying and reusing the best solutions and technologies for applications that are developed/provided or subscribed to support their business functions, mission, and target architecture.

Security Reference Model

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

- Provides a roadmap that assists agencies in integrating IT security/privacy with EA;
- Provides a mechanism for identifying security and privacy requirements;
- Promotes inclusion of security and privacy in business activities and processes;
- Integrates the NIST "Risk Management Framework" and the organization's system development life cycle processes to ensure that relevant security and privacy requirements are integrated and continuous monitoring is implemented; and
- Helps program executives understand how the Federal Information Processing Standards (FIPS) 199 of confidentiality, integrity, and availability and the eight privacy Fair Information Practice Principles (FIPPs) fit within enterprise architecture planning, while leveraging standards and services that are common to the enterprise and the government.

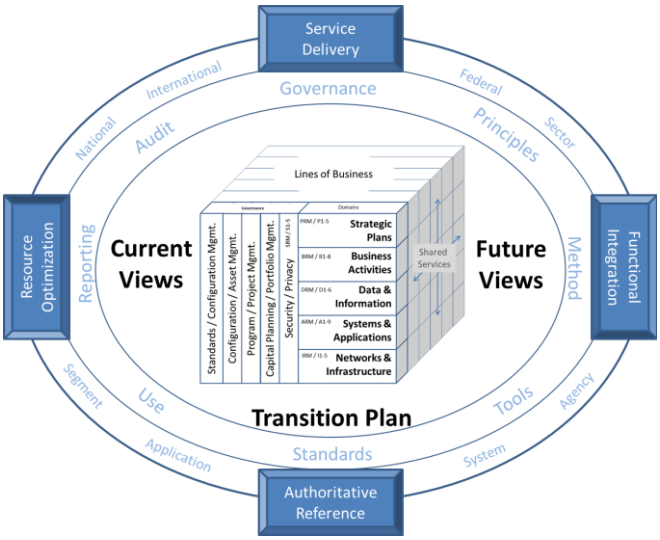
Federal Government organizations are mandated to implement both security and privacy protections for federal information and information systems. The SRM demonstrates how intertwined these two requirements are in the design and implementation of a federal architecture. All too often, security and privacy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

PLANS AND VIEWS

In the common approach, there is one enterprise roadmap for the overall enterprise, and one transition plan / two views for each architecture project:

- Enterprise Roadmap
- Transition Plan
- Current Views
- Future Views

The roadmap, plan and views provide a picture of the architecture in terms of what exists currently, what is planned for the future, and what the transition paths will be in all six domains.



Enterprise Roadmap

The Enterprise Roadmap (Roadmap) documents and maps the organization's strategic goals to business services, integrating technology solutions across all of the Agency's lines of business. The Roadmap discusses the overall EA and identifies performance gaps, resource requirements, planned solutions, transition plans, and a summary of the current and future architecture. The Roadmap also describes the EA governance process, the implementation methodology, and the documentation framework. The Roadmap should be a living document that is updated at regular intervals (at least annually) to provide clear version control for changes in current and future views of Agency changes at all levels of scope. The Roadmap should be archived in the on-line EA repository to support easy access to the information and to promote the linkage of EA to other management and technology processes. To support the annual Federal Budget process, each Federal Agency will submit an updated Enterprise Roadmap to OMB's Office of E-Government and IT on or before April 1st [10] so that it can serve as an authoritative reference for IT portfolio reviews using the PortfolioStat methods/tools and for program-level analysis and planning.

EA Program Management Section

[10] Except in 2012, when the agency Enterprise Roadmaps are due to OMB on or before August 31, 2012.

EA as a management program supports policy development, decision-making, and the effective/efficient use of resources. This section of the Roadmap documents the activities associated with administering EA as an ongoing program.

Governance and Use: This section of the Roadmap documents the way that policy and decision-making will occur within the EA program. It is also where the underlying principles of the EA program are articulated. EA governance is perhaps best described through a narrative that provides EA program policy and an accompanying flow chart that shows how and when decisions are made on EA issues such as IT investment proposals, project reviews, document approvals, and standards adoption/waivers. Examples of EA use include: (1) the degree to which the architecture promotes the open sharing of information, (2) level of stakeholder participation, (3) promoting the recognition that IT is normally a means and not an end in itself, (4) an emphasis on using commercial products that are based on open standards, (5) identification of areas of waste and duplication, and (6) a recognition that EA adds value for planning, decision-making, and communication.

Support for Strategy and Business: This section of the Roadmap emphasizes that one of the main purposes of the EA program is to support and improve the enterprise's strategic and business planning, as well as to identify performance gaps that architectural designs can help close. By showing how resources are being currently used, and identifying useful new processes and technologies at each level of the framework, improvements in performance can occur that are captured in future EA views. For EA to be recognized as part of Agency's strategic planning process, executives and managers must see the value of the EA program in promoting outcomes that matter to them.

EA Roles and Responsibilities: This section of the Roadmap documents roles and responsibilities of EA stakeholders, an example of which is provided in Table H:

Position	Role	Responsibilities
Agency Head	Executive Sponsor	Champion the EA program as a valuable methodology and authoritative reference. Approve resources. Assist in resolving high-level architecture issues.
Chief Information Officer (CIO)	Executive Leadership and Decision-Making	Work with the Agency Head, CXOs, business unit managers, and program managers to gain/maintain support for the EA program. Provide guidance and resources to the Chief Architect. Lead the resolution of high-level EA issues. Integrate EA with other areas of business and technology governance.
Other CXOs	Executive Support	Participate in EA Program governance. Promote the EA as an authoritative reference. Use EA information and products in planning / decision-making.
Chief Architect	Program	Manage the EA Program. Identify EA methods and standards. Coordinate architecture projects. Lead the configuration

	Management	management process.
Enterprise Architect	Architecture Integration	In coordination with the Chief Architect, works with executives, managers, staff to identify requirements and solutions in all domains and levels of scope.
Solution Architect	Problem Solving	In coordination with the Chief Architect, and/or an Enterprise Architect, works collaboratively with stakeholders to identify solutions for business and technology requirements. Does analysis/documentation.
Strategic Planner	Direction and Prioritization	In coordination with Agency leadership and other stakeholders, including the Chief Architect, works collaboratively to update strategic plans and priority goals, and identifies linkages to program activities.
Business Architect	Process Analysis and Design	In coordination with the Chief Architect and other architects, works collaboratively with stakeholders to create, improve, or re-engineer business processes and identify enabling IT. Does analysis/documentation.
Data Architect	Data Analysis and Design	In coordination with the Chief Architect and other architects, works collaboratively with stakeholders to provide technical analysis and design for data-level solution architecture projects and data-related business and technology requirements. Ensures that data solutions meet integration, interoperability, privacy requirements. Does analysis/documentation.
Systems Architect	Systems Analysis and Design	In coordination with the Chief Architect and other architects, works collaboratively with stakeholders to provide technical analysis and design support for systems-level architecture projects. Ensures that IT systems meet integration and interoperability requirements. Does analysis/documentation.
Infrastructure Architect	Network Analysis and Design	In coordination with the Chief Architect and other architects, works collaboratively with stakeholders to provide technical analysis and design support for infrastructure-level architecture projects. Ensures that IT network and data center hosting solutions meet integration and interoperability requirements. Does analysis/documentation.
Security Architect	Security and Privacy Analysis and Design	In coordination with the Chief Architect and other architects, works collaboratively with stakeholders to provide technical analysis and design for security-related architecture projects and security or privacy-related business and technology requirements. Ensures that security and privacy solutions support risk mitigation plans. Does analysis/documentation.
Line of Business Managers	Requirements Identification	Supports EA program and ensures that program managers participate in architecture projects by identifying business and IT requirements for program activities.
Program Managers	Requirements Identification	Participates in architecture projects and configuration management activities. Identifies business and IT requirements for program activities.
Capital Planner	Investment Analysis	Uses EA information to support the development of alternatives analyses and to make investment decisions.
Functional Expert	Subject Matter Expertise	Participates in architecture projects to provide subject matter expertise in a functional requirement area.
End-User Representative	Requirements Identification	Participates in architecture projects. Identifies business and IT requirements for systems/applications.
Tool Expert	Documentation Support	Documentation support and maintenance of EA tools. Supports architecture projects and the repository.
Repository Manager	Repository Support	Maintenance of EA website and repository, associated content, and links to other websites as needed.

Table H. Example Roles and Responsibilities

EA Program Budget: This section of the Roadmap documents the budget for the EA program and projects by fiscal year and over the total lifecycle, so that the total cost of ownership (TCO) is identified. While EA program is ongoing, a lifecycle period of five years is recommended to be able to calculate TCO. In general, the costs to be included are those for EA program start-up and operation, salaries and work facilities for the EA team, the initial documentation of the EA, periodic updates to the EA, annual updates to the Roadmap, EA tool purchase and support, and EA repository development and maintenance. The initial estimate of these costs represents the "baseline" for EA program funding. Spending during the lifecycle should be tracked against this baseline to promote effective management of the EA program. If changes in the scope of the EA program occur, a corresponding change in the funding baseline should also be made.

EA Program Performance Measures: This section of the Roadmap documents how the effectiveness and efficiency of the EA program will be measured. As was described in previous Chapters, there are two types of measures: outcome and output. Outcome measures identify progress being made toward some new end-state, such as better EA component integration, increased application end-user satisfaction, or more effective IT investment decision-making. Output measures provide data on activities and things, such as how many databases exist, how many e-mail are sent each day, or how closely an IT project is meeting baseline estimates for cost, schedule, and performance. Outcome measures often have both quantitative and qualitative elements to them, while output measures are usually quantitative in nature. While output measures are important for indicating progress in an initiative area, it is the attainment of outcomes that correlate to goal attainment, which is the most important thing to an enterprise. It is important to be able to measure the attainment of outcomes, so that the positive effects (added value) of the EA program can be identified.

Summary of Current Architecture

One of the purposes of the Enterprise Modernization Roadmap is to show an overview of the linkage between current services and resources in each area of the EA. In this way, the present role of IT within the enterprise is better understood and can be further analyzed from either a top-down, or bottom-up perspective. The objective of this part of the Roadmap is not to duplicate the extensive documentation that is available in the repository, but to provide an integrated view of current business activities and supporting technology solutions. This information sets the

stage for the next section of the Roadmap, which discusses future changes in the architecture to achieve improved performance and efficiency.

Strategic Goals and Initiatives: This section of the Roadmap identifies how the EA program and specific resources support the attainment of the Agency's strategic goals and initiatives. This section builds upon comments provided in the Strategic Plan, and is included to more clearly show which business activities and IT resources are involved in each strategic goal area. A general description is then provided of how IT components support each goal and initiative at the strategic level of the EA.

Business Services and Information Flows: This section of the Roadmap identifies and emphasizes the role that EA plays in supporting business process analysis and improvement, as well as identifying and optimizing information flows within and between these processes. It also re-affirms the EA principle that IT resources are a means to enable effective business services, and should not be procured unless there is a strong business case that supports investment. Within this section, the organization's main LOBs should be listed along with the key business services and associated information flows in each business unit and program area. A general description is then provided of how IT resources support mission and support services process at the business level of the EA. Selected models of information flows and data structure may also provided.

Applications: This section of the Roadmap identifies how current EA artifacts at the applications level of the EA support the information flows that are required for program activities throughout the Agency. The discussion should summarize how well this "suite" of commercial and custom developed IT systems and front/back office services provide the functionality the enterprise needs for mission and support. This can range from large scale, multi-module ERP solutions, to commercial applications and databases, to small custom-developed websites. Comments should focus on degree of integration, potential scalability, user satisfaction, and any reliance on proprietary solutions or outsourced services (e.g., cloud hosting services).

Infrastructure: This section of the Roadmap discusses the voice, data, video, and mobile hosting environments that make up the infrastructure level of the EA. The discussion should focus on how well these internal and external networks, systems, and cable plants integrate to create a "seamless" infrastructure. Comment should also be made on convergence activities to

consolidate the infrastructure where there is duplication in voice, data, video, and mobile solutions, as well as other commodity IT services at this level of the architecture (e.g., email, collaboration, help desk, asset management).

Security and Privacy. This section of the Roadmap discusses the general approach to IT security and data privacy at all levels of the EA framework. IT security should be part of any strategic goal or initiative that depends on accurate, properly authenticated information. High-level descriptions are provided on how security is built into business services and the control of information flows, as well as the design and operation of systems, services, and networks. Specific IT security information should not be part of the Roadmap because it could reveal vulnerabilities. This type of information should be documented in a separate IT Security Plan that only certain people in the Agency have access to.

Standards. The standards section of the Roadmap documents the business standards for mission and support services as well the technical standards for systems, applications and infrastructure, including voice, data, video, mobile and IT security solutions that are used during architecture development. The standards section can also provide a list of preferred vendors and products that meet the technical standards that an Agency adopts. EA standards are a key element of the configuration management (CM) process and come from international, national, local, government, industry, and enterprise sources. Selected standards should include standards for voice, data, and video technologies from leading standards bodies throughout the world, including the Institute of Electrical and Electronics Engineers (IEEE), the National Institute of Science and Technology (NIST), the International Enterprise for Standardization (ISO), the European Committee on Standardization (CEN), the Object Management Group (OMG), and the Federal law and guidance on EA.

Workforce Requirements. This section of the Roadmap describes required changes to knowledge and skill requirements. People are often the most valuable resource that any organization has, and human capital management plans should detail training requirements and position description changes that are needed to support changes in mission and support areas.

Summary of Future Architecture

The future architecture section of the Enterprise Modernization Roadmap should be based on a number of alternative operating scenarios, in recognition of the fact that no Agency can predict what the particular combination of internal and external conditions will be as time goes on, especially several years into the future.

Future Operating Scenarios. In this section, the future operating scenarios are presented along with a narrative description of the purpose of the scenarios and the spectrum of operating environments that the scenarios respond to. For example, three scenarios are presented with an opening narrative that explains that they represent:

Scenario 1: Continuing with the status quo.
Scenario 2: An expansion/update strategy when resources are available.
Scenario 3: A defensive strategy in the face of decreasing budgets.

Each scenario has planning assumptions built into it, that highlight changes that will need to occur in processes, people, and technology. In this section, a description is provided of the selected course of action for the Agency.

Planning Assumptions. The planning assumptions from the scenarios are further discussed in terms of what they mean to the priorities of the Agency as it implements the future EA. The assumptions identify new capabilities and resources that will be needed if the Agency is to be successful in each scenario. This section then focuses on the selected scenario and the planning assumptions that will underlie that course of action. Continuing the example from above, if Scenario 2 is being pursued, then several new shared services and related systems may need to be built or subscribed to. The planning assumptions that were identified in Scenario 2 become the guideposts for decisions about how to change the current EA, which needs to be described.

Updating Current and Future Views. Documentation of planned changes in processes and resources is what creates the future views of the EA at all levels of the framework. Using the EA as an example, these updates should be accomplished in a "top-down" manner, to preserve the emphasis on strategy and business, and to maintain the logic of the documentation's relationships. Therefore, these updates would begin with the organization's strategic goals and initiatives.

Changes to the Agency's Strategic Plan and priority goals are made periodically or in response to a significant new internal or external business

or technology drivers. Most strategic plans are intended to last several years, with associated goals, initiatives, and measures changing very little. Priority goals, initiatives, and measures should be considered as exchangeable resources. This means that a goal or measure can be added, dropped, or modified without nullifying the entire strategic plan.

A similar approach is used to review and update the Agency's business services at the second level of the EA. It is important to ensure that the current views of business services are complete and can show how they support the accomplishment of current strategic goals. The changes in mission or support services then can be made considering any changes in strategic goals, initiatives, and measures that may be planned and documented at the top level of the EA. Also, documentation at the business level of the EA should show future planning for more effective, cost-efficient, and technically integrated processes.

Documenting changes to the flow of information within and between mission and support services (and new data standards) will enable EA planners to select shared services at these two lowest levels of the EA that best support the information flows and data standards. A focal point for the discussion in this section of the Roadmap is to identify any current performance gaps that exist at the higher levels of the EA and map them to current EA components and products. The future view of the applications level of the EA should show which systems or services will be changing and in what timeframe via that is developed as part of each architecture project.

At the infrastructure level of the EA, future changes will reflect systems and shared services that will provide a more robust, reliable, secure voice, data, and video backbone transport capability. Interoperability, cost-effectiveness and open standards are additional factors to be considered.

Modernization: The modernization section of the Roadmap summarized the Transition Plans from the various architecture projects. This section documents the tasks, milestones, and timeframe for implementing new systems and services. Large and mid-size Agencies often have many new development, upgrade, retirement, or migration projects underway at any given time and these require coordination to establish the optimal sequencing of activities. Sometimes there are dependencies between projects that also require proper sequencing. For example, an improvement to the capacity of the data infrastructure may be required before additional systems and/or

databases can be effectively hosted so that maximum performance can be attained. Another example is the consolidation of IT resources such as systems, applications, and databases to improve both performance and cost effectiveness.

Configuration Management: The Configuration Management (CM) section of the Roadmap serves to support the sub-process by which changes to the EA are managed and standards are applied. Changes to the EA include the addition, upgrade, retirement of applications, systems, and services. CM ensures that (1) a standardized process is used in reviewing proposed changes, (2) technical standards for voice, data, and video are followed or waived, (3) there is a documented waiver process, (4) waivers have specific time limits, so that EA standards are eventually realized, (5) there is enforcement for EA documentation version control. The CM process should be overseen by the Chief Architect, and be supported by a working group that includes stakeholders from all EA domains and business units/programs throughout the organization.

IT Asset Inventory

The Enterprise Roadmap will include an inventory of all of the agency's IT applications, systems and services, using the definitions of these resources that are provided in this document, OMB Circulars A-11 and A-130, as well as OMB Memoranda 11-29 and 12-10.

APPENDIX A

Terms and Definitions [11]

Actionable means architecture analysis and documentation that is used by executives, managers, and staff to support resource planning, decision-making, and management.

Agency means any executive department, military department, bureau, government corporation, government-controlled corporation, independent regulatory agency, or other organization in the Executive Branch of the United States Federal Government.

Alignment means conformance to a policy, standard, and/or goal.

Architecture means a systematic approach that organizes and guides design, analysis, planning, and documentation activities.

Architecture Segment means a part of the overall EA that documents one or more lines of business, including all levels and threads.

Artifact means a documentation product, such as a text document, diagram, spreadsheet, briefing slides, or video clip.

Application Reference Model (ARM) version 1.0 is one of six reference models of the Federal Enterprise Architecture (FEA) version 2.0. It is a classification taxonomy used to describe the type of software applications in a particular architecture at the system, segment, agency, sector, federal, national, or international level. The ARM can help to identify opportunities for collaboration, shared services, and solution reuse in agency IT portfolios and inter-agency Lines of Business.

Baseline Architecture is the set of products that portray the existing enterprise, the current business practices, and technical infrastructure. Commonly referred to as the "As-Is" architecture

Business Case means a collection of descriptive and analytic information about an investment in resource(s) and/or capabilities.

Business Reference Model (BRM) version 3.0 is one of six reference models of the Federal Enterprise Architecture (FEA) version 3.0. It is a classification taxonomy used to describe the type of business functions and service types in a particular solution architecture at the system, segment, agency, sector, federal, national, or international level. The taxonomy identifies business function and sub-function areas as well as related services that are performed within and between federal agencies and with external partners. The BRM can help to identify opportunities for collaboration, shared services, and solution reuse in agency IT portfolios and inter-agency Lines of Business.

Capital Planning and Investment Control (CPIC) means the same as capital programming and is a decision-making process for ensuring 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. CPIC includes a management process for ongoing identification, selection, control, and evaluation of investments in IT. The CPIC process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.

Change Management means the process of setting expectations and involving stakeholders in how a process or activity will be changed, so that the stakeholders have some control over the change and therefore may be more accepting of the change.

Chief Information Officers Council (CIO Council) refers to the Federal CIO Council that was established in the E-Government Act of 2002.

[11] Sources: E-Gov Act of 2002, OMB Circular A-11 (July 2011), OMB Circular (November 2001) and other publications.

Composite means an artifact that uses several documentation modeling techniques and/or represents several types of EA components.

Configuration Management means the process of managing updates to business and technology resources (e.g., processes, systems, applications, and networks) to ensure that security controls are operating effectively and that standards are being followed.

Crosscutting Segment serves several Lines of Business within or between agencies. Examples include email systems that serve the whole enterprise, and financial systems that serve several lines of business.

Culture means the beliefs, customs, values, structure, normative rules, and material traits of a social organization. Culture is evident in many aspects of how an organization functions.

Current View means a collection of artifacts that represent processes and technologies that currently exist in the enterprise.

Data refers to an elementary description of things, events, activities, and transactions that are recorded, classified, and stored, but not organized to convey any specific meaning. Data items can be numeric, alphabetic, figures, sounds, or images. A database consists of stored data items organized for retrieval.

Data Reference Model (DRM) version 2.0 is one of six reference models of the Federal Enterprise Architecture (FEA) version 2.0. It is a classification taxonomy used to describe the context for information exchanges and the type of data entities and attributes in a particular solution architecture at the system, segment, agency, sector, federal, national, or international level. The DRM can help to identify opportunities for collaboration, shared services, and solution reuse in agency IT portfolios and inter-agency Lines of Business.

Electronic Government means the use by the Federal 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.

Enterprise means an area of common activity and goals within an organization or between several organizations, where information and other resources are exchanged.

Enterprise Architecture means a strategic information asset base, which defines the mission; the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture, a target architecture, and a sequencing plan.

Enterprise Roadmap refers to the document that is produced at least annually by the organization responsible for the enterprise (usually a Federal Agency) and which describes the current and future views of the enterprise-wide architecture, how changes occur, and how the EA program functions.

Executive Agency has the meaning defined in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

Federal Enterprise Architecture (FEA) is a business-based documentation and analysis framework for government-wide improvement. The FEA allows agencies to use standardized methods to describe the relationship between an agency's strategic goals, business functions, and enabling technologies at various levels of scope and complexity. The FEA is comprised of a framework for documentation in six domain areas (strategic goals, business services, data and information, systems and applications, infrastructure, and security) and six reference models areas that are designed to facilitate standardized analysis, reporting, and the identification of duplicative investments, gaps, and opportunities for collaboration within and across federal agencies. The FEA method is based on a 5-step repeatable method for solution architecture that can be used at various levels of scope and provides current views, future views, and a transition (sequencing) plan.

Federal IT Dashboard is a website enabling federal agencies, industry, the general public and other stakeholders to view details including performance for federal information technology investments.

Framework means a structure for organizing information that defines the scope of the architecture (what will be documented) and how the areas of the architecture are related.

Future View means a collection of artifacts that represent processes and technologies that do not yet exist in the enterprise.

Governance means a group of policies, decision-making procedures, and management processes that work together to enable the effective planning and oversight of activities and resources.

Government Information means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

Government Publication means information which is published as an individual document at government expense, or as required by law. (44 U.S.C. 1901)

Horizontal Segment means a crosscutting process, program, or resource that serves several Lines of Business.

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Life Cycle means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Information Management means the planning, budgeting, manipulating, and controlling of information throughout its life cycle.

Information Resources includes both government information and IT.

Information Resources Management means the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and IT.

Information Resource Management Strategic Plan is strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency's IRM strategic plan as required by 44 U.S.C. 3506(b) (2). IRM strategic plans should conform to guidance provided annually in OMB Circular A–11, provide a description of how IT management activities help accomplish agency missions delivery area and program decision, and ensure decisions are integrated with management support areas including organizational planning, budget, procurement, financial management, and HR.

Information Security involves all functions necessary to meet federal Information Security policy requirements. It includes the development, implementation and maintenance of security policies, procedures and controls across the entire information lifecycle. This includes implementation and activities associated with NIST SP-800-37, Security Awareness training, SP-800-39 regarding the implementation of a Risk Management Framework and continuous monitoring, SP-800-53A security controls, and FISMA compliance reporting, development of security policy, and security audits and testing.

Information System means a discrete set of IT, 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 in accordance with defined procedures, whether automated or manual.

Information System Life Cycle means the phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

Information Technology (IT) means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by an executive agency. IT is related to the terms Capital Asset, IT Investment, Program, Project, Sub-project, Service, and System.

Information Technology Investment means the expenditure of IT resources to address mission delivery and management support. An IT investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality and the subsequent operation of those assets in a production environment. While each asset or project would have a defined life-cycle, an investment that covers a collection of assets intended to support an ongoing business mission may not.

Infrastructure Reference Model (IRM) version 1.0 is one of six reference models of the Federal Enterprise Architecture (FEA) version 2.0. It is a classification taxonomy used to describe the type of voice, data, video, cloud, and mobile host environments in a particular solution architecture at the system, segment, agency, sector, federal, national, or international level. The IRM can help to identify opportunities for collaboration, shared services, and solution reuse in agency IT portfolios and inter-agency Lines of Business.

Interoperability means the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner.

Knowledge consists of data or information that have been organized and processed to convey understanding, experience, accumulated learning, and expertise as they apply to a current problem or activity. Data that are processed to extract critical implications and to reflect past experience and expertise provide the recipient with organizational knowledge, which has a very high potential value.

Line of Business (LOB) means a specific operating unit or shared service that exists within or between agencies. LOBs are also OMB-authorized service providers for the Federal Government, managed by designated executive agencies.

Major Investment means a program requiring special management attention because of its importance to the mission or function of the agency, a component of the agency, or another organization; has significant program or policy implications; has high executive visibility; has high development, operating, or maintenance costs; is funded through other than direct appropriations; or is defined as major by the agency's capital planning and investment control process. OMB may work with the agency to declare other investments as major investments. Agencies should consult with the respective OMB agency budget officer or analyst about what investments to consider as "major" and for those an OMB Circular A-11 Exhibit 300 annual submission is required. IT investments not considered "major" are categorized in the annual Exhibit 53 IT budget request submission as "non-major."

Managing Partner represents the agency designated as the lead agency responsible for coordinating the implementation of the E-Gov or Line of Business (LoB) initiative. The managing partner is also responsible for coordinating and submitting the Exhibit 300 for the initiative and the Exhibit 300 will be represented as part of the managing partner's budget portfolio. Please refer to the OMB MAX portal for additional information on managing partner reporting requirements for IT investments.

Meta Context is the highest level context for understanding an idea, design, enterprise.

Methodology (sometimes called "approach") refers to the repeatable process by which architecture documentation will be developed, archived, and used; including the selection of principles, a framework, modeling tools, artifacts, repository, reporting, and auditing.

Mission Statement is a succinct description of why the enterprise exists.

New IT Investment means an IT investment and its associated projects newly proposed by the agency that has not been previously funded by OMB. This does not include investments existing within the agency that have not previously been reported to OMB.

National Security System means any telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Non-Major Investment means an IT investment not meeting the definition of major as defined above but is part of the agency's IT Portfolio. All non-major investments are reported on the Exhibit 53.

On-Going Investment means an investment and its associated assets, including both maintenance projects and operations that have been through a complete budget cycle with OMB with respect to the President's Budget for the current year.

Operations mean the day-to-day management of an asset in the production environment and include activities to operate data centers, help desks, data centers, telecommunication centers, and end user support services. Operational activities for major IT investments are reported through Section C of the Exhibit 300B. Operational costs include the expenses associated with an IT asset that is in the production environment to sustain an IT asset at the current capability and performance levels including Federal and contracted labor costs; and costs for the disposal of an asset.

Operations and Maintenance (O&M) means the phase of an asset in which the asset is in operations and produces the same product or provides a repetitive service. O&M is the same as "steady state."

Partner Agency represents the agency for an E-Gov or LOB initiative designated as an agency that should provide resources (e.g., funding, FTEs, in-kind) to the management, development, deployment, or maintenance of a common solution. The partner agency is also responsible for including the appropriate line items in its Exhibit 53 reflecting the amount of the contribution for each of the E-Gov or LOB initiatives to which it is providing resources.

Performance Gap is an identified activity or capability that is lacking within the enterprise, which causes the enterprise to perform below desired levels or not achieve strategic or tactical goals.

Performance Reference Model (PRM)) supports architectural analysis and reporting in the strategy sub-architecture view of the overall EA. The PRM allows agencies to better manage the business of government at a strategic level, by providing a means for using the EA to measure the success of investments and their impact on strategic outcomes. The PRM shows the linkage between internal business components and the achievement of business and customer-centric outputs and outcomes. This line of sight is articulated through the PRM's hierarchical taxonomy and the use of "Measurement Area", "Category", "Grouping", and "Indicator" information areas.

Primitive means an artifact that uses one modeling technique to describe one type of EA component.

Privacy Impact Assessment (PIA) is a process for examining the risks and ramifications of using information technology to collect, maintain and disseminate information in identifiable form from or about members of the public, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information. Consistent with OMB M–03–22, implementing the privacy provisions of the E-Government Act, agencies must conduct and make publicly available PIAs for all new or significantly altered IT investments administering information in identifiable form collected from or about members of the public.

Program means an ongoing set of activities and projects managed in a coordinated way.

Project means a temporary activity to create a unique product, service, or result.

Quality Assurance is the systematic monitoring and evaluation of the various aspects of a project, service or facility to maximize the probability that standards of quality are being attained by the production process.

Records includes all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference and stocks of publications and of processed documents are not included.

Records Management means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

Reference Architecture is an authoritative source of information about a specific subject area that guides and constrains the instantiations of multiple architectures and solutions.

Security Reference Model (SRM) version 1.0 is one of six reference models of the Federal Enterprise Architecture (FEA) version 2.0. It is a classification taxonomy used to describe the type of security controls in a particular architecture at the system, segment, agency, sector, federal, national, or international level. The SRM can help to identify opportunities for collaboration, shared services, and solution reuse in agency IT portfolios and inter-agency Lines of Business.

Segment Architecture is a detailed, results-oriented architecture (baseline and target) and a transition strategy for a portion or segment of the enterprise. Segments are individual elements of the enterprise describing core mission areas and common or shared business services and enterprise services. They provide the core linkage of the IT Investment Portfolio to the Agency's performance management system. As such, segments are designed to be common across programs that support the same mission area. Increasingly, shared segments will be common across the government and agencies should plan to use approved government-wide shared segments as their target architecture.

Service Consumer means an agency or business unit that receives business or technology service(s) from a Line of Business provider. A service consumer may be either internal or external to the organization responsible for providing services.

Service Oriented Architecture (SOA) is a set of principles and methodologies for designing and developing software in the form of interoperable services

Service Provider means an agency or business unit that provides business or technology service(s) as a Line of Business consumer(s). This includes a discrete set of personnel, IT, and support equipment with the primary function of providing service(s) to more one or more other agencies or business units on a reimbursable basis.

Shared Service means a mission or support function provided by one business unit to other business units within or between organizations.

Solution Architecture is a standardized method of identifying business requirements and viable technology solutions within the context of a single agency's enterprise architecture or a multi-agency sector or government-wide/international architecture. Solution architecture includes current and future views as well as transition plans at a number of levels of scope including applications, systems, segments, enterprise, sector, government-wide, national, and international. The Federal Solution Architecture Methodology (FSAM) is the repeatable process for doing solution architecture through projects at various levels of scope in the federal sector.

Stakeholder means those who are or will be affected by a program, activity, or resource.

System means a tangible IT asset that is comprised of hardware devices, software applications, databases, users, processes, and security controls.

Systems Development Life Cycle (SDLC) is guidance, policies, and procedures, for developing systems throughout their life cycle, including requirements, design, implementation testing, deployment, operations, and maintenance.

Target Architecture is the representation of a desired future state or "to be built" for the enterprise within the context of the strategic direction

Vision Statement is the part of a strategic plan that succinctly describes the competitive strategy of the enterprise.

Web-enabled means applications and services that are accessed through a web browser and function through an internal and/or external Internet-protocol based collaboration environment (e.g., Internet, local area network, wide area network, public cloud, private cloud, and hybrid cloud).

APPENDIX B

References

National Institute of Science and Technology (NIST) Federal Information Processing Standard Publication 199: Standards for Security Categorization of Federal Information and Information Systems.

NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems.

NIST Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook.

NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems and Organizations.

NIST Special Publication 53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans.

NIST Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categorization Levels.

Office of Management and Budget (OMB) Circular A-11: Preparation of Federal Budgets, Strategic Plans, Annual Performance Plans/Annual Program Performance Reports, July 2011.

OMB Circular A-76: Performance of Commercial Activities, August 1983.

OMB Circular A-94: Discount Rates to be Used in Cost-Benefit Analysis, October 1992.

OMB Circular A-130: Management of Federal Information Resources, November 2000.

OMB Memorandum M-03-18: Implementation Guidance for the E-Government Act, August 2003.

OMB Memorandum M-03-22: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 2003.

OMB Memorandum M-04-04: E-Authentication Guidance, December 2003.

OMB Memorandum M-04-16: Software Acquisition, July, 2004.

OMB Memorandum M-04-19: IT Project Manager (PM) Qualification Guidance, July 2004.

OMB Memorandum M-04-26: Personal Use Policies and File Sharing Technology, September 2004.

OMB Memorandum M-05-22: Transition Planning for Internet Protocol v6 (IPv6), August 2005.

OMB Memorandum M-05-23: Improving Information Technology (IT) Project Planning and Execution, August 2005.

OMB Memorandum M-05-24: Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees/Contractors, August 2005.

OMB Memorandum M-06-02: Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model, December 2005.

OMB Memorandum M-06-15: Safeguarding Personally Identifiable Information, May 2006.

OMB Memorandum M-06-16: Protection of Sensitive Agency Information, June 2006.

OMB Memorandum M-08-01: HSPD-12 Implementation Status, October 2007.

OMB Memorandum M-08-26: Transition from FTS-2001 to Networx, August 2008.

OMB Memorandum M-08-27: Guidance for Trusted Internet Connection (TIC) Compliance, September 2008.

OMB Memorandum M-09-02: Information Technology Management Structure and Governance Framework, October 2008.

OMB Memorandum M-09-32: Update on Trusted Internet Connections Initiative, September 2009.

OMB Memorandum M-10-22: Guidance for Online Use of Web Measurement and Customization Technologies, June, 2010

OMB Memorandum M-10-23: Guidance for Agency Use of Third-Party Websites and Applications, June 2010

OMB Memorandum M-10-26: Immediate Review of Financial Systems IT Projects June, 2010.

OMB Memorandum M-10-25: Reforming the Federal Government's Efforts to Manage Information Technology Projects, June 2010.

OMB Memorandum M-10-27: IT Investment Baseline Management Policy, June, 2010.

OMB Memorandum M-10-28, Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security, July 2010.

OMB Memorandum M-10-32: Evaluating Programs for Efficacy and Cost Efficiency, July 2010.

OMB Memorandum M-10-31: Immediate Review of IT Projects, July 2010.

OMB Memorandum M-11-02: Sharing Data While Protecting Privacy.

OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors, February 2011.
OMB Memorandum M-11-29: Chief Information Officer Authorities, August 2011.

OMB Memorandum M-12-10: Implementing PortfolioStat, March 31, 2012

United States Government Accountability Office (GAO): Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management v2.0, GAO-10-846G, August 2010.

United States Congress; Government Performance and Results Act of 1993 (Public Law 103-62).

United States Congress; Paperwork Reduction Act of 1995 (Public Law 104-13).

United States Congress; Clinger-Cohen Act of 1996 (Public Law 104-106).

United States Congress; Workforce Investment Act of 1998; Title IV, Rehabilitation Act Amendments, Section 508 (Public Law 105-220).

United States Congress; Government Paperwork Elimination Act of 1998 (Public Law 105-277).

United States Congress; Electronic Signatures in Global and National Commerce Act of 2001 (Public Law 106-229).

United States Congress; E-Government Act of 2002 (Public Law 107-398) includes the Federal Information Security Management Act.

United States Congress; Government Performance and Results Modernization Act of 2011 (P.L. 111-325).