

Federal Enterprise Architecture Security and Privacy Profile

Version 3.0

Sponsored By:

National Institute of Standards and Technology

Office of Management and Budget

**Federal Chief Information Officers Council,
Architecture and Infrastructure Committee**

September 2010

Final

Table of Contents

Table of Contents.....	i
Acknowledgements.....	iii
Section 1.0: Introduction.....	1
Section 1.1: The Federal Enterprise Architecture.....	1
Section 1.2: The FEA-SPP.....	1
Section 1.3: FEA-SPP Governance.....	3
Section 1.4: FEA-SPP, Version 3.0.....	3
Section 1.5: How to Use This Document.....	3
Section 1.6: Target Audience.....	4
Section 2.0: Key FEA-SPP Stakeholders and Management Officials.....	5
Section 3.0: Architecture, Security and Privacy Fundamentals.....	7
Section 3.1: Implementing Security Controls.....	7
Section 3.2: Implementing Privacy Controls.....	11
Section 3.3: The Relationship Between the FEA-SPP and NIST Standards and Guidance.....	14
Section 4.0: FEA-SPP Methodology.....	15
Section 4.1: Stage I – Identification.....	16
Section 4.1.1: Overview.....	16
Section 4.1.2: Activities.....	17
Section 4.2: Stage II—Analysis.....	18
Section 4.2.1: Overview.....	18
Section 4.2.2: Activities.....	19
Section 4.3: Stage III—Selection.....	23
Section 4.3.1: Overview.....	23
Section 4.3.2: Activities.....	26
Section 5.0: Integrating the FEA-SPP with the Federal Enterprise Architecture.....	30
Section 5.1: Enterprise Architecture Overview.....	30
Section 5.2: The Three Levels of Enterprise Architecture.....	31
Section 5.3: The Relationship Between the FEA and the RMF.....	32
Section 5.4: The Relationship Between FEA-SPP and the FEA Reference Models.....	35
Section 5.5: The Enterprise Architecture Perspective on Security and Privacy.....	36
Section 6.0: Integrating Security / Privacy and the FSAM.....	38
Section 6.1: FSAM Overview.....	38
Section 6.2: Using the FSAM to Implement Security & Privacy Controls.....	38
Section 6.3: The Relationship Between FEA-SPP Methodology Process and the FSAM.....	39
Section 6.4: Example: Leveraging the FSAM to Understand and Improve the Enterprise.....	44
Appendix A: The FEA-SPP Assessment Tool.....	1
Appendix B: FEA-SPP History.....	4
Background.....	4
FEA-SPP Version 1.0.....	4
FEA-SPP Version 2.0.....	5
Appendix C: The FEA Reference Models.....	7
Appendix D: The Federal Segment Architecture Methodology.....	9
Appendix E: FSAM Artifacts.....	13

Appendix F: Privacy Control Families – Descriptions and Explanations	23
Glossary	29
References.....	34
Laws.....	34
Executive Policy	34
Federal Standards.....	34
International Standards	34
Guidance	35
Other Resources	35

Acknowledgements

Version 3.0 of the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) was collaboratively developed with the help of subject matter experts from government, industry, and academia. This collaboration strengthened the document significantly in terms of identifying and incorporating best practices from both the public and private sectors while doing so within the context of federal law and guidance on enterprise architecture, information security, data privacy, capital planning, project management, and records management.

During the preparation of Version 3.0 the FEA-SPP Working Group was co-led by Scott Bernard of the U.S. Department of Transportation’s Federal Railroad Administration, Martha Landesberg of the Department of Homeland Security, and Ron Ross of the National Institute of Standards and Technology. Members of the FEA-SPP Version 3.0 Working Group included:

<u>Name</u>	<u>Organization</u>
John Anderson	Cougaar Software, Inc.
Marian Cody	U.S. Dept. of Housing & Urban Development
Dominic Cussatt	U.S. Department of Defense, ASD-NII
Hazem Eldakdoky	OnPoint, Inc.
Roxanne Everetts	LMI Government Consulting
Christopher Feudo	Edgewater Federal Solutions
Bob Haycock	Haycock Strategies, LLC
Waylon Krush	Lunarline, Inc.
John McCue	Executive Office of the President
James McKenzie	PricewaterhouseCoopers, LLP
Dale Meyerrose	Harris Corporation
Norman Milford	U.S. Department of State, Office of EA & Planning
Kenneth Mortensen	Boston Scientific Corporation (former co-lead)
Ping Oberst	U.S. Dept of Justice, U.S. Marshals Service
Tanaia Parker	T. White Parker
Christine Robinson	Christine Robinson & Associates, LLC
Scott Selby	Booz Allen Hamilton
Roanne Shaddox	Federal Deposit Insurance Corporation
Rick Smith	Deloitte, LLP
Joseph Verscharen	Pension Benefit Guaranty Corporation
Scott Ward	GiniCorp

We would like to provide special thanks to Kshemendra Paul at OMB for his support and guidance; to John Gilligan and Sally MacDonald for their prior work in producing Version 2.0 of the FEA-SPP; to Ken Mortensen and Toby Levin for their work with the privacy community and on Version 3.0; to Colleen Coggins for her work on the FSAM and tie-ins to the FEA-SPP; and to each of the working group members and those others who provided input and feedback on the various drafts. This document could not have been completed without the help of these dedicated and knowledgeable individuals.

Dr. Scott Bernard
Deputy CIO, Chief Enterprise
Architect / ISSO, Office of IT,
Federal Railroad Administration,
Department of Transportation

Ms. Martha Landesberg
Associate Director, Privacy
Policy, Privacy Office
Department of Homeland
Security

Dr. Ron Ross
Manager, FISMA
Implementation Project,
National Institute of Standards
and Technology

Document History

The Federal Chief Information Officers Council published the initial version of the *Federal Enterprise Architecture Security and Privacy Profile* (FEA-SPP) in July 2004, with an update in July 2005. Version 2.0 was published in June 2006 and provided modified steps in the methodology that were based on validation exercises and an assessment of related documents. Work on Version 3.0 started in mid-2008 and its release in mid-2010 represented a further update of the methodology as well as incorporation of key concepts from the federal architecture, security, and privacy communities of practice.

The inclusion of concepts from updated policy documents, federal standards, and industry best practices added to the utility of this document. This included the Federal Information Processing Standards Publications (FIPS PUB) 199: *Standards for Security Categorization of Federal Information and Information Systems*; FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*; and the FEA's *Data Reference Model* (DRM). FEA-SPP Version 3.0 supersedes previous FEA-SPP releases and incorporates updates to IT security, privacy, and risk management procedures and practices contained in the National Institute for Standards and Technology (NIST) Special Publications (SP) 800-37, SP-800-39, SP-800-53, SP-800-53A, and the new SP-800-122, as well as the concepts contained in the CIO Council's document on the *Federal Segment Architecture Methodology* (FSAM) and concepts from Office of Management and Budget (OMB) Line of Business initiatives such as the "Information Sharing Environment" (ISE). The new "Security Content Automation Protocol" (SCAP) from NIST is also referenced as an emerging federal security standard.

Version 3.0 incorporates a security and privacy control assessment tool, which is intended to be a non-proprietary software product that can be used to identify security controls at the enterprise, segment, and system levels of an architecture and to illustrate how concepts in this document can be put into practice. The tool is available for trial and downloads at the Federal CIO Council's website under Enterprise Architecture (FEA-SPP Assessment Tool v4).

Version 3.0 of the FEA-SPP also supports the implementation of the Obama Administration's "Open Government" initiative and its underlying principles of transparency, public participation, and collaboration, as well as major federal data sharing initiatives such as Data.gov and the National Information Exchange Model (NIEM) that the Department of Justice is coordinating.

The FEA-SPP is voluntary guidance applicable to any Federal Government agency. This FEA-SPP Version 3.0 document does not supersede, modify, or interpret any law, regulation, or executive branch policy. The FEA-SPP provides best practices and recommendations to promote the successful incorporation of security and privacy into an organization's enterprise architecture and to ensure appropriate consideration of security and privacy requirements in agencies' strategic planning and investment decision processes.

Agencies are advised to consult all laws, regulations, and policies that pertain to privacy, including the Privacy Act of 1974 (5 U.S.C. § 552a), the E-Government Act of 2002 (Public Law No. 107-347, 116 Statute 2899), OMB Circular A-130, OMB Memorandum M-03-22, and OMB Memorandum M-07-16.

Section 1.0: Introduction

Section 1.1: The Federal Enterprise Architecture

The Federal Enterprise Architecture (FEA) encompasses the U.S. Federal Government's approach to enterprise architecture and provides a framework for cross-agency information technology investment analysis, management, and use. The FEA is comprised of five, inter-related reference models incorporated into a Consolidated Reference Model, and three general profiles which are intended to promote common, consistent enterprise architecture practices that improve government performance. The reference models include: (1) Performance Reference Model (PRM), (2) Business Reference Model (BRM), (3) Service Component Reference Model (SRM), (4) Data Reference Model (DRM) and (5) Technical Reference Model (TRM). Collectively, these reference models enable cross-agency analysis and the identification of redundancies, gaps, and opportunities for collaboration. The FEA profiles include: (1) Geospatial Profile, (2) Records Management Profile and (3) Security and Privacy Profile (FEA-SPP). The FEA-SPP is the focus of this document.

Section 1.2: The FEA-SPP

The FEA-SPP is a scalable, repeatable, and risk-based methodology and framework for addressing information security and data privacy requirements in the context of an agency's architecture at the enterprise, segment, and solution levels. This is particularly useful when sharing common application components and data. The FEA-SPP provides a common language for discussing security and privacy in the context of federal agencies' business and performance goals. The FEA-SPP also provides best practices and recommendations that promote the successful incorporation of information security and privacy into an organization's enterprise architecture. Specifically:

- Provides a roadmap that assists agencies in integrating IT security and privacy with enterprise architecture;
- Provides a mechanism for identifying and documenting security and privacy requirements;
- Promotes inclusion of security and privacy in business activities and processes;
- Integrates the National Institute for Standards and Technology (NIST) Risk Management Framework (RMF) and System Development Life Cycle (SDLC) processes to ensure that relevant security and privacy requirements are integrated; and
- Helps program executives understand the Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems; the foundational concepts therein of confidentiality, integrity, and availability; the eight privacy Fair Information Practice Principles (FIPPs)¹ and how these fit within enterprise architecture planning, while leveraging standards and services that are common to the enterprise and the federal government.

Federal agencies are mandated to implement both security and privacy protections for federal information and information systems. All too often, security and privacy have been considered

¹ The FIPPs (i.e., privacy control families) are discussed in detail in Section 3.2.

at the end of program development, resulting in higher costs and implementation delays. In coordination with other laws and policies, the FEA-SPP describes how these two requirements are intertwined in the design and implementation of a federal architecture. Consistent with existing OMB guidance, the FEA-SPP framework brings security and privacy requirements that must be considered to the forefront of the program decision making process, and incorporates them into the architecture definition and system design process at the earliest stages.

Government agencies are becoming increasingly aware of the important role privacy protection plays in the success of their missions. Failure to adequately address privacy concerns throughout all areas of a program can reduce mission effectiveness by eroding public confidence and creating barriers to the development and implementation of federal programs that use information systems containing personal information and compromises the security goal of confidentiality, as required by law. System integrity plays an important role in privacy protection. For example, compromised data may result in poor decision making regarding the provision of benefits to an individual. Privacy protection is also closely related with the security goals of integrity and availability. Availability is integral to assuring that federal systems and capabilities foster and protect privacy. Information on individuals is maintained for specific purposes, so if the government is unable to fulfill those purposes because the data is unavailable, then the individual may be denied the benefit for which he or she is eligible. Other aspects of privacy not directly aligned with the security goals of confidentiality, integrity, and availability involve a number of important privacy-related considerations, which are addressed in law and OMB guidance (e.g., what information is collected; who is authorized to have access to it; what opportunities are provided for individual consent, access, or correction; how is the information to be used and disclosed; what information quality and integrity criteria should be applied; and what tools will be implemented to ensure compliance and accountability). Thus, privacy, just as security, has broad organizational, operational, and technical implications.

The FEA-SPP also provides a description of how privacy controls should be incorporated into the architecture of the enterprise, segment, and or solution. Privacy controls are driven by legal, regulatory, and administrative requirements. Privacy controls are implemented through policies and procedures and tools established by OMB and NIST. Within this framework, Federal agencies usually tailor privacy controls for the specific needs of the agency. In particular, NIST has provided guidance for information technology security in the form of Special Publications for many years. The privacy community is working with OMB, NIST, and others to establish common nomenclature, controls, and tools to standardize privacy best practice across the federal government. The FEA-SPP provides a critical opportunity to help ensure that privacy is fully integrated into all aspects of the FEA.

The FEA-SPP, Version 3.0 supports the implementation of the Obama Administration’s “Open Government” initiative and the principles of transparency, public participation, and collaboration. As is stated in – OMB’s December 8, 2009 Open Government Directive (M-10-06), these three principles form the cornerstone of an open government. *Transparency* promotes accountability by providing the public with information about what the Government is doing. *Public participation* allows citizens to contribute ideas and expertise so that their government can make policies with the benefit of information that is widely dispersed in society. *Collaboration* improves the effectiveness of Government by encouraging partnerships and

cooperation within the Federal Government, across levels of government, and between the Government and private institutions. The FEA-SPP supports the identification of security and privacy risk along with mitigation strategies as agencies develop strategies for implementing the open government principles.

Section 1.3: FEA-SPP Governance

The FEA-SPP was developed by government and industry volunteers with oversight from OMB's FEA Program Office, NIST's FISMA Project Office, and the Federal Chief Information Officer (CIO) Council's Architecture and Infrastructure Committee. Mr. Kshemendra Paul (then the OMB Chief Architect) served as executive sponsor and three SES or GS-15 level government agency employees served as co-leaders of the FEA-SPP Working Group, with one co-lead being from each of the architecture, security, and privacy communities. Other FEA-SPP stakeholders include agency Chief Information Officers (CIOs), line of business managers, Chief Information Security Officers (CISOs), Chief Privacy Officers (CPOs), Enterprise Architects, and program officials.

Section 1.4: FEA-SPP, Version 3.0

This version of the FEA-SPP is intended to present more detailed guidance on how to integrate security and privacy into enterprise architecture activities. The FEA-SPP is voluntary guidance applicable to any Federal government agency; it does not supersede, modify, or interpret any law, regulation, or executive branch policy. The goal is to enhance and enable security and privacy acceleration into the enterprise architecture mainstream allowing a more complete picture of an agency's capability and a more cyber-focused budget and transition plan. The nation's recent focus on cyber security, virtualization, cloud computing, and transparency in government data presents major new challenges for agencies in terms of information, infrastructure and solution sharing within an increasingly open and collaborative environment, and reinforces the need for and application of the FEA-SPP. The FEA-SPP, Version 3.0 builds upon earlier versions in terms of guidance while aligning with the movement toward a more secure cyberspace and transparent government that securely but effectively capitalizes on the advantages of cloud computing and virtualization.

This version presents the FEA-SPP framework, its associated methodology, framework, and new architecture methods at a level that is intended to be understandable across a wide technical and non-technical audience. This version of the FEA-SPP describes how the FEA-SPP fits together with other tools used to assess and implement security and privacy including: the NIST Risk Management Framework, the FEA, and the Federal Segment Architecture Methodology (FSAM). Additional tools, specifically regarding privacy, are under development. Individually and collectively, each tool is critical to successful implementation of the FEA-SPP.

Section 1.5: How to Use This Document

This document is intended to be a useful resource for individuals seeking an understanding of the FEA-SPP and how to integrate security and privacy with federal enterprise architecture activities. Although this document may be read from start to finish, one can review specific topics that are applicable to the reader's interest. There are six sections of the document:

- Section 1.0 Introduction: Provides readers a general, yet brief overview of FEA and the FEA-SPP.
- Section 2.0 FEA-SPP Overview: Provides an in-depth overview of the FEA-SPP and its relationships with enterprise architecture, IT security and privacy.
- Section 3.0 Security and Privacy Fundamentals: Provides an overview of key security and privacy concepts which are relevant to the integration of the FEA-SPP.
- Section 4.0 FEA-SPP Methodology: Provides an overview of the three stages of the FEA-SPP methodology.
- Section 5.0 Integrating FEA-SPP with the Federal Enterprise Architecture: Provides an overview of enterprise architecture within the context of the FEA-SPP.
- Section 6.0 Integrating Security and Privacy with FSAM: Provides an overview of the FSAM and discusses how to leverage the methodology to integrate security and privacy controls.

The appendices provided at the end of the document provide supporting material that is referenced throughout.

Section 1.6: Target Audience

The FEA-SPP is a cross-disciplinary methodology that requires support and participation from not only the security and privacy teams, but the enterprise architecture, capital planning, and business groups as well. Although the FEA-SPP is written at a high level to ensure the methodology is understandable to a wide audience, it does include advanced concepts that require a basic understanding of security and privacy, such as how agency architectures are implemented at the enterprise, segment, and solution levels; how the RMF is implemented in a way that includes needed security controls at all levels of the architecture.

Section 2.0: Key FEA-SPP Stakeholders and Management Officials

The FEA-SPP fosters awareness and interaction among stakeholders promoting coordinated approaches to security and privacy which result in efficiency, interoperability and business alignment. Using the FEA-SPP requires a coordinated effort between organizational leaders and IT governance representatives (e.g., security, privacy, enterprise architecture, and capital planning). Implementing the FEA-SPP requires the participation of key stakeholders at the executive, management, and staff levels in each agency. This includes:

- Chief Information Officers
- Chief Information Security Officers
- Chief Privacy Officers (or Senior Agency Officials for Privacy)
- Chief Financial Officers
- Chief Enterprise Architects
- Chief Risk Management Officers
- Agency Records Management Officers
- Program Officials
- Enterprise Architecture, Security, and Privacy Program Staffs

Other participants may include security and privacy program officials including the Designated Approving Authority (DAA); the Information System Security Office Manager (ISOM), the Information Systems Security Site Manager (ISSM); the Information System Owner (ISO), and the Information System Security Officer (ISSO).

Chief Information Officer (CIO)

The CIO is responsible for information resource management and related governance, including security, privacy, architecture, capital planning, program management, and IT workforce management – all of which have a role in implementing FEA-SPP concepts.

Chief Risk Management Officer (CRMO)

The CRMO is the executive accountable for enabling the efficient and effective governance of significant risks and related opportunities to a business and its various segments.

Chief Information Security Officer (CISO)

The CISO has primary responsibility for ensuring IT security in an agency and should be familiar with external and internal security requirements as well as the enterprise-level capabilities currently in place to satisfy those requirements. The CISO contributes knowledge of the organization's current security posture. More than one CISO may be needed to support the FEA-SPP methodology in agencies where security responsibilities are decentralized.

Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO)

The SAOP/CPO has overall responsibility and accountability for ensuring the agency's implementation and compliance with respect to information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to privacy. The SAOP/CPO also has a central policy-making role at the agency and is involved in all activities that involve personally identifiable information. Privacy may have several advocates within an agency.

The Agency Federal Records Officer

The Agency Federal Records Officer is responsible for ensuring that all electronically stored information (ESI) has been scheduled for disposition in accordance with retention periods approved by National Archives and Records Administration (NARA).

Chief Enterprise Architect

The Chief Enterprise Architect has primary responsibility for developing and promoting the operationalization of the enterprise architecture of an organization. In light of those responsibilities, the Chief Enterprise Architect may be the best person to lead FEA-SPP activities and to capture outcomes.

Chief Financial Officer (CFO)

The CFO has responsibility for planning, proposing, and monitoring major agency investments. The CFO is often the chair of agencies' Investment Review Boards (IRB), but at a minimum has responsibility for insuring that the agencies funds are allocated to the highest performing and effective risk-based investments. The organization's goal of promoting informed and strategic investment decisions makes it important that the CFO participates in this process.

Chief Privacy Officer

The Privacy Officer has the responsibility for planning, implementing and overseeing the activities mandated by the Privacy Act of 1974

Program Officials

Program officials are responsible for accomplishing the business of an agency. They drive decisions about investments and are responsible for planning and budgeting for security and privacy. While security and privacy officials will be knowledgeable about enterprise security and privacy requirements, program officials may have unique, programmatic requirements. Senior agency officials' decisions in the course of developing the FEA-SPP will impact the program-level as the program officials will implement many of the security and privacy decisions. Including program officials in the FEA-SPP activities will ensure that decisions made will be practical and useful to everyone.

Program Staff

Program staff includes those government and contractor personnel who are assigned to agency enterprise architecture, security, privacy and other IT and business-related programs.

Section 3.0: Architecture, Security and Privacy Fundamentals

Section 3.1: Implementing Security Controls

In addition to the Privacy Act of 1974 and the E-Government Act of 2002, the Federal Information Security Management Act (FISMA) of 2002 is one of the main pieces of legislation driving federal agencies' information security activities.² Designed around accountability, FISMA sets forth specific security activities and associated reporting requirements. Further implementation of FISMA occurs through OMB Circular A-130, numerous related regulations, and NIST standards and guidance. Generally speaking, information security describes many of the activities that ensure the confidentiality, integrity and availability of information and information systems. *Confidentiality* refers to what data may be disclosed and to whom the data may be disclosed ensuring that only legally authorized and appropriate disclosures are made. *Integrity* is the assurance that information and information systems are protected against improper or accidental modification. *Availability* is the assurance of timely and reliable access to information and information systems by authorized persons.³

FISMA mandates a risk-management approach to securing federal information and information systems. According to the law, each Agency Head is responsible for (1) “providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction” of agency information and information systems and (2) “ensuring that information security management processes are integrated with agency strategic and operational planning processes.” This is a key concept underlying FEA-SPP implementation – that there should be close linkage between security, privacy management, and enterprise architecture. The growth of information and infrastructure sharing, as reflected in Cloud Computing and Service-Oriented Architecture concepts, all drive the need for a broader, more integrated management of security and privacy risk within agency architectures, and this is where the FEA-SPP can add value.

Federal agencies achieve FISMA goals and, thus, ensure information confidentiality, integrity, and availability, by applying safeguards and countermeasures (controls). To that end, eighteen families of managerial, operational, and technical security controls have been identified by NIST in SP-800-53, Revision 3 to support such interests (see Table 1).⁴ To accomplish this, agencies' information security officials identify the appropriate set of controls from each control family through categorizing each information system. Categorization describes the potential impact a

² The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

³ CNSSI Instruction No 4009 defines integrity, confidentiality, and availability as follows: (A) confidentiality – assurance that information is not disclosed to unauthorized individuals, processes, or devices; (B) integrity – quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data; and (C) availability – timely, reliable access to data and information services for authorized users.

⁴ The eighteen control families are defined by NIST SP-800-53, Revision 3 which was released in May, 2010.

loss of one or more of the three security objectives defined by FISMA, based on the data the systems contain. These eighteen security control families cover the minimum requirements with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. The eighteen security control families represent a broad-based and balanced information security program that address the management, operational, and technical aspects of protecting federal information and information systems. A control family is associated with a given “class” (technical, operational, or management). The eighteen security control families from SP-800-53 are provided in Table 1.

Table 1. Security Control Families

Security Control Family	Description
1. Risk Assessment	Assessing the risk to organizational operations, assets, and individuals resulting from the operation of information systems, and the processing, storage, or transmission of information.
2. Planning	Developing, documenting, updating, and implementing security plans for systems.
3. System and Services Acquisition	Allocating resources to protect systems, employing SDLC processes, employing software usage and installation restrictions, and ensuring that third-party providers employ adequate security measures to protect outsourced information, applications, or services.
4. Certification and Accreditation and Security Assessments	Assessing security controls for effectiveness, implementing plans to correct deficiencies and to reduce vulnerabilities, authorizing the operation of information systems and system connections, and monitoring system security controls.
5. Personnel Security	Ensuring that individuals in positions of authority are trustworthy and meet security criteria, ensuring that information and information systems are protected during personnel actions, and employing formal sanctions for personnel failing to comply with security policies and procedures.
6. Physical and Environmental Protection	Limiting physical access to systems and to equipment to authorized individuals, protecting the physical plant and support infrastructure for systems, providing supporting utilities for systems, protecting systems against environmental hazards, and providing environmental controls in facilities that contain systems.
7. Contingency Planning	Establishing and implementing plans for emergency response, backup operations, and post-disaster recovery of information systems.
8. Configuration Management	Establishing baseline configurations and inventories of systems, enforcing security configuration settings for products, monitoring and controlling changes to baseline configurations and to components of systems throughout their SDLC.
9. Maintenance	Performing periodic and timely maintenance of systems, and providing effective controls on the tools, techniques, mechanisms, and personnel that perform system maintenance.
10. System and Information Integrity	Identifying, reporting, and correcting information and system flaws in a timely manner, providing protection from malicious code, and monitoring system security alerts and advisories.

Security Control Family	Description
11. Media Protection	Protecting information in printed form or on digital media, limiting access to information to authorized users, and sanitizing or destroying digital media before disposal or reuse.
12. Incident Response	Establishing operational incident handling capabilities for information systems, and tracking, documenting, and reporting incidents to appropriate officials.
13. Awareness and Training	Ensuring that managers and users of information systems are made aware of the security risks associated with their activities and of applicable laws, policies, and procedures related to security, and ensuring that personnel are trained to carry out their assigned information security-related duties.
14. Identification and Authentication	Identifying and authenticating the identities of users, processes, or devices that require access to information systems.
15. Access Control	Limiting information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems), and to types of transactions and functions that authorized users are permitted to exercise.
16. Audit and Accountability	Creating, protecting, and retaining information system audit records that are needed for the monitoring, analysis, investigation, and reporting of unlawful, unauthorized or inappropriate information system activity, and ensuring that the actions of individual users can be traced so that the individual users can be held accountable for their actions.
17. System and Communications Protection	Monitoring, controlling and protecting communications at external and internal boundaries of information systems, and employing architectural designs, software development techniques, and systems engineering principles to promote effective security.
18. Program Management	Organization-wide information security program management controls that are independent of any particular information system and are essential for managing information security programs (e.g., Information Security Program Plan).

Security control baselines are the starting point for organizations in determining the security controls necessary to integrate into their enterprise architecture, its component segment architectures and the information systems that support the segments. An organization-wide view of information security lends itself to the partitioning of security controls in order to map them to the organization's segment architectures at the enterprise, segment and solution levels.

Security controls are grouped into three partitions: Common Controls (Organizational), Hybrid Controls (Mission/Business Process), and System Specific (Information System) security controls. These security control partitions map to the three segment architectures at the enterprise, segment, and solution levels respectively. Mapping security controls to the segment architectures begins with partitioning the security control baseline by the identification of common, hybrid, and system-specific controls.

Common Security Controls (Organizational)

Common security controls are identified by how they are applied by the organization. Common security controls can apply to: all organizational information systems; a group of information systems at a specific site; or common information systems, subsystems, or applications; i.e., common hardware, software, and/or firmware deployed at multiple operational sites. Common security controls have the following properties:

- The development, implementation, and assessment of common security controls can be assigned to responsible organizational officials or organizational elements; other than the information system owners whose systems will implement or use the common security controls.
- The results from the assessment of the common security controls can be used to support the security certification and accreditation processes of organizational information systems where the controls have been applied.

This characterization of common security controls correlates to similar qualities of an enterprise segment architecture. Enterprise segment architecture is characterized by common or shared assets such as: business processes, investments, data, systems or technologies and the security controls that protect information. Further, enterprise segment architecture is agency, organization-wide and cross-agency in scope, and generally is comprised of common or shared IT services supporting the enterprise at all levels from core mission areas (supported by solutions and secured by solution level security controls) to business and enterprise services.

Potential examples of common security controls are: contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls. These controls lend themselves to central management, development, implementation, and assessment.

Hybrid Security Controls (Mission/Business/Process)

Hybrid security controls are identified when one part of a control is deemed to be common, while another part of the control is deemed to be system-specific. Hybrid controls may serve as templates for further control refinement. An organization may choose to implement, for example, a specific common security control, like CP-2 -Contingency Planning, as a master template for a generalized contingency plan for all organizational information systems with individual information system owners tailoring the plan, where appropriate, for system-specific issues.

Segment architecture is analogous to hybrid security controls in that it can be deemed to be common while another part of the control can be system-specific. For example, segment architecture is related to enterprise architecture through three principles: structure, reuse and alignment. First, segment architecture inherits the framework used by the enterprise architecture, although it may be extended and specialized to meet the specific needs of a core mission area or common or shared service. Second, segment architecture reuses important assets defined at the enterprise level including: data; common business processes and investments; and applications and technologies. Third, segment architecture aligns with elements defined at the enterprise

level, such as business strategies, mission, values, mandates, standards and performance goals. Hybrid controls can apply these same principles.

System-Specific Security Controls (Information System)

Baseline security controls not designated as common controls or hybrid are considered system-specific controls and are the responsibility of the information system owner. These controls apply to the solution architecture mapped to the LOB and sub-function levels of the BRM. At this level, agency IT assets such as applications or components used to automate and improve individual agency business functions are defined. The scope of a solution architecture is typically limited to implementing all or part of a system or business solution at the LOB or sub-function level. The primary stakeholders for solution architecture are system owners and developers.

Implementing Security Controls Across all Levels of the Enterprise

Implementing security and privacy controls within enterprise-level (Organization), segment-level (mission or business process), and solution/system-level architectures is accomplished by applying FEA reference model principles and the NIST RMF methodology. The FEA provides relevant information in the development of the enterprise, segment, and solution architectures. The NIST RMF, on the other hand, provides the required controls needed to ensure that each architecture is compliant with laws, regulations, standards, guidelines, and the organizations risk requirements; see Figure 1.

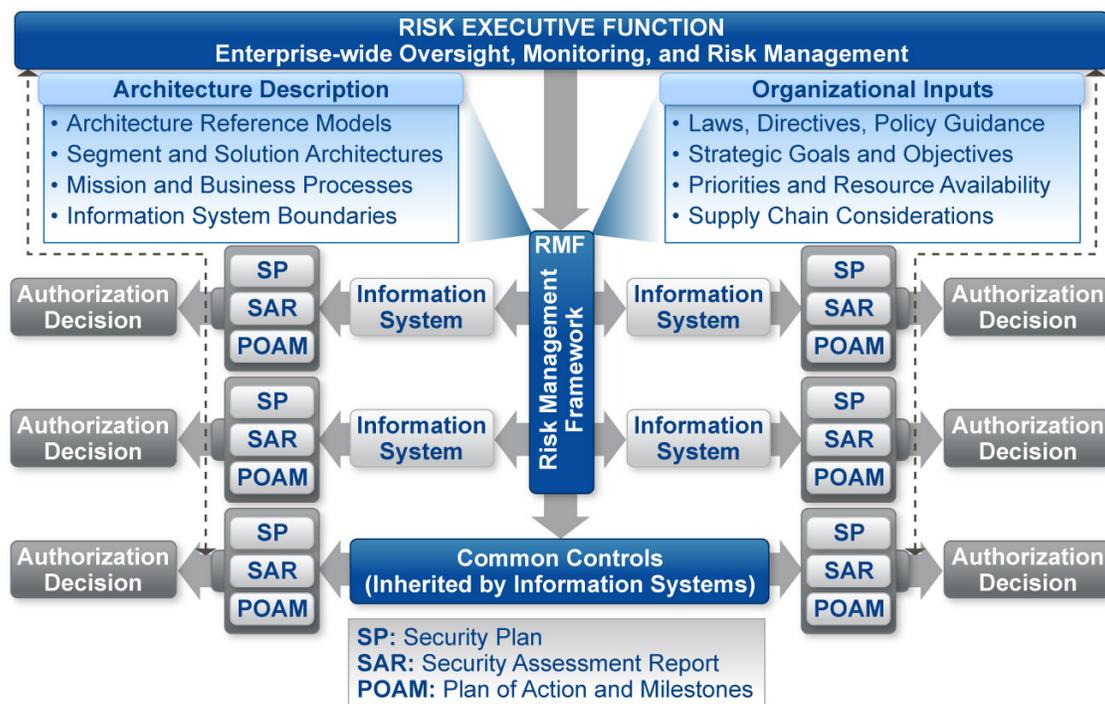


Figure 1: The RMF and Compliance

Section 3.2: Implementing Privacy Controls

There are many laws, regulations, and policies that govern an agency’s collection, maintenance, use, and dissemination of personally identifiable information (PII). Key examples include the Privacy Act of 1974, the E-Government Act of 2002, policies issued by OMB, and individual

agency policies. In addition, many other statutes provide privacy-like protections for particular types of information; (e.g., financial, tax, grand jury, and health information).

The Privacy Act establishes the fundamental requirements that govern the collection, maintenance, use and dissemination of information in a “record” that is part of a “system of records.” The *Overview of the Privacy Act of 1974*, prepared by the Department of Justice's Office of Privacy and Civil Liberties (OPCL), provides that: "Broadly stated, the purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them The Act focuses on four basic policy objectives: (1) To restrict disclosure of personally identifiable records maintained by agencies. (2) To grant individuals increased rights of access to agency records maintained on themselves. (3) To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete. (4) To establish a code of 'fair information practices' that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records."⁵ For additional information about the Privacy Act, agencies should consult OMB's 1975 Implementation and other OMB guidance.

In addition to the Privacy Act, Section 208 of the E-Government Act elaborates specific requirements for agencies' collection, use, maintenance, and dissemination of information in identifiable form through the utilization of information technology systems. Section 208(d) of the e-Gov Act defines information in identifiable form as “any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.” Section 208 requires federal agencies to perform a risk-based analysis of their activities in the form of a Privacy Impact Assessment (PIA).⁶ The requirements of Section 208 were further explained in OMB Memorandum M-03-22, which interprets the statute and provides guidance for agencies in applying it.

Moreover, numerous OMB memoranda set forth specific requirements for agencies' handling of personally identifiable information (PII). For example, the OMB Memorandum on *Safeguarding Personally Identifiable Information*, M-06-15 (May 22, 2006), emphasizes the importance of safeguarding personally identifiable information (PII) under both the Privacy Act and the FISMA. OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007),⁷ provides additional guidance regarding agencies' obligations to protect PII. OMB M-07-16 reminds agencies of the requirements established in the Privacy Act - that they must “establish appropriate administrative, technical, and physical

⁵ US Department of Justice, Office of Privacy and Civil Liberties, *Overview of the Privacy Act (2010 Edition)*: <http://www.justice.gov/opcl/1974privacyact-overview.htm>.

⁶ While not a government-wide standard, a representative example of a comprehensive agency response to these requirements is the Department of Homeland Security guidance for Privacy Threshold Analysis (PTA), Privacy Impact Assessments (PIA), System of Records Notices (SORNs), technology implementation and incident handling. This guidance may be found at http://www.dhs.gov/files/publications/gc_1209396374339.shtm.

⁷ OMB M-07-16 defines PII as “information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.”

safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.”

As the discussion above demonstrates, the privacy requirements set forth in the Privacy Act, the E-Government Act, OMB policies, and other sector or information specific laws, provide a full framework of privacy requirements. It is important, therefore, in the design of an enterprise architecture to ensure identification of and compliance with all applicable privacy laws and policies. Specifically, the privacy control families outlined below will help agencies identify the covered information, determine the context of the information, and apply the applicable laws and privacy controls to ensure that personally identifiable information is protected. These families support the full framework of privacy requirements by helping agencies consider these issues; each agency should work with their privacy officials and their counsel to ensure that they comply with all applicable laws, regulations, and policies.

The eight FIPPs privacy control families are provided in Table 2.

Table 2: Fair Information Practice Principles – Privacy Control Families

Privacy Control Family	Description
1. Transparency	Providing notice to the individual regarding the collection, use, dissemination, and maintenance of PII.
2. Individual Participation and Redress	Involving the individual in the process of using PII and seeking individual consent for the collection, use, dissemination, and maintenance of PII. Providing mechanisms for appropriate access, correction, and redress regarding the use of PII.
3. Purpose Specification	Specifically articulating the authority that permits the collection of PII and specifically articulating the purpose or purposes for which the PII is intended to be used.
4. Data Minimization & Retention	Only collecting PII that is directly relevant and necessary to accomplish the specified purpose(s). Only retaining PII for as long as is necessary to fulfill the specified purpose(s) and in accordance with the National Archives and Records Administration (NARA) approved record retention schedule.
5. Use Limitation	Using PII solely for the purpose(s) specified in the public notice. Sharing information should be for a purpose compatible with the purpose(s) for which the information was collected.
6. Data Quality and Integrity	Ensuring, to the greatest extent possible, that PII is accurate, relevant, timely, and complete for the purpose(s) for which it is to be used, as identified in the public notice.
7. Security	Protecting PII (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Privacy Control Family	Description
8. Accountability and Auditing	Providing accountability for compliance with all applicable privacy protection requirements, including all identified authorities and established policies and procedures that govern the collection, use, dissemination, and maintenance of PII. Auditing for the actual use of PII to demonstrate compliance with established privacy controls.

The FIPPs provide a framework for the privacy control families outlined in the FEA-SPP.⁸ In general, this set of principles is rooted in the tenets of the Privacy Act, and was articulated in Department of Homeland Security Privacy Policy Memorandum 2008-01 (December 29, 2008)⁹ and is mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. These privacy control families, which are based upon the FIPPs, are common across many privacy laws and provide a framework that will help agencies address privacy requirements.

Most privacy controls, as is the case with security controls, have technical, policy, and administrative elements and should be addressed at the enterprise, segment, and system levels. The processes that they describe must be addressed at every stage of system or business lifecycle, regardless of whether personal information is collected or a program or technology is under development that may have a privacy impact.

Section 3.3: The Relationship Between the FEA-SPP and NIST Standards and Guidance

NIST provides a wide range of information security standards and guidance that identify how security and privacy services can be effectively implemented. The FEA-SPP does not replace or alter those standards and guidance; it does, however, seek to capture the outputs of enterprise, segment, and solution security activities and use them to support enterprise decisions. The context for the FEA-SPP is the FEA and associated reference models, as well as guidance provided in OMB policy, the FSAM, and NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*, SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, and 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* as is shown in Figure 2.

⁸ In 1973, an advisory committee of the U.S. Department of Health, Education, and Welfare (HEW) issued a report, *Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, which articulated the fair information principles. The report examined the impact of computerization of information on privacy and included recommendations on developing policies that would allow the benefits of computerization to go forward, and provide safeguards for personal privacy. The backdrop surrounding the HEW report and the 1974 Privacy Act included several years of intense Congressional hearings examining the surveillance activities of the Nixon and J. Edgar Hoover era and the post-Watergate support for government reform. Flowing from the numerous abuses of power uncovered by Congress and the media during the early 1970s, the Privacy Act set out a comprehensive regime limiting the collection, use and dissemination of personal information held by government agencies. The Privacy Act established penalties for improper disclosure of personal information and gave individuals the right to gain access to their personal information held by agencies.

⁹ Appendix F contains additional details on the Privacy Control Families

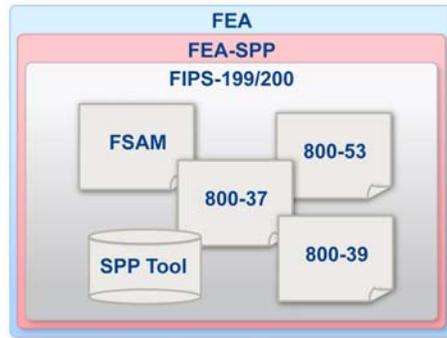


Figure 2: The FEA-SPP Context

Section 4.0: FEA-SPP Methodology

The FEA-SPP methodology is a multi-step process that documents enterprise-level information security and privacy tools (see Figure 3 below). Each stage has goals, objectives, implementing activities, and output products for formal inclusion in agency enterprise architecture and capital planning and investment control (CPIC) processes.

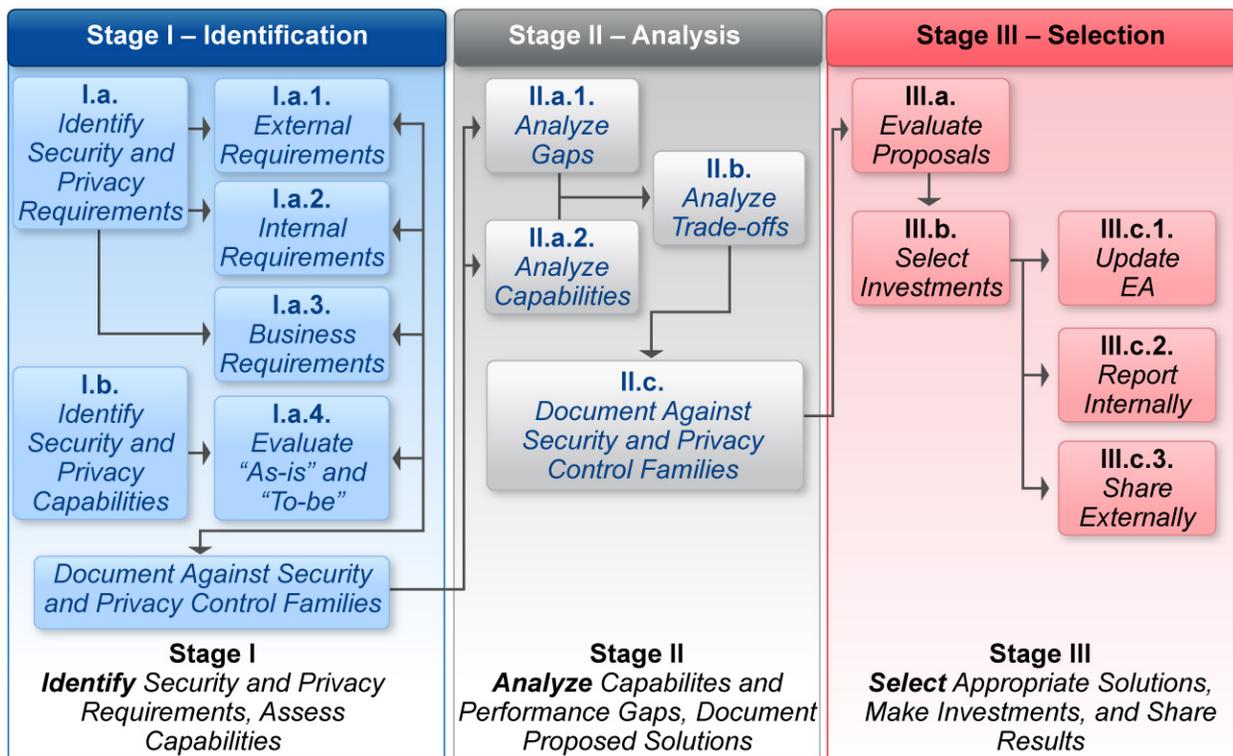


Figure 3: The FEA-SPP Methodology

Section 4.1: Stage I – Identification

SECTION 4.1.1: OVERVIEW

Stage I encompasses the research and documentation activities necessary to identify security and privacy requirements in support of the mission objectives so that they may be incorporated into the enterprise architecture. Stage I outputs serve as the foundation for Stage II and Stage III analysis and requires periodic updates to accommodate changes to enterprise capabilities. Stage I outputs enable an organization to:

- Specify program and enterprise-level and cross-agency security and privacy requirements, including previously unknown requirements
- Specify program and enterprise-level security and privacy capabilities, including current and planned future requirements, and cross-agency requirements
- Populate the enterprise architecture with requirements and capabilities using nomenclature that is common across the federal government.

Agencies can take a top-down or bottom-up approach to Stage I. Stage I accommodates either approach. The FEA-SPP supports a top-down approach in which the high-level requirement and capability identification begins at the enterprise level. Results from that activity are available to a LOB, segment, or more specific program or system for customization. The advantage of this approach is that agencies capture common requirements once, which improves programmatic efforts. In addition, a top-down approach helps to ensure an enterprise-centric application of the FEA-SPP rather than a stove-pipe point of view. Adopting an enterprise-centric point of view is consistent with OMB FEA guidance. Funding to support implementation of FEA-SPP concepts and practices are most likely found through agency program budgets in the operations, security, and privacy cost areas. Therefore, some organizations may launch Stage I activities in a bottom-up approach. In those cases the first completed programmatic effort can serve as a model for others.

After identifying security and privacy requirements and capabilities, agencies can then evaluate them against the “as-is” and “to-be” architectures to ensure that these requirements and capabilities are adequately represented and supported by the enterprise architecture. Stage II introduces approaches for analyzing Stage I outputs of, leading to proposed additions to or changes in agencies’ security or privacy capabilities. Specifically, Stage I activities immediately enable agencies to improve operations by:

- Analyzing gaps between requirements and capabilities to identify unmet requirements
- Analyzing their portfolio of current capabilities (an “as-is” security and privacy architecture) to identify opportunities to increase interoperability and standardization within the context of security and privacy requirements, and reduce costs appropriately
- Proposing future capabilities based on improved insights into the enterprise and program performance requirements
- Facilitating enterprise-level choices about the implication of security and privacy decisions and investments consistent with appropriate risk levels.

SECTION 4.1.2: ACTIVITIES

The following activities support Stage I goals and objectives. For each activity, agencies should identify and document the owners of associated data, the location where that data is maintained, and any corrective actions identified to improve the data or complete the activity.

Table 1: Stage I Goals, Objectives & Activities

Goals, Objectives, Activities
<p>1. Identify Business Requirements. These include performance, business, and data requirements.</p> <p>a. Assess enterprise architecture descriptions of performance objectives to determine if they support measuring compliance. In addition to compliance oversight, metrics should assess adequacy of performance, and support service-level agreements.</p>
<p>i. Document performance objectives and metrics associated with each Stage I requirement.</p>
<p>ii. Evaluate performance metrics to ensure consistency with NIST SP 800-55 or a comparable agency methodology.</p>
<p>b. Assess enterprise architecture descriptions of lines of business, functions, and sub-functions to determine if they describe security and privacy attributes. The business architecture should highlight security and privacy-sensitive activities related to each business function and sub-function to ensure that appropriate controls are developed and in place that relate to key business functions.</p>
<p>c. Ensure that enterprise architecture descriptions of data incorporate security and privacy attributes.</p> <p>i. Describe security attributes in terms of high, moderate, and low requirements for information confidentiality, integrity, and availability. FIPS PUB 199 and NIST SP 800-60 describe the methodology for this activity. This guidance help agencies map security impact levels in a consistent manner to types of: information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation) and information system delivery objectives (mission critical, mission support, administrative).</p>
<p>ii. Identify data that contains personally identifiable information that may be subject to privacy legislation and policies. Especially consider the Privacy Act, E-Government Act, HIPAA, and OMB policies.</p>
<p>iii. Link information types to lines of business and sub-functions. Information must be associated with a business purpose to properly assess associated risks.</p>
<p>d. Identify security and privacy commitments established through inter and intra-agency trust agreements and contracts. Evaluate whether those commitments have programmatic or enterprise-wide impact on security and privacy.</p>
<p>e. Identify and document security and privacy practices driven by organizational preferences and market practices. Evaluate the criticality of non-mandatory practices in terms of the risk and cost, and program performance requirements.</p>
<p>2. Document requirements in the enterprise architecture.</p>
<p>a. Capture and document mission and support requirements.</p>

Goals, Objectives, Activities
b. Document performance objectives in the PRM and relate them to business outcomes.
3. Identify Security and Privacy Capabilities
a. Identify processes and technologies that provide dedicated security or privacy services. For example, a stand-alone Internet firewall or a web-based PIA tool.
b. Identify processes and technologies that are not security or privacy-centric but which accomplish security or privacy as an ancillary function. For example, a grants-management system that encrypts data.
c. Document capabilities in the agency SRM or TRM as applicable. Describe each capability in terms of how it supports one or more of the 18 security control families. The controls families will be used in Stage II to map requirements to capabilities and identify gaps.

Section 4.2: Stage II—Analysis

SECTION 4.2.1: OVERVIEW

Stage II is an analysis of agency security and privacy requirements, and the existing or planned capabilities that support security and privacy. Stage II activities enable an organization to:

- Identify gaps between requirements and current or planned capabilities
- Identify opportunities to increase interoperability between or reduce costs of current or planned capabilities
- Propose solutions to address gaps or improve capabilities based on an informed trade-off analysis of alternatives.

In Stage II, the FEA-SPP team reviews each control family, comparing each requirement to available components. Requirements that are not satisfied by an existing component are noted as gaps. The analysis conducted in Stage II may identify a need to change existing capabilities or propose new capabilities as a solution to gaps or suboptimal capabilities which lead to analysis of alternative solutions. Analysis of alternatives recognizes that there are multiple solutions for each problem and that each solution introduces different levels of residual risk and varying financial burdens. OMB directs agencies to consider alternative solutions and evaluate them based on functionality, risk, cost and interoperability. Alternatives are addressed through a series of trade-off analyses, resulting in a set of proposed investments that can be mapped to the agency’s “to-be” architecture.

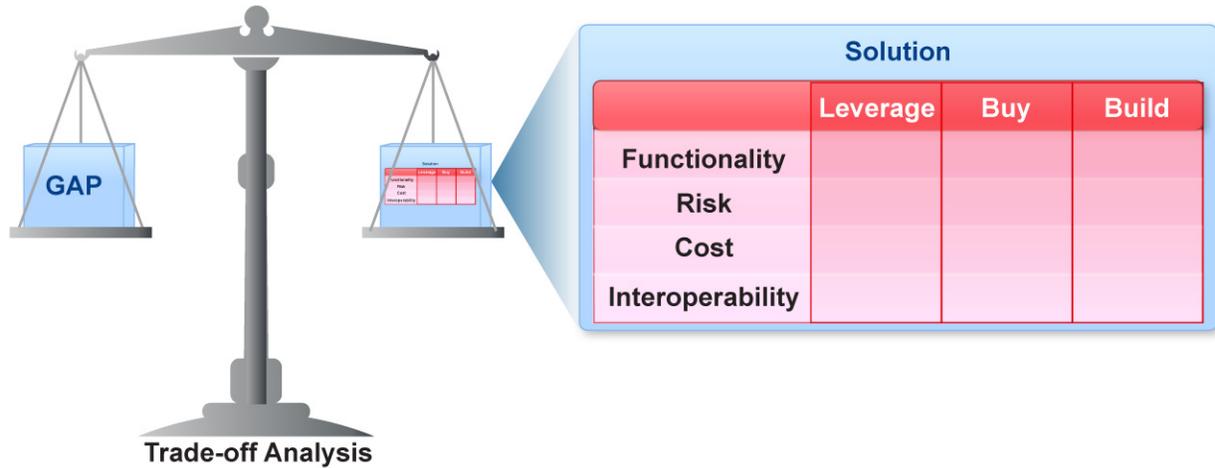


Figure 4: Analyzing Trade-Offs

All things being equal, OMB prefers leveraging an existing capability over buying a commercial solution. Similarly, OMB prefers purchasing commercial solutions over developing custom solutions. This is because leveraging an existing capability is usually more cost effective than purchasing a commercial solution, and purchasing a commercial solution is usually more cost effective than developing a custom solution. When agencies evaluate which options to select, they should consider solutions in their own agency as well as solutions from other agencies. Leveraging solutions across federal agencies is a goal of FEA efforts.

The results of the trade-off analysis support the IRB investment prioritization process. Incorporation of the trade-off analysis in the business cases, and the references to the risk analyses and enterprise architecture content provide the basis for informed risk-based decision-making during investment review, prioritization, and funding activities.

SECTION 4.2.2: ACTIVITIES

The following activities support Stage II goals and objectives. As in Stage I, agencies should identify and document the owners of associated data, the location where that data is maintained, and any corrective actions identified to improve the data or complete the activity.

Table 2: Stage II Goals, Objectives & Activities

Goals, Objectives, Activities
<p>I. Analysis Stage</p> <p>A. Security and Privacy Analyses</p> <p>1. Analyze Requirement and Capability Gaps. The purpose of these activities is to determine where gaps exist between current requirements and the current or planned capabilities to meet those requirements. Unmet requirements are then assessed to verify whether or not they must be met to appropriately manage security and privacy risks.</p> <ul style="list-style-type: none"> a. Identify the gap between requirements and capabilities. <ul style="list-style-type: none"> i. Assess the gap between security requirements and capabilities through use of the 17 security control families. Requirements and capabilities have each been mapped to the control families. Conduct a family-by-family assessment to identify requirements that are not supported by a specific capability. Unmet requirements are addressed in subsequent activities in Stage I. ii. Assess the gap between privacy requirements and capabilities through the use of the privacy control families. Requirements and capabilities have each been mapped to the control families. Conduct a family-by-family assessment to identify requirements that are not supported by a specific capability. Unmet requirements are addressed in subsequent activities in Stage I.
<ul style="list-style-type: none"> iii. Determine if unmet requirements are addressed in the agency's current future plans (through a review of the "target" architecture).
<ul style="list-style-type: none"> b. Assess the risks associated with gaps between requirements and capabilities. An accounting of security and privacy features is necessary to justify investments in OMB business cases. <ul style="list-style-type: none"> i. Assess risk for each business activity exposed to a gap to determine if the unmet requirement can be mitigated or accepted.
<ul style="list-style-type: none"> ii. Assess the set of individual gaps and their impact on the broader enterprise. Determine whether currently funded security and privacy capabilities address residual risks.
<ul style="list-style-type: none"> iii. Document the gaps that pose un-addressable or unacceptable risks in the "to-be" architecture.
<ul style="list-style-type: none"> c. Document gaps in the enterprise architecture and FISMA Plan of Action & Milestones (POA&M).
<p>2. Analyze Capabilities. Evaluate the overall capabilities portfolio to assess common risks, identifying opportunities for consolidation and standardization.</p> <ul style="list-style-type: none"> a. Aggregate program and system-level security and privacy assessments such as FIPS PUB 199 security characterizations and Privacy Impact Assessments. <p>An agency with 100 systems may find that 50 are all subject to the Low/Low/Low security control baseline; another 25 may be subject to the High/High/Medium baseline; and the remaining 25 to an assortment of other combinations.</p> <p>An agency may determine that 30 of their systems hold personally identifiable information subject to the Privacy Act, HIPAA or other privacy law considerations.</p>

Goals, Objectives, Activities
<p>b. Evaluate the controls mandated for groups of systems. Use Stage I's mapping of requirements and capabilities to control families to assess current or planned capabilities.</p>
<p>i. Identify opportunities to provide more effective and less expensive centralized security and privacy capabilities. Determine which controls are most complex or expensive to deploy at the system-level but which may be appropriate and cost effective - for an enterprise solution.</p> <p style="padding-left: 40px;">NIST SP 800-53 summarizes required security control baselines and enhancements.</p> <p style="padding-left: 40px;">Privacy laws, regulations, and policies establish a framework of appropriate privacy controls.</p>
<p>ii. Identify capabilities that are inconsistent with common agency standards. Determine if standardizing those inconsistent capabilities on an agency standard will reduce security and privacy risk, increase interoperability, or reduce costs. For example, consider operating systems with similar security and privacy requirements for implementation within the same or similarly configured infrastructure.</p>
<p>iii. Identify capabilities not driven by specific requirements. Capabilities may be identified through this assessment because their requirements have not been adequately captured in Stage I. If that is not the case, assess the need for the capability.</p>
<p>B. Analyze Trade-offs</p> <p>1. Establish criteria. Select agency-specific criteria for selecting among alternative solutions. Informed risk-based decision making requires alternative analyses with regard to sufficiency of the solution and associated costs and benefits managed to expectations for functionality. Criteria should include a review of all risk, benefit and cost factors leading to the selection of the most effective plan of action to address unsupported requirements.</p>
<p>a. Evaluate the extent to which each alternative will meet the applicable security and privacy requirements, and the extent to which they leave the agency exposed to residual risks.</p>
<p>b. Evaluate lifecycle costs required to fund the investment or modification. If the alternative is already included in PO&AM, then use the costs from the POA&M in the analysis of the alternative. If not, then develop a cost estimate or all lifecycle costs associated with the alternative. All costs should also be risk-adjusted to account for foreseeable investment risks over the investment lifecycle to facilitate comparison.</p>
<p>c. Evaluate the agency's inventory of approved technologies and services to identify the preferred standards. Select solutions consistent with the agency technical reference model. If appropriate standards are not included in the TRM they should be evaluated and incorporated. To reduce risks in the target environment, specific security and privacy investments may be needed in the technical and service infrastructures that are not addressed with the current security and privacy services and technologies.</p>

Goals, Objectives, Activities

2. Evaluate gaps or capabilities to be improved and prioritize one or more to be addressed through an investment of new funds or realignment of existing resources. Whether addressing gaps at the programmatic or enterprise levels, ensure that enterprise needs are considered. Prioritize the selection based on:

- Breadth of impact across the enterprise

- Amount of cost savings gained from an enterprise investment

- Impact of the gap on the accomplishment of agency business

- Relevance of the gap to outstanding POA&M items. Addressing these items is important because agencies must report the status of POA&M corrective actions to OMB along with associated risks.

- a. The analysis of alternatives evaluates the technically viable alternatives through a systematic paring down of the potential alternatives to feasible ones to the most viable alternatives. Viable alternatives are established by examining:

- The baseline environment and the requirements requiring attention

- Potential alternatives – those alternatives theoretically possible for addressing requirement needs

- Feasible alternatives – of the potential alternatives, those alternatives that can address the requirement needs given the constraints and limitations of the environment

- Viable alternatives – of the feasible alternatives, those alternatives that can be realistically implemented

- b. Once feasible alternatives have been identified, an analysis of the costs, benefits, and risks of each viable alternative should be performed. OMB A-11 states that each prospective investment should include at least three alternatives (i.e., a baseline and at least two viable alternatives).

- c. To make sound investment decisions, decision-makers must consider how cost, benefit, and risk interact.

- d. The most useful financial results in an investment decision appear in a time-based cash flow summary. This summary is used to describe the alternative solutions considered for mitigating the capability gap that the investment is expected to address. Each alternative should provide comparisons of the costs over time for each alternative.

3. Identify opportunities to leverage services and technologies from other agencies or to reuse internally deployed capabilities.

- a. Assess internally reusable capabilities. As part of this activity, evaluate the agency inventory of software licenses.

Goals, Objectives, Activities
<p>b. Research other agencies' solutions; many agencies have similar security and privacy challenges and some have centrally registered available capabilities for reuse at http://www.apps.gov/. Other capabilities may be found through inquiries to OMB or other federal agencies.</p>
<p>c. Join or establish relevant communities of practice around specific unmet requirements to facilitate the creation of capabilities that are broadly applicable across the federal government.¹⁰</p>
<p>4. Identify opportunities to obtain capabilities from the marketplace. (i.e., commercial off the shelf solutions) other agencies and evaluate the opportunities for cross-agency re-use.</p>
<p>5. Evaluate alternatives and select the best option. When all the cost, benefit, and risk components have been identified, comparisons can be made to the baseline and among the viable alternatives.</p>
<p>C. Document proposed solutions</p>
<p>1. Update the enterprise architecture to reflect findings from the gap analysis and legacy capabilities analysis.</p>
<p>2. Capture proposed security and privacy solutions and alternatives using OMB and agency business case formats.</p>
<p>3. Submit proposed solutions to the Agency IRB.</p>

Section 4.3: Stage III—Selection

SECTION 4.3.1: OVERVIEW

Stage III is an enterprise evaluation of the solutions proposed in Stage II and the selection of major investments. In Stage III, the CFO and IRB lead the integration of outputs from previous stages into the Agency-wide capital planning process to ensure:

- Evaluation of individual proposals so that each fully reflects the outputs of Stages I and II
- Selection of individual proposals that best support the business, security, and privacy needs of the organization
- Documentation of the updated “to-be” architecture and sharing of reusable components.

The CFO and IRB begin by evaluating all proposals using consistent criteria. Ideally, the Stage II analysis is consistent with the evaluation criteria. The CFO and IRB are enforcing expectations articulated in enterprise architecture principles and OMB Exhibit 300 budget justification criteria. Table 5 provides a list of FEA-SPP documentation needed to meet OMB Circular A-11,

¹⁰ <http://www.et.gov/> is a growing Federal government resource that may contribute to the identification of communities of practice and associated shared capabilities.

Exhibit 300 evaluation criteria. This mapping of Exhibit 300 evaluation criteria to the outputs of the FEA-SPP applies to those investments that are dedicated privacy and security services. For other investments, the FEA-SPP outputs may only provide supporting content for the security and privacy section.

Table 3: FEA-SPP Documentation Meets Exhibit 300 Evaluation Criteria

Exhibit 300 Evaluation Criteria	FEA-SPP Documentation Support ¹¹
Acquisition Strategy	<p>Investments receive a 5 (out of 5) if the investment demonstrates a strong acquisition strategy that mitigates risk to the federal government, accommodates Section 508 as needed and uses contracts and statements of work that are performance based.</p> <p>The alternatives analysis of Stage II documents security and privacy risk for various acquisitions and favors investments that pose less risk to the federal government.</p>
Project Management	<p>Investments receive a 5 (out of 5) if the project is very strong and has resources in place to manage it.</p> <p>Stage II and III activities seek to ensure that individual investment proposals include adequate resources plans supporting security and privacy.</p>
Enterprise Architecture	<p>Investments receive a 5 (out of 5) if the investment is ...</p> <ul style="list-style-type: none"> • Included in the agency's enterprise architecture and CPIC process, and for new development projects include in the EA transition plan. • mapped to and supporting the FEA, and is clearly linked to the BRM, PRM, SRM and TRM and the business case demonstrates the relationship of the investment to the business, data, application and technology layers of the enterprise architecture <p>Stage I and II activities will clearly link the investment to the FEA and layers of the enterprise architecture.</p>
Alternatives Analysis	<p>Investments receive a 5 (out of 5) if the investment includes three viable alternatives, alternatives were compared consistently, and reasons and benefits (e.g., return on investment) were provided for the alternative chosen.</p> <p>The trade-off analysis of Stage II will provide agencies with documentation of to demonstrate effective alternative analysis.</p>
Risk Management	<p>Investments receive a 5 (out of 5) if a risk assessment was performed on all mandatory elements and risk (including security risk) is managed throughout the investment.</p> <p>Stage II encourages evaluating risks associated with each alternative.</p>

¹¹ OMB scoring criteria is adapted from OMB Circular A-11.

Exhibit 300 Evaluation Criteria	FEA-SPP Documentation Support ¹¹
Performance Goals	<p>Investments receive a 5 (out of 5) if ...</p> <ul style="list-style-type: none"> performance goals are provided for the agency and are linked to the annual performance plan the investment discusses the agency's mission and strategic goals and performance measures are provided <p>Stage I activities establish clear performance goals for security and privacy. Stage II analysis activities will ensure capabilities support these performance goals.</p>
Security and Privacy	<p>Investments receive a 5 (out of 5) if ...</p> <ul style="list-style-type: none"> security and privacy issues for the investment are addressed, all questions are answered and a privacy impact assessment is provided in appropriate circumstances security/privacy is accounted for throughout the lifecycle of the individual investment (to include budgeting for security and privacy) <p>Stages I and II link security and privacy requirements to capabilities. The trade-off analysis will support documentation of life-cycle costs.</p>
Performance-Based Management System	<p>Investments receive a 5 (out of 5) if the agency will use, or uses an earned value management system that meets the American National Standards Institute Electronics Industry Alliance Standard 748 and investment is earning the value as planned for costs, schedule and performance goals.</p> <p>The FEA-SPP activities do not explicitly map to this criteria section (this should be addressed by having Earned Value Management principles established in each investment area.</p>
Life-Cycle Costs	<p>Investments receive a 5 (out of 5) if the lifecycle costs for the investment reflect a formulation that includes all of the required resources and is risk-adjusted to accommodate items addressed in the risk management section.</p> <p>Stage II alternative analyses require the identification of realistic life-cycle costs.</p>
Supports the President's Management Agenda Items	<p>Investments receive a 5 (out of 5) if ...</p> <ul style="list-style-type: none"> it is a collaborative investment that includes industry, multiple agencies, state, local, or tribal governments, it uses e-business technologies and is governed by citizen needs (if appropriate) it is fully aligned with one or more of the Presidential initiatives. <p>Stage I and II support identification of linkages to the business objectives and opportunities to collaborate with business partners to reduce risk.</p>

Stage II promotes the development of solutions that are consistent with enterprise needs. Ultimately, it is the role and responsibility of the IRB to select a mix of solutions that optimizes business needs; maximizes available funds; and appropriately addresses confidentiality, integrity, availability, and privacy of the underlying federal information and federal information systems. This selection is made with consideration of the “as-is” and “to-be” architectures. IRBs may

wish to prioritize proposals based on various agency needs; OMB promotes the selection of shared or sharable capabilities over unique, non-shareable solutions.

Resource constraints will require the IRB to balance functional needs against security and privacy. In many cases, the centralized security and privacy investments may need to take precedence over functional capability improvements, since they are enabling technologies that may support multiple capabilities. Risk mitigation strategies must be defined and implemented to address the residual risks from unfunded security and privacy aspects of investments. Risk mitigation strategies should feed back into Stages I and II because business processes and other aspects of the enterprise architecture may need to be changed to mitigate the security and privacy risks identified.

Once the CFO and IRB make the selection, the agency will have new capabilities to document and capture in the agency enterprise architecture. The new capabilities will need to be reflected in the “to-be” architecture and the transition plan. Agencies will want to communicate results internally to ensure program offices and security and privacy stakeholders are aware of the new capabilities. Agencies should consider publicizing externally leveragable capabilities at <http://www.apps.gov>.

SECTION 4.3.2: ACTIVITIES

The following activities support Stage III goals and objectives. For each activity, agencies should identify and document the owners of associated data, the location where that data is maintained, and any corrective actions identified to improve the data or complete the activity.

Table 4: Stage III Goals, Objectives & Activities

Goals, Objectives, Activities
<p>II. Enterprise Strategy Stage</p> <p>A. Evaluate Individual Proposals.</p> <p>1. Establish and promulgate standards for documenting security and privacy aspects of proposals in a manner consistent with FEA-SPP activities and based on the adequacy of security and privacy considerations.¹²</p> <p style="padding-left: 40px;">a. Define minimally acceptable processes for assessing proposals.</p>
<p>i. Validate the identification and mapping of security and privacy controls to the five enterprise architecture reference models.</p>
<p>ii. Validate the identification and mapping of security and privacy controls to the 17 security control families and the eight privacy control families.</p>

¹² ISO/IEC Standard 21827 provides guidance for defining processes and acceptable evidence.

Goals, Objectives, Activities
<ul style="list-style-type: none"> iii. Scrutinize the alternatives considered in Stage II and the manner in which the program selected the proposed option. The review of alternatives is an essential part of effective budget planning. Require program executives to incorporate the results of trade-off analyses into OMB and agency business cases to demonstrate informed risk-based decision-making and to comply with OMB and agency budget submission requirements.
<ul style="list-style-type: none"> iv. Require compliance with OMB or agency business case criteria.¹³ This should include establishing an appropriate level of detail for security and privacy budget discussions.
<ul style="list-style-type: none"> b. Define acceptable evidence to support those processes.
<ul style="list-style-type: none"> c. Express a preference for leveraging existing capabilities.
<ul style="list-style-type: none"> 2. Reject proposals that fail to demonstrate compliance with established standards.
<p>B. Select investments.</p> <ul style="list-style-type: none"> 1. Sample Selection Criteria. <ul style="list-style-type: none"> a. Consistency. Question and closely examine justifications for deviations from the agency's inventory of approved security and privacy-related technologies and services as described in the "to-be" architecture. Security and privacy controls that lay outside the current enterprise architecture are likely to be less effective, more expensive, and less interoperable. Consider whether the goals of such investments may be accomplished differently, within the context of the current enterprise architecture. Carefully weigh the implications of approving any deviation.
<ul style="list-style-type: none"> b. Necessity. Evaluate the need for new security and privacy capabilities. <ul style="list-style-type: none"> i. Leverage Stage I activities to ensure that each security and privacy capability maps to one or more specific requirements and directly contributes to associated performance metrics.
<ul style="list-style-type: none"> ii. Evaluate existing shared security and privacy capabilities to verify that a new capability is necessary. New security and privacy capabilities should be designed to be leveragable beyond the immediate need.
<ul style="list-style-type: none"> c. Enterprise risk. Evaluate potential risks to the enterprise. <ul style="list-style-type: none"> i. Assess risks accepted through the proposed investment. Determine the impact that security and privacy choices may have on the broader enterprise.
<ul style="list-style-type: none"> ii. Assess the impact and risks of not fully funding security and privacy aspects of proposed investments. Unaddressed security and privacy requirements may impact other parts of the enterprise and other interconnected organizations.
<ul style="list-style-type: none"> iii. Establish a risk mitigation strategy for underfunded security and privacy requirements. The IRB and program executives must understand risks associated with underfunding of security and privacy requirements. Lack of investment into mitigating identified risks will increase overall risk to an agency.

¹³ OMB Circular A-11.

Goals, Objectives, Activities
<ul style="list-style-type: none"> d. Cost. Assess the adequacy of security and privacy-related budget lines. <ul style="list-style-type: none"> i. Ensure that security and privacy are budgeting throughout the lifecycle. OMB budget preparation guidance requires specific budget allocation for security management.
<ul style="list-style-type: none"> ii. Evaluate the adequacy of specific funding for functional and compliance activities across the 17 security and 8 privacy controls. For example, do they include funding for mandated security and privacy assessments? Do they include funding to provide security and privacy awareness, training, and education?
<ul style="list-style-type: none"> iii. Evaluate IT investments for which security and/or privacy are underfunded. Determine if the agency can reduce costs by leveraging other initiatives or technologies and services used elsewhere in government, including leveraging specific services or the entire capability from other agencies.
<ul style="list-style-type: none"> 2. Prioritize the funding of common solutions for security and privacy requirements. OMB requires all investments to have corresponding security budgets included and explicitly indicated in the budget, unless they satisfy the security or privacy component through another budget line item. Highlight shared security and privacy investments to ensure that they are funded. Otherwise, investments that depend upon them will not have sufficient security and privacy and may not be compliant. <ul style="list-style-type: none"> a. First, prioritize central security and privacy capabilities.
<ul style="list-style-type: none"> b. Second, prioritize other IT investments that best provide or leverage shared capabilities.
<ul style="list-style-type: none"> c. Third, fund IT investments that do not provide shared capabilities.
<ul style="list-style-type: none"> 3. Evaluate the current enterprise and newly approved security and privacy capabilities across the control families to identify opportunities to reduce risk, reduce cost, increase functionality, and increase interoperability. <ul style="list-style-type: none"> a. Identify opportunities to centralize capabilities – the senior agency officials for security and privacy should conduct a trade-off analysis to determine the best approach to centralizing capabilities.
<ul style="list-style-type: none"> b. Identify opportunities to appropriately reduce (but not eliminate) diversity of standards and approaches for accomplishing security and privacy objectives. Such changes may have a positive impact on security, privacy, interoperability, and cost, but should not be undertaken without careful consideration of the up-front costs, and especially the impact on accomplishing agency business objectives. Periodically assess the inventory of approved technologies and services to determine their sufficiency with regard to the target architecture and/or new investment proposals.
<p>C. Document outputs.</p> <ul style="list-style-type: none"> 1. Documentation <ul style="list-style-type: none"> a. Update the “to-be” architecture after each budget cycle to reflect new investments and associated residual risks. The “to-be” architecture should portray the security and privacy features of the enterprise with respect to its mission, and characterize its exposure to risks in terms of the agency’s enterprise architecture components.

Goals, Objectives, Activities	
i.	Map security impact levels in a consistent manner to types of: i) information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation); and ii) information systems (e.g., mission critical, mission support, administrative).
ii.	Determine which systems are national security systems following the guidance in NIST SP 800-59, Guideline for Identifying an Information System as a National Security System.
iii.	Map the agency technical/systems architecture to security categories in accordance with FIPS PUB 199 and NIST SP 800-60.
b.	Update the transition plan after each budget cycle to reflect activities supporting new investments. Relate security and privacy funding request to agency Enterprise Architecture components including transition plans. Effective impact analyses to the enterprise as a whole will include architecture analyses. Investments with DME funding are a component of the transition plan and may impact other ongoing or concurrent investment plans, as well as the ultimate target architecture.
c.	Generate a report from the agency's enterprise architecture system summarizing security and privacy features across each architecture component or reference model.
i.	The report should summarize key security and privacy drivers (including trust agreements established with external entities exchanging information), and enumerate the elements of the transition strategy that are funded to manage the security and privacy risks associated with fulfilling the mission of the agency.
ii.	Use the report as a baseline for future FEA-SPP iterations and with each update of the enterprise architecture and/or budget cycle.
2.	Communicate results
a.	The enterprise should ensure internal awareness of major security and privacy capabilities. Document and publicize available shared security and privacy capabilities with program developers responsible for implementing and maintaining business processes and systems. This may begin as an artifact of the agency enterprise architecture system. Outreach and publicity may provide valuable assistance to programmatic trade-off analysis efforts.
b.	The agency should consider promoting and sharing security and privacy capabilities with other federal agencies. Publish sharable security and privacy capabilities to http://www.apps.gov .

Section 5.0: Integrating the FEA-SPP with the Federal Enterprise Architecture

Section 5.1: Enterprise Architecture Overview

Enterprise Architecture is a technique for documenting, evaluating, and planning organization business objectives and the business activities, information, standards, and capabilities that support those objectives. “A Practical Guide to Federal Enterprise Architecture” defines enterprise architecture as *“a strategic information asset base, which defines the mission, the information necessary to perform the mission, and the transitional processes for implementing new technologies in response to the changing mission needs”* (Chief Information Officer Council Version 1.0, February 2001).

Agency enterprise architectures typically contain three components: (1) baseline, or “as-is” architecture, (2) future, or “to-be” architecture and (3) transition plan, or modernization blueprint. The component of the enterprise architecture which presents the existing enterprise strategy, the current business practices and the associated technical infrastructure is defined as a “baseline” or “as-is” architecture. The “as-is” architecture can be used to reduce costs and increase interoperability. By helping organizations become aware of existing assets, they can develop enterprise solutions with reuse and interoperability in mind.

The second component of the enterprise architecture, the “target” or “to-be” architecture, describes the desired, future state for an organization. Like the “as-is” architecture, the “to-be” architecture defines the enterprise in terms of its strategy, business, and technical dimensions. The third component of an enterprise architecture, the “transition plan” or “modernization blueprint” presents the plan for how an agency will transform from its baseline or “as-is” state to its target or “to-be” state. The transition plan speaks to the lifecycle of the security and privacy controls at each level of the enterprise architecture.

Section 5.2: The Three Levels of Enterprise Architecture

There are three levels of scope within enterprise architecture: (1) enterprise level, (2) segment level, and (3) solution level.

Level	Scope	Detail	Impact	Audience
Enterprise Architecture	Agency/ Organization	Low	Strategic Outcomes	 All Stakeholders
Segment Architecture	Line of Business	Medium	Business Outcomes	 Business Owners
Solution Architecture	Function/ Process	High	Operational Outcomes	 Users and Developers

Figure 5: Levels of Enterprise Architecture

Enterprise-level architecture is concerned with identifying common or shared assets – whether they are strategies, business processes, investments, data, systems or technologies. Enterprise architecture is driven by strategy and helps an agency identify whether its resources are properly aligned to agency mission, strategic goals and objectives. From an investment perspective, enterprise architecture is used to drive decisions about the IT investment portfolio as a whole. Consequently, the primary stakeholders of the enterprise architecture are the senior managers and executives tasked with ensuring the agency fulfills its mission as effectively and efficiently as possible. However, all stakeholders within and outside of an agency can benefit from the enterprise architecture.

Segment architecture defines a roadmap for a core mission area, business service or enterprise service. From an investment perspective, segment architecture drives decisions for a business case or group of business cases supporting a core mission area or common or shared service. The primary stakeholders for segment architecture are business owners and managers.

Segment architecture is related to enterprise architecture through three principles: structure, reuse and alignment. First, segment architecture inherits the framework used by the enterprise architecture, although it may be extended and specialized to meet the specific needs of a core mission area or common or shared service. Second, segment architecture reuses important assets defined at the enterprise level including data, common business processes and investments, and applications and technologies. Third, segment architecture aligns with elements defined at the enterprise level, such as business strategies, mandates, standards and performance goals.

Solution architecture defines agency individual IT assets such as applications or components used to automate and improve individual agency business functions. The scope of solution architecture is typically limited to a single project and is used to implement all or part of a system or business solution. The primary stakeholders for solution architecture are system users and developers.¹⁴

Additional levels of scope for federal enterprise architectures are in work by the FEA Program Management Office (FEAPMO) that encompass multi-agency and multi-line of business initiatives. These levels would accommodate “sector” and “government-wide” architecture initiatives, including those that involve stakeholders with State, Local, and Tribal agencies as well as industry, academic, and international groups. Security and privacy controls for these new levels of scope will need to be developed when FEAPMO provides guidance on architecture methods at these new levels.

Section 5.3: The Relationship Between the FEA and the RMF

The FEA-SPP provides a risk-based framework to help agencies incorporate security and privacy into the enterprise architecture for federal operations. This FEA-SPP, however, evidences that security and privacy, while interrelated concepts, are not identical in their methodologies or in the maturity of their existing documentation. The privacy community is continuing to develop best practice tools to support privacy programs throughout the federal government and will supplement the FEA-SPP with these tools as they are developed.

The FEA-SPP brings together the concepts of the FEA and the NIST RMF to derive a security profile at the enterprise, segment and solution (or system) levels of the agency. The FEA-SPP recognizes the influence of SDLC and maintenance processes in that it provides a sequence of program activities. The FEA-SPP uses this and other agency governance processes to ensure proper compliance with program management best practices and information security regulations regarding the management of information security process, activities and controls. Figure 6 shows the relationship between the FEA and NIST RMF which serve as the foundation for the FEA-SPP:

¹⁴ Federal Enterprise Architecture Practice Guidance (November 2007).

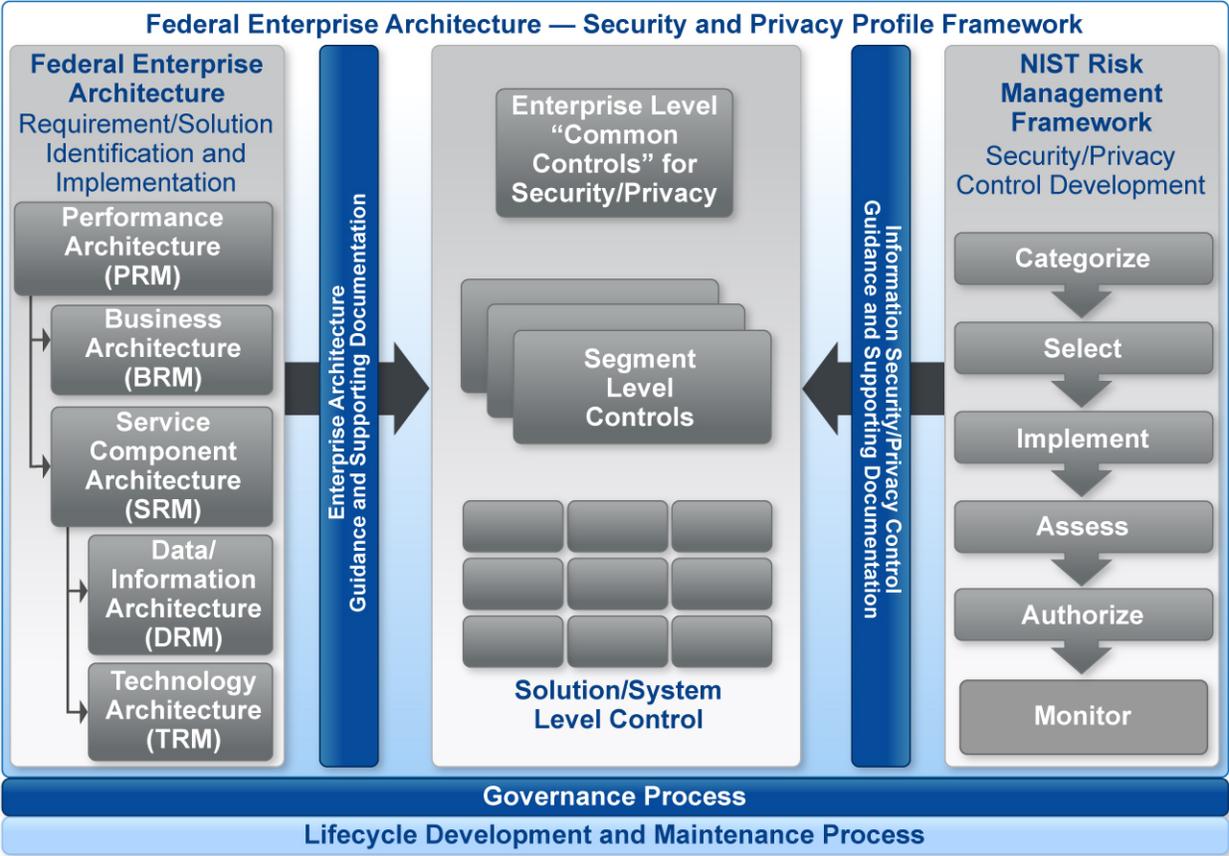


Figure 6: The FEA-SPP Framework

In Figure 6, the FEA-SPP Framework, the left side of the FEA-SPP represents the FEA and the five reference models. The reference models establish common taxonomies of performance goals and measures, lines of business, services, technologies and data for organizing and managing agency enterprise architectures. At the center of the figure are the segment architectures represented at each of the three levels of the OMB FEA framework (i.e., enterprise, segment, and system/solution). Security controls, derived from the RMF, are mapped and implemented at each of the three architectures levels. The right side of the FEA-SPP framework in Figure 6 represents the NIST RMF guidelines for managing risk to organizational operations, organizational assets, and individuals. Adherence to these guidelines results in the development of security controls that are applied at the three segment architectures, and are effectively integrated across those three levels.

The FEA and NIST RMF processes should utilize the same data sources to begin their respective processes; i.e., mission statement, strategic goals and objectives, legislative mandates, common or shared business and information requirements. Utilizing the shared set of inputs, the output of the FSAM “Analyze” and “Define” phases aid in defining and categorizing a system and its data as part of the initial security categorization phase of the RMF. This is accomplished by mapping enterprise/organizational assets; i.e., programs, processes, information, applications, technology, investments, personnel, organizations, and facilities to the agency-level reference models to create a segment-oriented view of the enterprise. Enterprise/organizational assets are mapped to the organizational mission and goals in relation to the agency enterprise architecture by utilizing

the FEA Performance Reference Model (PRM) to define measurement areas, measurement categories, and measurement groupings. This analysis leads to the identification and mapping of organizational business areas (measurement areas), LOB (measurement categories), and sub-functions (measurement groupings) through the use of the FEA BRM to an enterprise, segment, or solution architecture.

The key output from the FEA Business Reference Model (BRM) that integrates the NIST RMF and FEA is the identification of the sub-functions. The FEA BRM sub-functions map to the information types that support the segment architecture. The NIST RMF utilizes the information type(s) identified from the FEA BRM as input data to perform the security categorization of federal information and information systems. Security categorization provides a vital step in integrating security into the agencies' business and information technology management functions and establishes the foundation for security standardization across segment architectures and information systems. The result is strong linkage between missions, information, and applications through the RMF.

The NIST RMF starts with security categorization, which is dependent on the identification of what information supports which government lines of business (as defined by the FEA) and the resultant segment architectures as described above. The NIST RMF includes guidance from NIST Special Publication 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I and Volume II) which provides guidance on the assignment of security families to information systems. The NIST RMF provides guides on the assignment of security control families to segment architectures as per the following governing legislation and guidance:

- E-Government Act 2002 (P.L. 207-347) Title III Federal Information Security Management Act (FISMA), which addresses the specification of minimum security requirements for federal information and information systems
- Federal Information Processing Standards (FIPS) 199, which establishes security control families for both information and information systems
- FIPS 200, which established security-related controls to evaluate information systems
- OMB Circular A-130, which establishes policy for the management of federal information resources.
- Privacy Act of 1974, which establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.
- OMB Memoranda addressing privacy and security requirements.
- Paperwork Reduction Act as it pertains to information collections by federal agencies.
- Federal Records Act as it pertains to retention schedules.

The FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems) provides guidance to organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity,

and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security families that have been determined for each type of information as identified from the FEA PRM and BRM analysis.

For federal civilian architectures the “high-water mark” concept is used to determine the impact level of the information system for the specific purpose of selecting an initial set of security controls from one of the three security control baselines (i.e., common, hybrid, system-specific) defined in NIST Special Publication 800-53, Revision 3. Thus, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high-impact system is an information system in which at least one security objective is high. Once the overall impact level of the information system is determined, security controls can be selected from the minimum controls recommended by NIST for low, moderate, or high baselines. Each of the three baselines provides an initial set of security controls for a particular impact level associated with a security category. These controls represent the minimum mandatory controls, although depending on the system control enhancements may be employed.

Section 5.4: The Relationship Between FEA-SPP and the FEA Reference Models

The FEA is a business-based framework for government-wide improvement. The goals of the FEA are to locate and reduce or eliminate duplicative investments, discover areas where investments should be made, and identify where departments and agencies can collaborate to improve government operations or services. Initial FEA efforts involve mapping government operations to five “reference models.” Figure 7 depicts the reference models and demonstrates how these five models interrelate and are mutually supporting. Their purpose is to facilitate cross-agency collaboration that will lead to greater consistency and efficiency in support of citizen-focused delivery of services. While each agency’s enterprise architecture will be unique, all agency enterprise architectures should map to the five reference models.

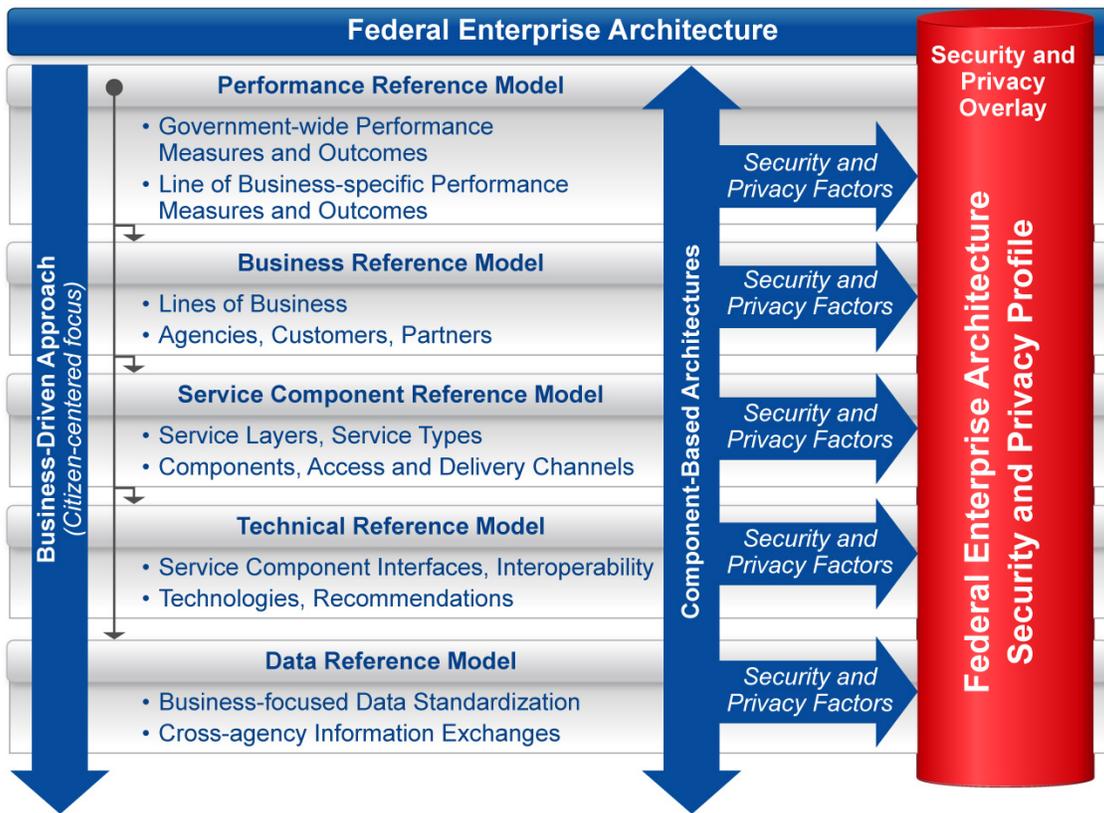


Figure 7: FEA Reference Model & SPP Relationship

Section 5.5: The Enterprise Architecture Perspective on Security and Privacy

Linking security and privacy to an agency enterprise architecture has two major benefits:

1. Integrating security and privacy into agency performance objectives, business processes, service-components, technologies, and data helps to ensure that each aspect of the business receives appropriate security and privacy attention.
2. Describing security and privacy using enterprise architecture reference models promotes interoperability and aids in the standardization and consolidation of security and privacy capabilities as appropriate.

Enterprise architecture discussions of security and privacy span two types of capabilities. In some instances, security or privacy features may be inherent in a particular asset, such as the security features built into a web server, or part of a particular service, such as the web security and privacy policy for an e-Gov initiative. In other instances, security or privacy may be the primary objectives of a capability; e.g., an Internet firewall protecting an organization web site. Agency enterprise architectures must capture information about both types of capabilities and document their security and privacy features across each reference model. Doing so enables agencies to better understand and align security and privacy activities to the business and performance objectives of the organization. In addition, effectively representing security and

privacy information in the enterprise architecture ensures that security and privacy are adequately included in the lifecycle processes of the agency.

By defining the desired end-state from several distinct perspectives (e.g., business, data, technology), the target FEA provides stakeholders with a view into the complex relationships that exist among these different perspectives. Security and privacy considerations must be addressed within all layers of the target architecture: performance, business, services and applications, data, and technology.

Section 6.0: Integrating Security / Privacy and the FSAM

Section 6.1: FSAM Overview

The FSAM top level consists of five process steps that help architects:

- identify and validate the business need and scope of the architecture
- define the performance improvement opportunities within the segment
- define the target business, data, services, and technology architecture layers required to achieve the performance improvement opportunities.

The FSAM process concludes with the creation of a modernization blueprint document that includes a transition sequencing plan for using and implementing the segment architecture; refer to Appendix D for a detailed overview of the FSAM.

The FSAM can produce 54 potential artifacts (see Appendix E: FSAM Artifacts) which can be useful inputs for various security practices. The FEA-SPP identifies security controls at three levels; i.e., enterprise, segment and solution/system. Per NIST 800-39, “Security controls should be reflected in the FEA solution architectures and should be traceable to security requirements allocated to mission/business processes defined in the FEA segment architectures.” The Federal Information System Controls Audit Manual (FISCAM) states, “The consistency of the entity’s enterprise architecture and IT strategy with its business strategies can affect the proper planning and implementation of IT systems and related security.”

An output of the FSAM process using the FEA-SPP framework will be an Enterprise Information Security Architecture (EISA). An EISA is a set of artifacts that describe the business architecture and what security controls are required. Specifically, for the FEA-SPP, these controls will be newly identified or inherited at the segment level, and all three levels of controls will be tracked in the EISA, which is likely to be an additional component of the program’s enterprise architecture repository.

Section 6.2: Using the FSAM to Implement Security & Privacy Controls

FSAM can be used to implement security and privacy controls across the five process steps of segment architecture activities. FSAM security and privacy integration is a strategic initiative that defines the business security requirements and provides the backbone for secure enterprise solutions. FSAM security and privacy integration accomplishes this by aligning functional, organizational (internal and external stakeholders), system boundaries and trust models to protect federated data. The FEA-SPP framework is flexible and aligns to the five FSAM steps that assist security and privacy stakeholders with an opportunity to define the business and performance improvement outcomes consistent with the risk levels determined through the FEA-SPP. The FSAM security and privacy integration touch points are shown in Figure 8.

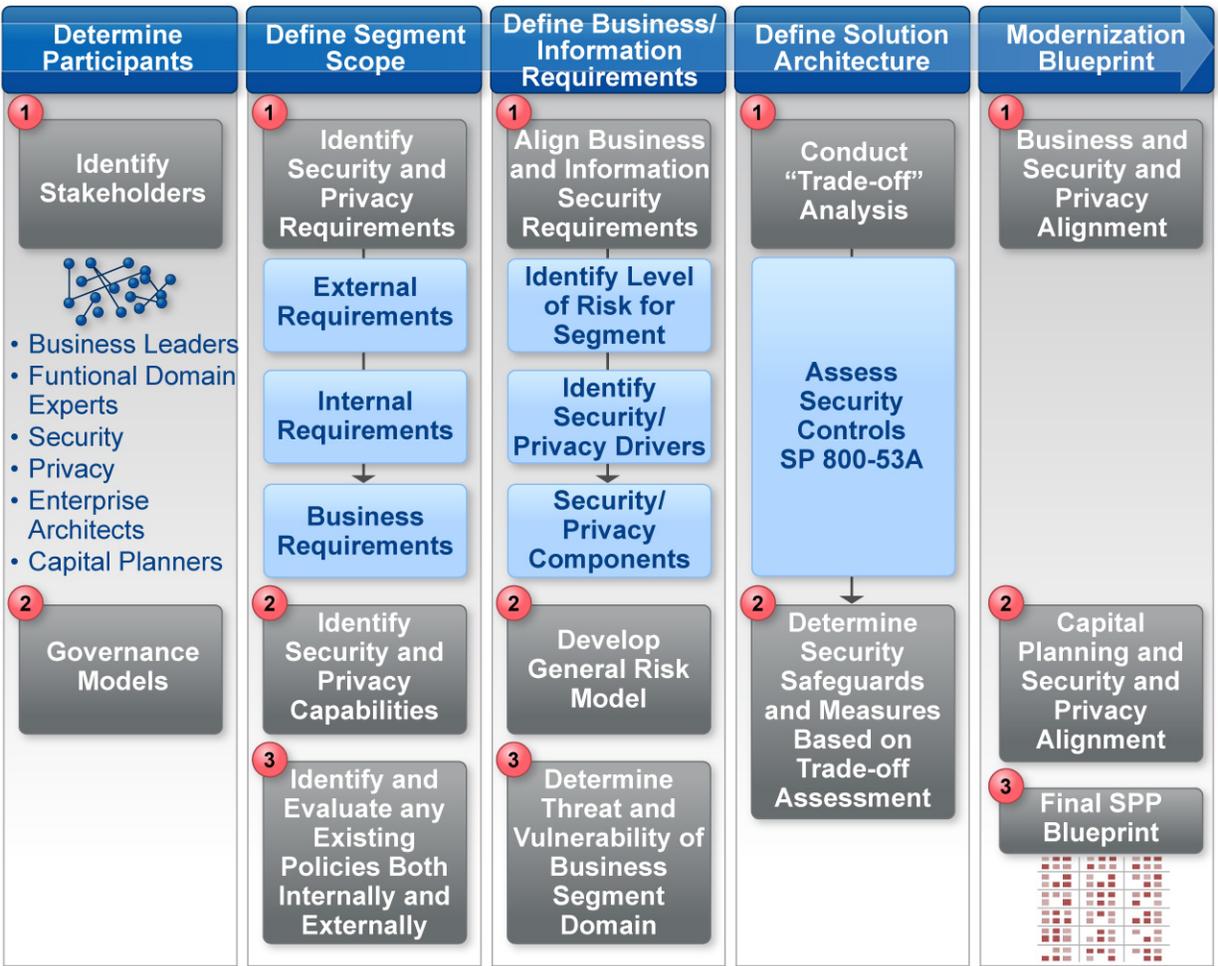


Figure 8: The FSAM Privacy & Security Touchpoints

Section 6.3: The Relationship Between FEA-SPP Methodology Process and the FSAM

The FEA-SPP methodology supports security and privacy officers and other key stakeholders to ensure that the security and privacy aspects are considered, fully defined, and to provide the information necessary for key investment decision makers to make informed decisions based on segment workflow analysis. Each of the FSAM process steps are important with establishing an understandable, consistent, repeatable, scalable, and measurable methodology for deriving a set of security and privacy controls that best meet the segments business requirements. The five FSAM security and privacy integration process steps are:

1. Determine Participants and Launch the Project
2. Define the Segment Scope and Strategic Intent
3. Determine Business/Information Requirements
4. Define the Conceptual Security Solution Architecture
5. Author the Modernization Blueprint

Step 1 – Determine Participants and Launch the Project

The use of this methodology requires the coordinated efforts of business leaders and functional domain experts, including security, privacy, enterprise architecture, and capital planning. By working together, these individuals enable secure business transformation. Agencies may wish to consider inclusion of other key stakeholders who can make significant contributions to the methodology such as representatives of the acquisitions, contracts, and legal departments. Ideally, implementation of the FEA-SPP includes the following officials:

Table 5: Suggested FEA-SPP Officials

Roles	Responsibilities
Chief Information Officer (CIO)	The CIO is responsible for information resource management and will be a natural stakeholder for the FEA-SPP methodology.
Senior Agency Official for Security	The senior agency official for security has primary responsibility for security in the agency and should be familiar with external and internal security requirements as well as the enterprise-level capabilities currently in place to satisfy those requirements. The senior agency official for security also contributes knowledge of the organization's current security posture. More than one security official may be needed support the FEA-SPP methodology in agencies where security responsibilities are decentralized.
Senior Agency Official for Privacy / Chief Privacy Officer	The SAOP/CPO has overall responsibility and accountability for ensuring the agency's implementation and compliance with respect to information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to privacy. The SAOP/CPO also has a central policy-making role at the agency and is involved in all activities that involve personally identifiable information. Privacy may have several advocates within an agency.
Chief Enterprise Architect	The Chief Enterprise Architect has primary responsibility for developing and promoting the operationalization of the enterprise architecture of an organization. In light of those responsibilities, the Architect may be the best person to lead FEA-SPP activities and to capture outcomes.
Chief Financial Officer (CFO)	The CFO has responsibility for planning, proposing, and monitoring major agency investments. The CFO is also often the chair of agencies' investment review boards (IRB). The FEA-SPP goal of promoting better-informed and more strategic investment decisions makes it important that the CFO participates in this process. By following the guidance in the FEA-SPP, an organization is more likely to effectively address security and privacy requirements in Exhibit 300 and Exhibit 53 submissions.
Program Officials	Program officials are responsible for accomplishing the business of an agency. They drive decisions about investments, and are responsible for planning and budgeting for security and privacy. While security and privacy officials will be knowledgeable about enterprise security and privacy requirements, program officials may have unique, programmatic requirements. Senior agency officials' decisions in the course of developing the FEA-SPP will impact the program-level as the program officials will implement many of the security and privacy decisions. Including program officials in the FEA-SPP activities will ensure that decisions made will be practical and useful to everyone.

This list is not exhaustive and agency officials may wish to expand this list to meet specific, organizational needs. The methodology discussions include activities that may benefit from other agency officials' inputs. Additional considerations for agency officials may include establishing a formal governance process or leadership structure when initiating FEA-SPP activities. In addition, agency officials may want to review the stages of the methodology to gain a common understanding of the goals, objectives, and activities among all team members. Team members can help translate requirements as necessary.

Step 2 – Define the Segment Scope and Strategic Intent

Segment architects need to ensure that security and privacy laws, directives, policy guidance, strategic goals, and objectives are established to determine compliance, risks, and safeguards for agency segments. The goal of this stage is to encourage federal organizations to address security and privacy at the beginning of the business process/IT systems development effort when high-level requirements are being defined. Within this step, the FEA-SPP assists agencies in, first, identifying security and privacy needs for segment artifact and then linking those needs to NIST guidance at the program and system levels in support of segment. For example, a particular LOB Comments on the draft FEA-SPP v3.0 may achieve its strategic objectives by using a variety of systems; however, it is the process that sets them apart. An agency would use NIST SP 800-60 and FIPS 199 to determine what the impact of loss of systems would be for each of the three security objectives: confidentiality, integrity and availability. In some cases, it may be necessary to decompose the LOB further to the sub-function and process level to achieve a level of detail necessary to engage the process or business owners and partners in determining specific elements of risk. This additional information will allow accountable officials to make informed risk based decisions to drive the selection of appropriate security and privacy controls, leveraging NIST SP 800-30.

The FEA-SPP provides a complementary integration taxonomy that guides accountable decision makers in risk-based decision-making. The shared security and privacy concerns can be documented as part of the baseline agreements in information and data sharing that cross traditional organizational boundaries. Stakeholders will benefit through their ability to make well-informed decisions, thus leading to highly accurate, effective IT capital planning and increased coordination between stakeholder counterparts; e.g., business managers, infrastructure operators. The resulting guidance ensures that IT security and privacy priorities are tied to business and mission needs and may support identification of a common, initial set of security and privacy controls for systems sharing the same categorization within a given segment.

Step 3 – Determine Business / Information Requirements

The FEA-SPP facilitates early identification and understanding of essential security and privacy requirements. The FEA-SPP assists agencies in defining four variables that support well-informed, risk-based decision-making:

1. **Initial Risk Exposure** By analyzing information from the FEA reference models, stakeholders can develop an initial estimate of the risk exposure associated with any given business process¹⁵. This is accomplished by examining security patterns based

¹⁵ A formal risk assessment should be conducted once the actual system design begins. See NIST Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems.

on threats, risks, security and privacy mechanisms and the development and operational costs of applying those mechanisms. Alternatives should be defined based on the risk versus ease-of-use attributes of the alternatives. If the initial estimate is too high, business owners can save both time and money by looking for other options earlier in the process.

2. **Range of Controls** The FEA-SPP will allow stakeholders to initiate discussions early in the process by addressing the range of controls that may be available to support security and privacy goals. The methodology helps business owners understand the nature, extent, multfluence, and impact that controls have on LOB, business processes, or IT systems. Knowing the range of controls provides stakeholders the ability to determine alternative approaches in mitigating risk, with alternatives being fundamental to the decision-making process.
3. **Relevant Potential Costs** The FEA-SPP provides information to derive potential costs associated with controls. As with risk exposure, these costs will be projected at the “rough order-of-magnitude” (ROM) level, rather than the precise determinations that will be developed when the system’s physical design has been initiated. Identifying financial impacts early may help avoid costly redesign or unexpected costs later in the process.
4. **Options Analysis** The FEA-SPP helps business owners in risk-based decision-making achieve security objectives by establishing a range of options. In the options analysis, business owners specify the level of service performance desired, view an initial set of security controls providing a level of residual risk, and determine if the associated cost is acceptable. The result is an ROM cost estimate that can be analyzed against a predetermined budget or cost feasibility plan. If the initial estimates are too high, business owners can reassess—or reduce—the types of controls needed to mitigate risk, thereby increasing residual risk yet reducing cost. Thus, within the options analysis, stakeholders can begin to prioritize mitigation strategies in determining the most effective balance of benefit, cost, and risk factors.

In addition, the FEA-SPP methodology paves the way for establishing trust among partners. By using a common approach and documenting decisions that result from an options analysis decision, business partners (government-to-government or government-to-business) will be able to better understand what decisions were made, why a given set of controls was adopted, and whether any changes should be made to protect a similar or interconnecting LOB.

Step 4 – Define the Conceptual Security Solution Architecture

Developing a conceptual security architecture solution requires an analysis of alternatives for agency security and privacy requirements, and the existing or planned capabilities that support security and privacy. As a result of this activity an agency will be able to:

- Identify gaps between requirements and current or planned capabilities
- Identify opportunities to increase interoperability between or reduce costs of current or planned capabilities

- Propose solutions to address gaps or improve capabilities based on an informed trade-off analysis of alternatives.

The discovery of gaps between requirements and capabilities will assist federal agencies with identifying and mapping requirements and capabilities to the enterprise architecture and control families. The FEA-SPP team reviews each control family, comparing each requirement in a family to available components. Requirements that are not satisfied by an existing component are noted as gaps. In this example, an agency is likely to determine that no agency capability fully supports the FISMA requirement to conduct security awareness training – a gap has been identified.

The analysis supports the optimization of security and privacy capabilities. This optimization promotes improved security and privacy functionality, increased standardization and interoperability, and reduced risk. Historically, agencies selected capabilities based on programmatic needs. They may not have considered the impact of local choices on the broader enterprise security and privacy posture; or, the environment may have changed, leading to unexpected impacts. Similarly, agencies may not have considered the opportunities for savings inherent in building interoperable or standardized capabilities. Agency TRMs document standards that drive standardization and interoperability. The selection of solutions consistent with agency TRMs reduces costs and increases interoperability through reduced integration costs and increased standardization. Lastly, over time, agencies may have unintentionally deployed redundant capabilities among which one or more could be phased out to achieve cost savings.

Outside the FEA-SPP, there are numerous system and program assessments that use common evaluation criteria across a wide set of capabilities. Consider the example of the FIPS PUB 199 security categorization. Each variation in need for confidentiality, integrity, and availability leads to a mandated baseline set of security controls. It follows that if multiple systems in an environment share the same security categorization, they share the same baseline security control requirements. Certification and accreditation assessments may reveal for any given control that:

- Some systems will fail to exhibit the control
- Some systems will have the independent capability to support the control
- Some systems may leverage a shared capability to support the control.

Depending on the complexity and cost of the control, those situations may imply a need to standardize or even centralize the provision of certain controls. The provision of smart cards for identification and authentication is an example of a control that would be costly and inefficient to replicate across an agency.

Step 5 – Author the Modernization Blueprint

Some artifacts which are listed as outputs in the “Summary of FSAM Outputs and Suggested Analytical Techniques” in the FSAM toolkit, map directly to the eighteen security control families in the NIST 800-53. An example is the optional “Risk and Impacts” document which could be used as input to the risk assessments for the individual systems contained in the segment. The FSAM core team could identify a risk at a coarse business perspective; e.g., a lack of role-based security in a financial segment; NIST Control User Identification and

Authorization IA-02. In the certification and accreditation risk assessments for the financial systems the likelihood and impact of this, and other risks, would be mathematically assessed and scored at the systems or solution level. Ideally, this early identification of a gap during the enterprise architecture phase in a control such as IA-02, could allow for early action prior to closing the gap from an enterprise architecture perspective or mitigate the risk from a security perspective. In this example, the gap could be identified and CPIC/alternatives analysis performed earlier and more effectively than during the security certification and accreditation process at the individual system level.

Integration of the FSAM and security and privacy practices cannot be totally prescriptive. For example, the FSAM outputs from Step #1 related to governance framework are not explicitly security-related or identified as such in the FSAM guidance. If an organization were to be assessed from a Control Objectives for Information (COBIT) and related Technology / Certified Information Systems Auditor (CISA) perspective, IT governance is one of the first areas to be audited. Without proper security representation in the governance framework, it would be possible to “govern out” security concerns and makes them a lower priority. For illustration, a Strengths-Weaknesses-Opportunities-Threats (SWOT) analysis might find functional weaknesses and privacy weaknesses, it is important for the “baked in” concept of security for these security gaps be addressed as early in the lifecycle as possible, to achieve proper funding and executive and business owner sponsorship.

Section 6.4: Example: Leveraging the FSAM to Understand and Improve the Enterprise

In the example shown in Figure 9 for a financial segment, all systems will inherit OMB A-127 requirements for system integration and other controls, while non-financial systems will not necessarily inherit these controls. For a Human Resources (HR) segment containing PII, a specific control related to technical controls (such as encryption) may be emphasized. These controls should be communicated as design goals from a solutions architecture perspective.

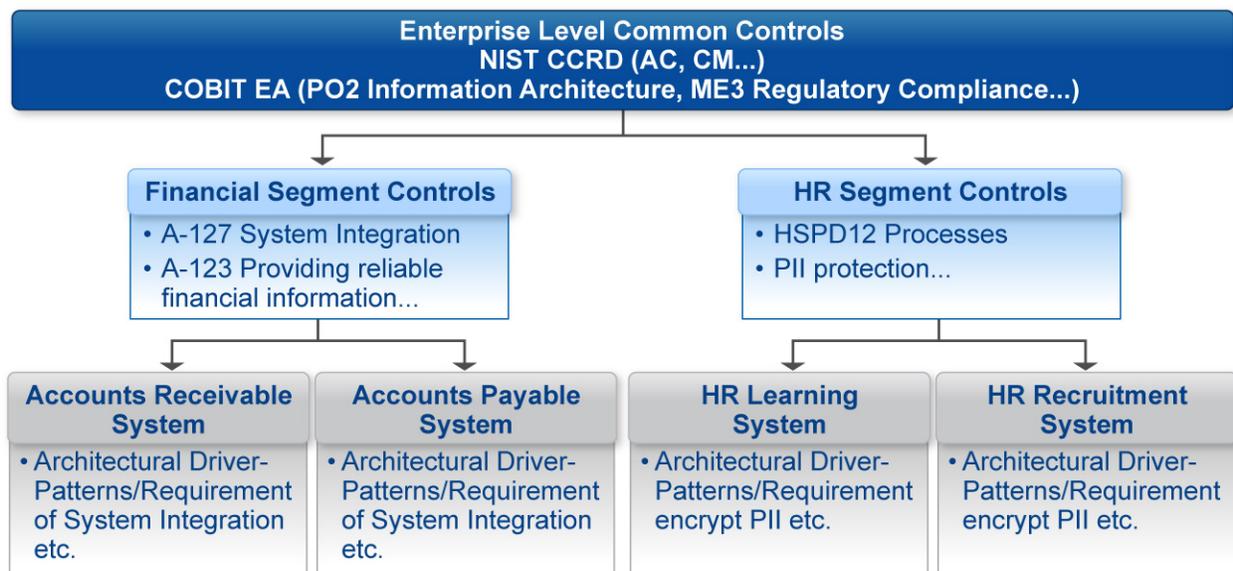


Figure 9: Example: IT Security & Privacy Inheritance

A properly structured and populated PRM is critical for enterprise architecture influence on security and privacy controls and progress measurement. To continue with the Financial Segment example, the lack of system integration could be captured in the PRM as a number of systems in the financial segment which are un-integrated. As progress is made, this number would be decremented and the need to integrate these systems would be made explicit as a design goal in artifacts from the FSAM. It is important to note that the strategy described here emphasizes the “build from” aspect of segment architectures as opposed to the “decide from” aspect used for executive decision making and CPIC that has had traction to date. Another measurable output of the FSAM which would be critical in this example is standard data classifications for recording financial events in the segment, an attribute of an integrated financial management system according to the OMB office of Federal Financial Management. It would be difficult for individual project teams with separate contractors to achieve this goal at the project level without this enterprise architecture standardization input. Ideally, the FSAM will uncover relevant security controls as part of the interview and discovery activities. This is also an excellent example of how segment and solution level architectures should inherit key standards and components from the overall agency enterprise architecture.

Appendix A: The FEA-SPP Assessment Tool

The FEA-SPP Assessment Tool (Version 4.0) has been developed to help users determine a baseline of security, privacy, and security costs requirements that are needed for a federal enterprise architecture (at the enterprise, segment, and solution levels), federal process, or federal information system based on the following:

- The security categorization of data that is processed, stored, transmitted, managed, or reviewed in accordance with FIPS-199 for Civilian Federal Agencies, Department of Defense (DoD) 8500.1 for DoD, or the Committee on National Security Systems (CNSS) 1199 for the Intelligence Community (IC);
- The phase of the SDLC or acquisition phase; and
- The type of assessment method being used (see below).

The FEA-SPP Assessment Tool integrates NIST Procedures (e.g., RMF, SCAP), Committee on National Security Systems (CNSS), and the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) into a tool that can be used for security lifecycle planning. The RMF supports the development and implementation of security and privacy controls using NIST procedures and FEA guidance, planning to provide users with the ability to understand and select information security and privacy controls relevant to the system or process risk associated with the mission of the Agency. The FEA-SPP Assessment Tool works under the assumption that the system or process has undergone a preliminary security. It also works under the assumption that the user understands what phase of the SDLC (initiation, development, implementation, maintenance, or disposition) or acquisition lifecycle (pre-acquisition, acquisition, or sustainment) the system or process is in. The FEA-SPP software is also more effective if the organization has undergone a common control selection and has a clear understanding of when, where and how agency specific controls apply. The idea behind the software is that it will de-scope controls based on the Security Categorization (SC), the phase of the SDLC (1-5) or Acquisition phase (1-3), and what type of FEA-SPP the user is developing.

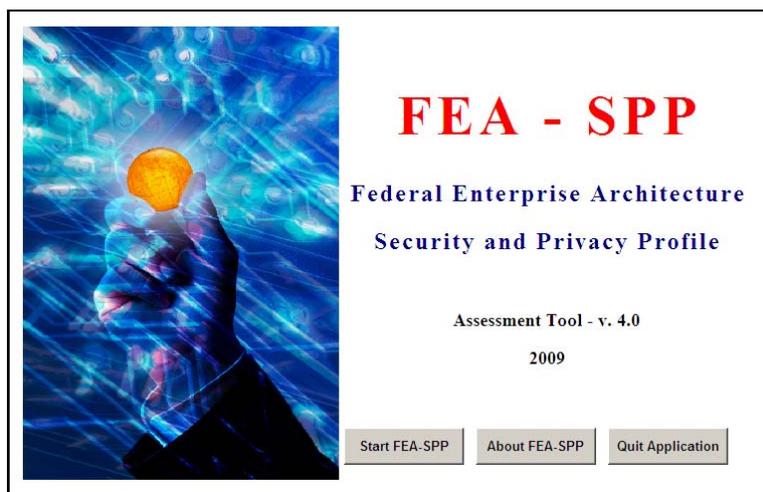


Figure A- 1: FEA-SPP Assessment Tool

Figure A- 2: FEASPP Assessment Tool – New Report Creation

The FEASPP Assessment Tool can also be used to estimate the costs related to implementing security controls (and to the extent these controls also support privacy objectives, some of the privacy costs as well). The FEASPP Assessment Tool uses all of the FEASPP information (security categorization, SDLC, and FEASPP type) plus information related to (1) the size of the information system, (2) hourly costs, (3) software and hardware costs, and (3) how the security control is going to be designed, mitigated, or fully remediated into the information system.

id	curr. archi	Responsible	Planned implement. Date (WHEN)	Lifecycle phase (implement.)	Hourly Rate	Hours Sugg	No. Hours	Software/Hardware Cost	Comments
AC	002	Richard Vaccaro			\$100.00	80	80	\$0.00	
AC	003				\$100.00	40	80	\$0.00	

Figure A- 3: FEASPP Assessment Tool – Security Controls

The FEA-SPP Assessment Tool is part of a pilot program to develop a platform- and product-neutral application that reflects the policies and procedures in security, privacy, and architecture related federal law and guidance. The tool is only provided as an example of how the FEA-SPP principles can be operationalized.

The tool is web-based, XML compliant, and provides for the addition of agency-specific security and privacy controls as well as other lifecycle development phases. The tool also provides for the ability to assess security costs.

Appendix B: FEA-SPP History

Background

In September 1999, the Federal CIO Council published the "Federal Enterprise Architecture Framework" (FEAF) Version 1.1 for developing an enterprise architecture within any federal agency or system that transcends multiple inter-agency boundaries. The FEAF provided a standard for developing and documenting architecture descriptions of high-priority areas. It proposed guidance in describing architectures for multi-organizational functional segments of the federal government.

The Office of Management and Budget (OMB) and the Chief Information Officer (CIO) Council's Architecture and Infrastructure Committee specified the need for an additional view of the FEA that addressed and highlighted elements of security and privacy. To that end, the Federal Chief Information Officers Council published an initial version of the FEA-SPP in August 2004. The second version of the FEA-SPP included a methodology and additional guidance.

FEA-SPP Version 1.0

The initial version of the FEA-SPP was developed by volunteers collaborating with the Architecture and Infrastructure Committee (AIC), of the Chief Information Officers Council. The AIC develops policy, direction, and guidance in concert with the Federal Enterprise Architecture Program Management Office (FEA PMO) to drive business process improvement, investment management, and technical decisions. The partnership of the AIC and the FEA PMO was designed to further the development and implementation of the FEA. The purpose of the AIC is to support the CIO Council's mission for a federal government that is transparent and responsive in servicing citizens and business needs and agile in meeting critical mission requirements.

The CIO Council envisioned the initial version of the FEA-SPP as a process to support stakeholders in identifying and implementing the level of protection necessary to mitigate or manage threats, risks, exposures, and vulnerabilities. To achieve this vision, the council established four objectives for developing the FEA-SPP:

1. Ensure the same management rigor that is applied to each FEA reference model is equally applied to security and privacy;
2. Address security and privacy throughout the decision-making process;
3. Facilitate early identification and understanding of essential security factors and establish a set of security and privacy services and patterns that can be trusted and shared among the government community; and
4. Ensure the approach integrates with National Institute of Standards and Technology (NIST) guidance thus fostering the integration of information assurance with enterprise lifecycle management practices.

The FEA-SPP recommended an overlay on each FEA reference model that could be used to:

- Assist agencies in, first, identifying security and privacy needs and then linking those needs to NIST guidance at the program and system levels in support of the LOB;
- Translate procedural security and privacy requirements found at the business level into the managerial, operational and technical controls necessary at the system level
- Promote early identification of security and privacy issues; and
- Disclose possible risk exposure, type of controls needed to manage the risk, potential costs for controls, and possible ways to combine controls to achieve the same goal at a lower cost.

FEA-SPP v 1.0 enumerated and explained some of the key concepts of security and privacy that needed to be addressed by agencies when building and managing their IT infrastructures, and recommended that security and privacy requirements be integrated in the FEA Reference Models. This document was, principally, a requirements document directing the establishment of more specific guidance. Before concluding, the subcommittee established a working group and modest funding to establish a methodology for addressing these requirements.

FEA-SPP Version 2.0

Version 2.0 integrated “disparate perspectives of program, security, privacy and capital planning into a coherent process, using an organization's enterprise architecture efforts.”

In short, version 2.0 of the FEA-SPP:

- Promoted an understanding of the organization's security and privacy requirements, its capabilities to meet those requirements and the risks to its business;
- Helped program executives select the best way to meet the requirements and improve current capabilities, using standards and services that are common to the enterprise or government; and
- Improved agencies' processes for incorporating privacy and security into major investments.

Version 2.0 also outlined a methodology that asked agencies to:

- Identify the program's needs and capabilities;
- Analyze how to effectively address those needs with a consideration to using existing systems to reduce costs;
- Select the tools to improve the security and privacy of systems including ensuring the agency had asked for adequate funding and the effort was coordinated across the department.

Version 2.0 of the FEA-SPP provided a three-stage methodology with a multi-disciplinary approach to ensure that an agency or business segment's security and privacy investments met business requirements. Each stage of the methodology included an introduction of the goals and objectives of that stage, and a collection of associated activities that promoted the accomplishment of those goals and objectives. Figure B-1 depicts the three stages of FEA-SPP version 2.0.



Figure B- 1: FEA-SPP V 2.0 Methodology Stages

More specifically, each stage of the methodology included an introduction of the goals and objectives of that stage and a collection of associated activities that promote the accomplishment of those goals and objectives. Table B-1 presents the three stages of the FEA-SPP methodology and contrasts the FEA-SPP’s enterprise approach with programmatic approaches. The FEA-SPP provides agencies with a framework to take both a program and enterprise perspective of security and privacy requirements and capabilities to ensure investments are managed more effectively. The goal of version 2.0 was for federated organizations to identify opportunities to share resources and capabilities across domains, programs, and agencies.

Table B- 1: FEA-SPP Methodology

Stage	Program Approach	Enterprise Approach
Stage I Identification	What are my program’s needs and capabilities?	How do my program’s needs and capabilities relate to those of my agency?
Stage II Analysis	How can I effectively and cost-efficiently address outstanding needs?	Can I reduce costs by leveraging currently deployed federal agency solutions?
Stage II Selection	Have I requested adequate funding to accomplish programmatic goals?	Have I requested adequate funding to accomplish mission goals in a manner consistent with my Agency’s security and privacy requirements? Are security and privacy features of investments coordinated across the organization?

Appendix C: The FEA Reference Models

Table C-1 describes the five FEA reference models and provides suggestions for how agencies may wish to document security and privacy in these reference models. Traditionally these reference models may not have considered security and privacy, but the table below indicated how security and privacy considerations can be included in each of them. As agencies capture security and privacy features in their enterprise architectures, they will be able to identify unmet requirements, determine what capabilities may be improved, and make strategic decisions that are best for the enterprise as a whole.

Table C- 1: FEA Reference Models

Reference Model	Description
Performance Reference Model (PRM)	<p>Information in the PRM helps agencies monitor the performance of an investment and/or program. By defining and tracking specific performance objectives and metrics, agencies are able to use the data to support portfolio decision-making, process improvement efforts, improve service-delivery approaches, improve underperforming programs, and leverage existing performance management tools across the federal government.</p> <p>Security and Privacy fall under PRM Measurement Area “Process and Activities.” Measurement Indicators show the extent to which security is improved and privacy addressed. Examples of security and privacy indicators include:</p> <ul style="list-style-type: none"> • Percentage of employees who received annual privacy and security awareness training • Percentage of agency websites with a machine-readable privacy policy • Percentage of systems with certification and accreditation • Percentage of applicable systems with a privacy impact assessment
Business Reference Model (BRM)	<p>Information in the BRM helps agencies understand what primary business functions are provided to citizens through the definition of business areas, lines of business and sub-functions.</p> <p>Various business areas, lines of business, and sub-functions are exposed to different types and levels of security and privacy risk. “Security and Privacy” is a support activity that falls under the “Management of Government Resources” Business Area. Various aspects of security and privacy will fall under the Information and Technology line-of-business and Administrative line-of-business. Sub-functions include IT Security and Security Management.</p>
Service-Component Reference Model (SRM)	<p>The SRM contains documentation of agencies’ capabilities. These capabilities are then mapped to service domains and service types. By understanding and classifying capabilities, agencies are better able to discover government-wide capabilities that can be leveraged.</p> <p>Non-security and non-privacy capabilities may have security or privacy features. Most security-specific capabilities will be located under the Service Domain “Support Services” under the Service Type, “Security Management.” “Audit Trail Capture and Analysis” is an example of a Service Capability within Security Management.</p>

Reference Model	Description
Technology Reference Model (TRM)	<p>The TRM contains documentation of the technologies and standards used to support the service components. It provides a component-driven, technical framework that categorizes the standards and technologies to support and enable the delivery of Service Components and capabilities. It provides a foundation to advance the reuse and standardization of technology and service-components from the agency and government-wide perspectives.</p> <p>Security is a Category under the Component Framework; however, an agency TRM will likely reference security and privacy in several areas. For example, “Data Types/ Validation” under Service Interface and Integration/ Interoperability. The data types may determine unique security and privacy requirements.</p>
Data Reference Model (DRM)	<p>The DRM asks, “What data and information does the Department have to support the business objectives.” The DRM describes the data at an aggregate level and enables agencies to describe the types of interaction and exchanges occurring between the federal government and citizens. Currently, the DRM standardizes three aspects of data management:</p> <ul style="list-style-type: none"> • Data Description: Provides a means to uniformly describe data, 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 community of interest • 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, re-occurring transactions between parties <p>Data described, contextualized and shared through the DRM may include personal information and/or proprietary information that will trigger security and privacy requirements. For example, data sharing involving social security numbers may require chain of trust agreements.</p>

As demonstrated above, security and privacy can be reflected in each reference model. As OMB continues to review security and privacy features in agency enterprise architectures, common taxonomies will continue to evolve and be appropriately included in the FEA reference models. For example, the BRM does not currently describe security activities in any more detail than the sub-function of IT security management. Additionally, only the PRM explicitly identifies privacy. Despite these omissions, agencies should still capture security and privacy to fully support the agency enterprise architecture goals.

Appendix D: The Federal Segment Architecture Methodology

The top level FSAM process steps are shown in Figure D-1:

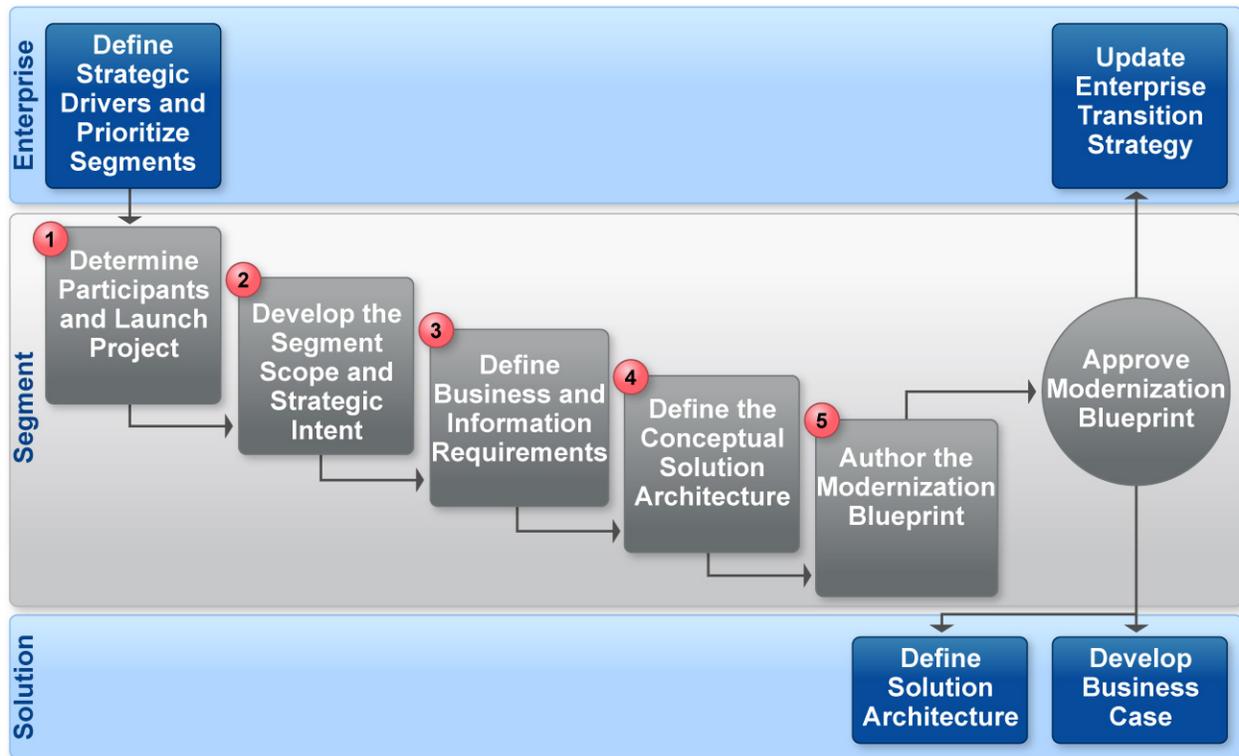


Figure D- 1: The FSAM Process

The OMB FEA Practice Guidance requires each agency to prioritize its segments and select a segment to architect. Once this is completed, the agency’s architects can leverage the FSAM to work with segment leadership to assign executive sponsorship, ensure participation of business owners, and develop a business-owner-approved segment architecture blueprint. Each of the FSAM process steps is important in the development of complete and actionable segment architecture. In order for the segment architecture to be “actionable”, it must include specific, measurable milestones and deliverables that, once achieved, will lead to the targeted performance improvements. The five FSAM process steps are:

1. Determine Participants and Launch the Project
2. Define the Segment Scope and Strategic Intent
3. Determine Business/Information Requirements
4. Define the Conceptual Security Solution Architecture
5. Author the Modernization Blueprint

Step 1: Determine Participants and Launch the Project The architect leverages the guidance in this process step to engage with key stakeholders to establish the segment

governance framework, validate the business owner(s) for the segment, formally appoint an executive sponsor and a core team, and establish the purpose statement to guide the architecture development. This process step also includes guidance for introducing a solid project management foundation for the segment architecture development effort with the creation of a project plan and communications strategy. Key questions addressed within this process step are similar to those that one might normally ask when initiating a project:

- What is the governance framework for the development of the segment architecture?
- Does the business owner(s) understand the process and time commitment for developing the segment architecture?
- Who is the executive sponsor?
- Who is on the core team? Are these the right people?
- What is the specific purpose for developing this segment architecture?
- Is the charter approved to develop the segment architecture in the context of the purpose statement crafted by the business owner(s)?
- Is there a project plan and communications strategy for developing the segment architecture?

Step 2: Define the Segment Scope and Strategic Intent The architect leverages the guidance in this process step to engage with key stakeholders to produce a segment scope and to define the strategic improvement opportunities for the segment. The architect then defines the segment strategic intent which consists of the target state vision, performance goals, and common / mission services and their target maturity levels. The subsequent FSAM process steps provide guidance for architects to align the architecture with the strategic intent to create a complete segment performance line-of-sight and to support achieving the target state vision. Key questions addressed within this process step include:

- Based on the high-level problem statement, what are the strategic improvement opportunities and gaps?
- What are the major common / mission services associated with the strategic improvement opportunities?
- Who are the segment stakeholders and what are their needs?
- What is the scope of the segment architecture?
- What are the current segment investments, systems, and resources?
- What are the deficiencies or inhibitors to success within the segment?
- What is the target state vision for the segment?
- What is the performance architecture for achieving the target state vision?

Step 3: Define Business and Information Requirements The architect leverages the guidance in this process step to engage with key stakeholders to analyze the segment business and information environments and determine the business and information improvement opportunities that will achieve the target performance architecture. Within this step, the architect begins with developing a broad, holistic view of the overall business and information requirements associated with the strategic improvement opportunities identified in the previous step. Information requirements include the information exchanges that relate to the critical business processes associated with the performance improvement opportunities. The business and data architectures are derived from these requirements. The business and data

architectures developed at the end of this step may include the specification of business and information services respectively, and should be sufficiently complete and actionable to result in more efficient processes and allocation of resources. Key questions addressed within this step include:

- How well does the current (“as-is”) business and information environment meet the needs of the segment stakeholders?
- How should the target business and information environment be designed?
- Have the segment’s goals and performance objectives been translated into actionable and realistic target business and data architectures expressed within business functions, business processes, and information requirements?
- Have the business and information requirements been analyzed and documented to the lowest level of detail necessary to form actionable recommendations?
- Did the business and information analysis provide a synchronized and cohesive set of recommendations?
- Does the core team understand the adjustments that are required for the current business and information environments to fulfill the target performance architecture?

Step 4: Define the Conceptual Solution Architecture The architect leverages the guidance in this process step to engage with key stakeholders to produce the conceptual solution architecture. The conceptual solution architecture is an integrated view of the combined systems, services, and technology architectures that support the target performance, business, and data architectures developed in the preceding process steps. This process step also includes guidance for developing recommendations for transitioning from the current (“as-is”) state to the target state. The conceptual solution architecture produced at the end of this step is of benefit to segment and solution architects as well as to downstream capital planning and budget personnel. Key questions addressed within this step include:

- What existing systems and services are deployed within the “as-is” conceptual solution architecture?
- How well do the existing systems and services currently support the mission?
- Which systems and services should be considered for retirement and / or consolidation?
- How should the target conceptual architecture be designed to fulfill the target performance architecture?
- Are the selected target systems, components, and services reusable?
- Does the conceptual solution architecture support the target performance, business, and data architectures developed in prior steps?
- Have the dependencies, constraints, risks, and issues associated with the transition been analyzed to identify alternatives to be considered?
- Are there existing external services that can be leveraged in the target architecture?

Step 5: Author the Modernization Blueprint The architect leverages outputs from previous process steps to engage with key stakeholders to create a segment architecture blueprint including sequencing and transition plans. The outcome of this process step is a series of validated implementation recommendations supported by holistic analysis of segment business, data, technology, systems, and service components. The modernization blueprint includes findings and recommendations as well as supporting artifacts and diagrams that

illustrate the analysis performed throughout the architecture development process. For instance, artifacts such as the SWOT analysis and the conceptual solution architecture are key visuals in the modernization blueprint. Note that recommendations in the modernization blueprint typically span a strategic time horizon on the order of 3-5 years. Key questions addressed within this step include:

- Have the strategic improvement opportunities from process step 2 been supported in the analysis, recommendations, and transition planning?
- Have the findings from the previous process steps been identified, categorized, and prioritized?
- Have the transition options been analyzed for costs, benefits, and risks in order to develop recommendations for implementation?
- Are the recommendations clearly described in the blueprint?
- Has the blueprint and sequencing plan been reviewed and approved by the executive sponsor, business owner(s), and core team?

The FSAM has been designed to assist architects as they develop and use actionable segment architectures. The outputs from the FSAM have also been designed specifically for use within other downstream processes, including investment management, enterprise transition planning, solution architecture development, and system lifecycle management.

Appendix E: FSAM Artifacts

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)							Suggested Analytical Technique
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAFF Reporting	Solution Development	Security / Privacy	Value Proposition	
Step 1	Governance framework	No			S				Identifies key roles and responsibilities for segment architecture development and shows relationships to existing governance bodies.	Governance framework
Step 1	Segment architecture development purpose statement	Yes	S	S	C	C			Articulates the issues that the segment architecture will address. Guides the core team in the development of the segment architecture.	Segment architecture development purpose statement
Step 1	Core team roster	No			S				Identifies core team and provides organizational and contact information.	Core team roster
Step 1	Core team formation memorandum	No			S				Communicates the existence of the core team, its members, and its purpose.	Core team formation memorandum
Step 1	Core team charter	No			S				Establishes the authority of the project, roles and responsibilities, operational ground rules, decision-making structure, preliminary scope, and stated objectives and goals.	Core team charter
Step 1	Project plan	No			C				Guides the segment architecture development process and ensures timely delivery.	Project plan
Step 1	Communications strategy	No			C				Identifies core stakeholders and ensures that messaging requirements for all stakeholders have been identified and planning for key communications has been accomplished.	Communications

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)							Suggested Analytical Technique
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAAF Reporting	Solution Development	Security / Privacy	Value Proposition	
Step 2	Stakeholder and their relationship	No	S		S	S			Identifies the appropriate stakeholders and the relationships between them and the servicing organization. Ensures the inclusion of all relevant perspectives on how to overcome the business challenges identified in the segment purpose statement.	Stakeholder map
Step 2	Business drivers and mandates	Yes	S		C				Provides the foundation from which the segment's performance line-of-sight will be built, demonstrating the linkage to the strategic, business, and investment improvement opportunities identified in subsequent steps.	Driver and policy map
Step 2	Segment scope	Yes			C	S			Helps build consensus within the core team on the range of strategic improvement opportunities and helps focus core team working sessions.	Segment summary
Step 2	Segment context	No			S	S			Provides a visual context diagram corresponding to the segment scope.	Current operating environment diagram
Step 2	Stakeholder needs	No			S				Provides the basis for formulating the consolidated business needs of the segment.	Stakeholder
Step 2	Risks and impacts	No		S	S		S	S	Identifies potential high-level risks and impacts associated with the segment scope and context, including risks not addressed optimally by the current environment.	Risk capture template

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)							Suggested Analytical Technique
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAAF Reporting	Solution Development	Security / Privacy	Value Proposition	
Step 2	Performance gaps	Yes	S	S	C	S	S	S	Identifies current state performance gaps in order to facilitate prioritization of performance improvement opportunities.	Performance gap analysis
Step 2	Strategic improvement opportunities	Yes	S	S	C	S	S	S	Identifies internal and external factors which affect the achievement of the segment purpose statement. Prioritizes performance improvement opportunities and aligns them with the business needs of the organization as a whole.	SWOT analysis
Step 2	Segment performance goals and objectives	Yes	S	S	C	S	S	S	Establishes the key performance indicators, measures, and metrics that will be used to measure the achievement of segment goals and vision.	Strategic alignment of opportunities
Step 2	Common / mission services target maturity levels	No	S		S				Establishes the target maturity levels required to achieve the segment vision according to segment strategic performance goals and objectives.	Common / mission services maturity framework
Step 2	Segment architecture vision summary	No	S		S				Summarizes the purpose, scope, mission and target vision for the segment, in text and visual forms.	Segment summary
Step 2	Performance scorecard	Yes	S	C	S	C	S	S	Includes strategic, business, program and segment performance data. Conforms to EAAF 3.0 reporting requirements	Performance scorecard

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)						Suggested Analytical Technique	
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAAF Reporting	Solution Development	Security / Privacy		Value Proposition
Step 3	"As-Is" business value chain	No			S	S	S	S	Identifies the high-level logical ordering of the chain of processes that deliver value.	"As-Is" business value chain analysis
Step 3	"As-Is" business function model	Yes				S	S	S	Identifies the business functions that will be affected by potential process improvements. Ensures that processes are analyzed in context with the correct business functions and that appropriate mappings to the FEA BRM are established.	"As-Is" business function model
Step 3	"As-Is" key business process model	No				S	S	S	Defines processes that may require process optimization. Assists in determining high-level information and information security requirements.	"As-Is" business activity model
Step 3	"As-Is" business process swim lane diagram	No				S	S	S	Defines processes that may require process optimization. Assists in determining high-level information and information security requirements.	"As-Is" business process swim lane diagram
Step 3	"As-Is" key information sources and qualitative assessment	No				S	S	S	Documents the sources of information in the current state and determines the most trusted sources of data by information class and data entity.	Authoritative Data Source (ADS) candidate qualitative analysis matrix

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)							Suggested Analytical Technique
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAAF Reporting	Solution Development	Security / Privacy	Value Proposition	
Step 3	Business and data architecture adjustment profiles	No	S	S		S	S	S	Groups related opportunities and formally documents the limitations of the current state, desired characteristics of the target state, how the target state will help achieve strategic improvement opportunities, and risk and cost considerations.	Business and data architecture adjustment profiles
Step 3	Target business value chain diagram	No	S	S		S	S	S	Identifies differences in the processes that are currently being provided between the current and target states. Helps determine where new processes are required and where existing processes may no longer be necessary.	Target business value chain analysis
Step 3	Target business function model	Yes				C	C	C	Identifies the business functions that will be affected by potential process improvements. Ensures that processes are analyzed in context with the correct business functions and that appropriate mappings to the FEA BRM are established.	Target business function model
Step 3	Target key business process model	No				S	S	S	Defines optimized processes as required to achieve segment performance objectives. Assists in determining high-level information and information security requirements.	Target business activity model

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)						Suggested Analytical Technique	
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAAF Reporting	Solution Development	Security / Privacy		Value Proposition
Step 3	Target business process swim lane diagram	No				S	S	S	Defines optimized processes as required to achieve segment performance objectives. Assists in determining high-level information and information security requirements.	Target business process swim lane diagram
Step 3	Target conceptual data model	Yes				C	C	C	Provides the structure and terminology for information and data in the target environment. Includes subject areas, information classes, key entity types, and relationships.	Target conceptual data model
Step 3	Target data steward assignments	Yes				C	C	C	Identifies the organization responsible for the creation, maintenance and quality of each information class appropriate to support business activities in the target environment.	Target data steward matrix
Step 3	Target business data mapped to key business processes (CRUD)	No				S	S	S	Help identify candidate information services, including new authoritative data sources, and producers and consumers of information.	CRUD matrix results table
Step 3	Target information sharing matrix	Yes				S	S	S	Assists in discovery of opportunities for re-use of information in the form of information-sharing services, within and between segments.	Target information sharing matrix
Step 3	Target Information Flow Diagram	Yes				S	S	S	Assists in discovery of opportunities for re-use of information in the form of information-sharing services, within and between segments.	Target information flow diagram

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)							Suggested Analytical Technique
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAAF Reporting	Solution Development	Security / Privacy	Value Proposition	
Step 4	"As-Is" system and services scoring	No					S	S	Determines where adjustments to the segment systems and services architecture should be investigated.	"As-Is" systems and services description and scoring
Step 4	"As-Is" conceptual solution architecture	Yes					C	C	Shows the existing systems and services in the "as-is" state and identifies the relationships between them. May also include an overlay to show the boundaries of key business functions and external organizational interfaces.	"As-Is" system interface diagram
Step 4	Target conceptual solution architecture	Yes		C			C	C	Shows the proposed systems and services in the target state and identifies the relationships between them. May also include an overlay to show the boundaries of key business functions and external organizational interfaces.	Target system interface diagram
Step 4	Target Service Component Architecture	Yes		C			C	C	Describes service components and the mechanisms for providing service delivery to customers. Provides a framework and vocabulary for guiding discussions between service providers and consumers.	Service component model (SCM)
Step 4	Target Technical Architecture	Yes		C			C	C	Shows the technology components that support service delivery for each SCM service component.	Technology model
Step 4	Integrated service component and technology model	No					S	S	Shows the service-to service interaction, supporting technical components, and information flows associated with each service component. Used to derive the TRM.	Integrated service component and technology model

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)							Suggested Analytical Technique
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAAF Reporting	Solution Development	Security / Privacy	Value Proposition	
Step 4	Transition recommendation profile	No			S		S	S	Describes a recommended transition alternative. May include intermediate target states and alternative recommendations based on multiple funding levels.	Transition recommendation profile
Step 4	Transition recommendation sequencing diagram	No			S		S	S	The single, consolidated diagram that shows the transition recommendation sequencing milestones for an implementation alternative.	Transition recommendation sequencing diagram
Step 4	Reuse Summary	Yes		C		C			Describes segment reuse of business, system, and service components from other segments and by other segments. Conforms to EAAF 3.0 reporting requirements.	Reuse summary
Step 4	Data Reuse	Yes		C		C			Describes segment reuse of information exchange packages and data entities from other segments and by other segments. Conforms to EAAF 3.0 reporting requirements.	Data Reuse
Step 4	Recommendation Sequencing Milestones	Yes		C	S	C			Preliminary version of the Step 5 Target Recommendation Sequencing Milestones. Conforms to EAAF 3.0 reporting requirements.	Recommendation sequencing milestones

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)						Suggested Analytical Technique	
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAAF Reporting	Solution Development	Security / Privacy		Value Proposition
Step 5	Analysis of cost, value and risk for transition options	No			S		S	S	Informs the prioritization (selection and sequencing) of transition options to formulate a set of implementation recommendations.	Value measuring methodology cost to value matrix
Step 5	Proposed implementation recommendations	No				S	S	S	Comprises the set of implementation recommendations that are used to develop the recommended high-level implementation plan.	Draft recommendation implementation overview visual
Step 5	Strategic systems migration / sequencing overview	Yes			C	S	C	C	The single, consolidated diagram that shows the transition recommendation sequencing recommendations for the selected implementation recommendations.	Recommendation sequencing diagram
Step 5	Recommendation implementation sequencing plan	No			C	S	S	S	Sequencing plan that includes all tasks associated with the overall transition of business processes, systems and services to achieve the target state. Identifies internal and external dependencies as milestones or predecessor tasks.	Implementation sequencing plan
Step 5	Segment architecture blueprint document (incl. sequencing plan)	Yes	S		C	S	C	C	Description of the overall segment transition plan that is focused on implementation of the business transformation recommendations. Contains descriptions of some of the key analysis performed in prior process steps.	Modernization blueprint

Process Step	Output	FSAM Core Output (Y/N)?	Support for Existing Mandatory Requirements and Management Processes (C=Core, S=Support)							Suggested Analytical Technique
			Strategic Planning	Capital Planning / Budget	Mission / IT Governance	EAAF Reporting	Solution Development	Security / Privacy	Value Proposition	
Step 5	Segment Mappings	Yes		C		C			Provides the FEA CRM mappings for the segment and shows the relationship between the segment and its investment portfolio, PART programs supported, and government-wide FTF and e-Gov initiatives.	Segment mappings
Step 5	Transition Plan Milestones	Yes	S	C	C	C	C	C	Provides the implementation and performance improvement milestones for the segment transition plan.	Transition plan milestones
Step 5	Document review log	No			S				A log used to collect review comments and change requests for the segment architecture blueprint.	Document review form
Step 5	Feedback tracking document and feedback action report	No			S				A log used to record feedback and document and track follow-up actions.	Feedback tracking and action report

Appendix F: Privacy Control Families – Descriptions and Explanations

Table F-1 provides guidance to assist agencies in the implementation of the privacy control families¹⁶ outlined in the FEA-SPP. The privacy control families are based upon the FIPPs. The FIPPs are widely accepted in the United States and internationally as a general framework for privacy. In a number of agencies, the FIPPs serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies. The privacy control families support agencies with complying with the full framework of privacy requirements; they do not supersede, modify, or interpret any law, regulation, or executive branch policy.

Each privacy control family corresponds to one of the eight FIPPs. The descriptions and explanations, described below, elaborate upon the privacy control families and are illustrative of the actions recommended to implement each. Agencies may identify additional actions, as this guide is not intended to be comprehensive. Agencies must analyze and apply each privacy control family to their distinct mission and operation based on their agency's respective legal authorities and obligations. Implementation of specific controls may vary based upon this analysis.¹⁷

The first three steps agencies must take when building or implementing privacy into a new or modified program, information system, technology, or any other business-related activity are:

- (1) Identify the types of PII involved;
- (2) Identify the legal framework (i.e., statutes, regulations, and policies) that must be applied; and
- (3) Implement steps to comply with the legal framework.

These key steps – identifying the types of PII, identifying agency specific legal requirements, and implementing steps to comply with the identified legal framework – are fundamental to the successful application and implementation of each privacy control family. By identifying the legal framework for the program or system, the agency is then able to appropriately consider legitimate national security, law enforcement, and privacy interests, and provide clear rules to those who handle the PII on how the FIPPs should be applied. For example, law enforcement and intelligence programs and systems, particularly those that are classified, will require modifications of the FIPPs in light of their legal and operational requirements.

Agencies should also consider and apply the privacy control families to activities involving technologies, data management, or other interactions with the public, contractors, or employees

¹⁶ “Control” refers to the specific management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the information within the system. “Family” refers to the broader category within which controls are categorized.

¹⁷ Identification of specific controls in support of a privacy control family is determined by the agency mission. For example new Health Insurance Portability and Accountability Act (HIPAA) regulations mandate breach notification under the American Recovery and Reinvestment Act (ARRA).

that may not involve the collection and use of PII, but nevertheless may raise privacy risks or concerns (e.g. the use of surveillance video or body imaging screening devices).

The privacy control families are interrelated, such that, action taken in one family likely will affect the implementation of another. The privacy control families also are not in any particular order and should be considered individually and as a whole when applying them to any agency mission or activity that may impact the privacy of the public or employees. That means that the families are iterative and must be revisited from time to time to determine the impact of changes to any particular family.¹⁸

Table F-1: Privacy Control Families

Privacy Control Family	Description	Explanation
<p>Transparency</p>	<p>Providing notice to the individual regarding the collection, use, dissemination, and maintenance of PII.</p>	<p>Enhance public confidence that the Government has disclosed any collection of PII.</p> <ul style="list-style-type: none"> • Provide notice through methods such as Privacy Act's system of records notice (SORN) and e(3) notices, or the E-Government Act's privacy impact assessment. • Publicly disclose privacy policies and analyses for a program, system, or technology. • Develop privacy policies in plain language so they are easy to read and comprehend. • Publish privacy policies online and in the Federal Register consistent with OMB guidance. • Make publicly available reports documenting agency compliance with privacy commitments. • Consider real time notice where appropriate and feasible.

¹⁸ An alignment of specific privacy controls to each privacy control family is under development. An example includes system of records notices (SORNs) to transparency and privacy impact assessments (PIAs) to accountability, etc.

Privacy Control Family	Description	Explanation
Individual Participation and Redress	Involving the individual in the process of using PII and seeking individual consent for the collection, use, dissemination, and maintenance of PII. Providing mechanisms for appropriate access, correction, and redress regarding the use of PII.	<p>Enhance public confidence by providing individuals with reasonable access to their information and the opportunity to correct, amend, or delete their information when it is inaccurate.</p> <ul style="list-style-type: none"> • Provide clear notice to the public through Privacy Act statements, privacy policies, and SORNs about how the program, system, or technology will collect, process, share, and protect their PII. Also provide notice for access and redress to the public. • To the greatest extent possible, provide the notice before or at the time of the collection. • Obtain individual consent to the extent practicable from the individual with regard to the collection, use, and disclosure of their PII and inform individuals about their choices, as well as the consequences of not providing the requested information. Where individual consent is not practicable, provide notice to the general public in the Federal Register and on Government websites. • Provide clear notice to individuals of their rights under the Privacy Act for access and amendment of records and other redress programs. • Establish procedures for allowing individuals to access, correct, and amend their PII. • Establish procedures for allowing individuals to seek redress for privacy-related complaints and violations involving the processing of their information.
Purpose Specification	Specifically articulating the authority that permits the collection of PII and specifically articulating the purpose or purposes for which the PII is intended to be used.	<p>Enhance public confidence by identifying the legal bases, directives, statutes, and any other authoritative directions that authorize PII collection.</p> <ul style="list-style-type: none"> • State all purpose(s) for which the PII is being collected and how the information is used.

Privacy Control Family	Description	Explanation
Data Minimization & Retention	Only collecting PII that is directly relevant and necessary to accomplish the specified purpose(s). Only retaining PII for as long as is necessary to fulfill the specified purpose(s) and in accordance with the National Archives and Records Administration (NARA) approved record retention schedule.	<p>Enhance public confidence that the Government only collects and retains information that is needed for the stated purpose.</p> <ul style="list-style-type: none"> Identify the minimum set of PII that is necessary and relevant to accomplish the legally-authorized agency purpose. The minimum data set may be a subset of the data the organization is authorized to collect. Not all relevant data may be necessary to accomplish the purpose(s) for which it was collected. Perform periodic evaluations of all of the data collected to ensure the data collected is necessary per the defined purpose of the information collection. Retain and destroy PII in accordance with the NARA-approved record retention schedules. Use audits and appropriate technology to ensure secure deletion or destruction of PII.
Use Limitation	Using PII solely for the purpose(s) specified in the public notice. Sharing information should be for a purpose compatible with the purpose for which the information was collected.	<p>Protect against mission creep and enhance public confidence that the scope of the information use does not extend beyond authorized purposes.</p> <ul style="list-style-type: none"> Use PII only for the purposes specified in the public notice or as legally authorized. Obtain prior approval for any new use or disclosure of PII to ensure such use is consistent with the notice and other approved privacy documentation including SORNs, Privacy Threshold Analysis (PTAs), Privacy Impact Assessments (PIAs), and sharing agreements or equivalent tools. For IT systems that collect and / or disseminate PII, limit the capabilities of the system to ensure that the system is not capable of collecting additional information or disseminating information beyond that for which it is authorized. Conduct periodic reviews of the PII collection and use to assess compliance. Limit disclosure of PII to authorized third parties in accordance with applicable notices, policies, and other legal requirements. Use audits and appropriate technology to support compliance with use and disclosure limitations.

Privacy Control Family	Description	Explanation
<p>Data Quality and Integrity</p>	<p>Ensuring, to the greatest extent possible, that PII is accurate, relevant, timely, and complete for the purposes for which it is to be used, as identified in the public notice.</p>	<p>Enhance public confidence that any PII collected by the Government is accurate, relevant, timely, and complete for the purpose for which it is to be used, as identified in the public notice.</p> <ul style="list-style-type: none"> • Incorporate mechanisms into program and system development and implementation to determine, at the point of collection (or shortly after) and periodically thereafter, that collected PII is, and continues to be, accurate, relevant, timely, and complete for the publicly stated purposes. • Collect information directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under federal programs. • Routinely check and update as necessary programs and systems through which individuals receive benefits, to determine if inaccurate or outdated PII could result in incorrect characterizations of eligibility, denial of benefits, or other harm. • For systems that collect PII for law enforcement or intelligence purposes, additional corroboration of information is necessary before any reliance is made that may affect an individual's rights.
<p>Security</p>	<p>Protecting PII (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.</p>	<p>Enhance public confidence that any PII collected by the Government is appropriately safeguarded against loss, unauthorized access or disclosure.</p> <ul style="list-style-type: none"> • Determine the level of information sensitivity and identify the level of privacy risks related to potential security risks. Based on that determination and by active cross-functional participation with the information security officer, work collaboratively to establish the necessary suite of safeguards based on the NIST security control families. • Tailor security controls and safeguards to help protect PII from loss, misuse, unauthorized access, disclosure, alteration or destruction. Mitigate privacy risks to the greatest extent practicable. • Develop an incident response plan designed to respond promptly to data privacy incidents. A response plan must provide for appropriate mitigation of risk and notification to individuals and agencies as specified in OMB guidance.

Privacy Control Family	Description	Explanation
<p>Accountability and Auditing</p>	<p>Providing accountability for compliance with all applicable privacy protection requirements, including all identified authorities and established policies and procedures that govern the collection, use, dissemination, and maintenance of PII. Auditing for the actual use of PII to demonstrate compliance with established privacy controls.</p>	<p>Enhance public confidence through effective monitoring and measuring controls to demonstrate that the Government is complying with all applicable privacy protection requirements.</p> <ul style="list-style-type: none"> • Determine the level of information sensitivity and identify applicable statutory, regulatory, agency-specific requirements, policies, and procedures. • Create, disseminate, and implement privacy policies, procedures, and compliance audit systems that govern the appropriate privacy and security controls for the agency's respective program, system, or technology. Privacy reviews and controls should be integral components of life-cycle development. This will help in early identification and mitigation of risks. • Aid compliance with privacy policies by clearly defining roles and responsibilities, conducting routine oversight to monitor compliance, and providing staff (including management) with the training needed to fulfill their respective privacy responsibilities. • Obtain senior management support for expanding training for implementation of privacy risk prevention and information security procedures. • Ensure senior managers and oversight officials regularly receive results of the monitoring and evaluation of privacy controls.

Glossary

<p>Artifact</p>	<p>A product or byproduct of the enterprise architecture development process. Examples can include completed FEA reference models, architecture diagrams and process models.</p>
<p>Business Reference Model (BRM)</p>	<p>An organized, hierarchical construct for describing the day-to-day business operations of the Federal government. The BRM is the first layer of the Federal Enterprise Architecture and it is the main viewpoint for the analysis of data, service components and technology. Information in the BRM helps agencies understand what primary business functions are provided to citizens through the definition of business areas, lines of business and sub-functions.</p>
<p>Cloud Computing</p>	<p>Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flow charts and diagrams.</p>
<p>Common Security Controls</p>	<p>Common security controls are identified by how they are applied by the organization. Common security controls can apply to: all organizational information systems; a group of information systems at a specific site; or common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites. Common security controls have the following properties:</p> <ul style="list-style-type: none"> • The development, implementation, and assessment of common security controls can be assigned to responsible organizational officials or organizational elements (other than the information system owners whose systems will implement or use the common security controls) and • The results from the assessment of the common security controls can be used to support the security certification and accreditation processes of organizational information systems where the controls have been applied

Cyber Security	The protection of data and systems in networks that are connected to the Internet.
Data Reference Model (DRM)	<p>The Data Reference Model provides a structure that facilitates the development and effective sharing of government data across communities of practice and lines of business. The DRM asks, “What data and information does the Department have to support the business objectives.” The DRM describes the data at an aggregate level and enables agencies to describe the types of interaction and exchanges occurring between the federal government and citizens. Currently, the DRM standardizes three aspects of data management:</p> <ul style="list-style-type: none"> • Data Description: Provides a means to uniformly describe data, 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 community of interest • 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, re-occurring transactions between parties
Enterprise Architecture	A strategic information asset base which defines the mission, the information necessary to perform the mission and the transitional processes for implementing new technologies in response to the changing mission needs. It helps to align resources to improve business performance and help agencies better execute their core missions. An enterprise architecture describes the current and future states of the agency and lays out a plan for transitioning from the current state to the desired future state.
Fair Information Practice Principles (FIPPs)	Set of principles that provide general guidelines on how entities may collect and use personal information and the safeguards required to assure those practices are fair and provide adequate privacy protection.
Federal Enterprise Architecture (FEA)	Represents the U.S. federal government’s enterprise architecture and provides a framework for cross-agency information technology investment analysis, management and use. The FEA is comprised of five, inter-related reference models (PRM, BRM, SRM, DRM and TRM) and three profiles (Geospatial Profile, Records Management Profile, and FEA-Security and Privacy Profile) which are intended to

	<p>promote common, consistent enterprise architecture practices that improve government performance.</p>
<p>Federal Enterprise Architecture Security and Privacy Profile (SPP)</p>	<p>A scalable, repeatable risk-based conceptual methodology for addressing information security and privacy requirements within and across architecture segments. It provides a common language for discussing security and privacy in the context of federal agencies’ business and performance goals. The FEA-SPP provides best practices and recommendations that promote the successful incorporation of information security and privacy into an organization’s enterprise architecture.</p>
<p>Federal Information Processing Standards (FIPS)</p>	<p>Standards and guidelines developed by the National Institute of Standards and Technology (NIST) for federal computer systems. These standards and guidelines are for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.</p>
<p>Federal Segment Architecture Methodology (FSAM)</p>	<p>A five step process for developing and using federal segment architectures.</p>
<p>Hybrid Security Controls</p>	<p>Where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific.</p>
<p>Performance Reference Model (PRM)</p>	<p>The PRM is a “reference model” or standardized framework to measure the performance of major IT investments and their contribution to program performance. The PRM has three main purposes:</p> <ol style="list-style-type: none"> 1. Help produce enhanced performance information to improve strategic and daily decision-making; 2. Improve the alignment — and better articulate the contribution of — inputs to outputs and outcomes, thereby creating a clear “line of sight” to desired results; and 3. Identify performance improvement opportunities that span traditional organizational structures and boundaries <p>Information in the PRM helps agencies monitor the performance of an investment and/or program. By defining and tracking specific performance objectives and metrics, agencies are able to use the data to support portfolio decision-making, process improvement efforts,</p>

	improve service-delivery approaches, improve underperforming programs, and leverage existing performance management tools across the federal government.
Privacy Control Family	Control categories which are designed to help agencies protect personal information. Eight privacy control families exist (transparency, individual participation and redress, purpose specification, data minimization and retention, use limitation, data quality and integrity, security, accountability and auditing).
Risk Management Framework (RMF)	Provides a structured, yet flexible approach for managing the portion of risk resulting from the incorporation of information systems into the mission and business processes of the organization.
Security Control Family	A set of control categories which help promote information confidentiality, integrity, and availability. Seventeen security control families exist (risk assessment, planning, system and services acquisition, certification and accreditation and security assessments, personnel security, physical and environmental protection, contingency planning, configuration management, maintenance, system and information integrity, media protection, incident response, awareness and training, identification and authentication, access control, audit and accountability, system and communications protection).
Service Component Reference Model (SRM)	The SRM contains documentation of agencies' capabilities. These capabilities are then mapped to service domains and service types. By understanding and classifying capabilities, agencies are better able to discover government-wide capabilities that can be leveraged.
Segment Architecture	Detailed results-oriented architecture (baseline and target) and a transition strategy for a portion or segment of the enterprise.
Solution Architecture	An architecture for an individual IT system that is part of a segment. A solution architecture is reconciled to the segment architecture above it.
System-Specific Security Controls	Baseline Security Controls not designated as common controls or hybrid and are responsibility of the information system owner. These controls apply to the solution architecture which is characterized by being mapped to the LOB and sub-function levels

	of the BRM.
Technical Reference Model (TRM)	The TRM contains documentation of the technologies and standards used to support the service components. It provides a component-driven, technical framework that categorizes the standards and technologies to support and enable the delivery of Service Components and capabilities. It provides a foundation to advance the reuse and standardization of technology and service-components from the agency and government-wide perspectives.
Virtualization	A technique for hiding the physical characteristics of computing resources to simplify the way in which other systems, applications, or end users interact with those resources.

References

Laws

Clinger Cohen Act of 1996. (Clinger Cohen Act)

E-Government Act of 2002. (E-Gov Act)

Federal Acquisition Streamlining Act of 1994. (FASA)

Federal Information Security Management Act of 2002. (FISMA)

Health Insurance Portability and Accountability Act of 1996. (HIPAA)

Privacy Act of 1974. (Privacy Act)

Executive Policy

OMB *Privacy Act Implementation*, July 9, 1975

OMB Circular A-11, *Preparation, Submission, and Execution of the Federal Budget*, November 2005. (OMB A-11)

OMB Circular A-130, *Management of Federal Information Resources*, November 2000. (OMB Circular A-130) and Appendix I – *Federal Agency Responsibilities for Maintaining Records About Individuals*

OMB Memorandum 03-22, *Guidance on Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003. (M-03-22)

OMB Memorandum 05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, June 2005. (M-05-15)

OMB Memorandum 06-15, *Safeguarding Personally Identifiable Information*, May 2006 (M-06-15)

OMB Memorandum 06-16, *Protection of Sensitive Agency Information*, June 2006. (M-06-16)

OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007. (M-07-16)

Federal Standards

FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, U.S. Department of Commerce, December 2003

FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, U.S. Department of Commerce, March 2006.

International Standards

ISO/IEC Standard 21827:2002, *Systems Security Engineering – Capability Maturity Model*, October 2002.

Guidance

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, Revision 1, August 2008 (Draft).

NIST SP 800-39, *Managing Risk from Information Systems, an Organization Perspective*, April 2008

NIST SP-800-53, Revision 3: *Recommended Security Controls for Federal Information Systems*, May 2010.

NIST SP 800-53A, Revision 1: *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, May, 2010.

NIST SP 800-55, *Security Metrics Guide for Information Technology System*, July 2003.

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

NIST SP 800-60, Volume 1: *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

NIST SP-800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information*, April 2010.

Federal CIO Council, *A Practical Guide to Federal Enterprise Architecture Version 1.0.*, Chief Information Officer Council, February 2001. <http://www.gao.gov/bestpractices/bpeaguide.pdf>

Federal CIO Council, *Consolidated Reference Model*, October 2007.

Federal CIO Council, *FEA Practice Guidance*, November 2007.

Federal CIO Council, *Federal Segment Architecture Methodology*, June 2008 (Draft)

Federal Information Sharing Environment, *ISE Privacy Protections*.
<http://www.ise.gov/pages/privacy-implementing.html>

U.S. Department of Justice, Office of Justice Programs, *Justice Information Sharing Privacy and Civil Liberties*. <http://www.it.ojp.gov/default.aspx?area=privacy&page=1265>

Other Resources

“Component Organization and Registration Environment,” <http://www.core.gov>, April 2006.

“EmergingTechnology.gov,” <http://www.et.gov>, April 2006.

Federal Enterprise Architecture Reference Model Maintenance Process, Chief Information Officer Council, et. al., June 2005.

FY07 Budget Formulation: FEA Consolidated Reference Model Document, OMB, May 2005.

Practical Guide to Federal Enterprise Architecture – Chief Information Officer Council Version 1.0 February 2001.