The Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP)

Architecture and Infrastructure Committee
Federal CIO Council

FEA-SPP Briefing Topics

- Defining the FEA-SPP
- Visualizing an Architecture
- The SPP-FEA Methodology
- Validating the FEA-SPP
- Recent Activities / Next Steps
- Points of Contact

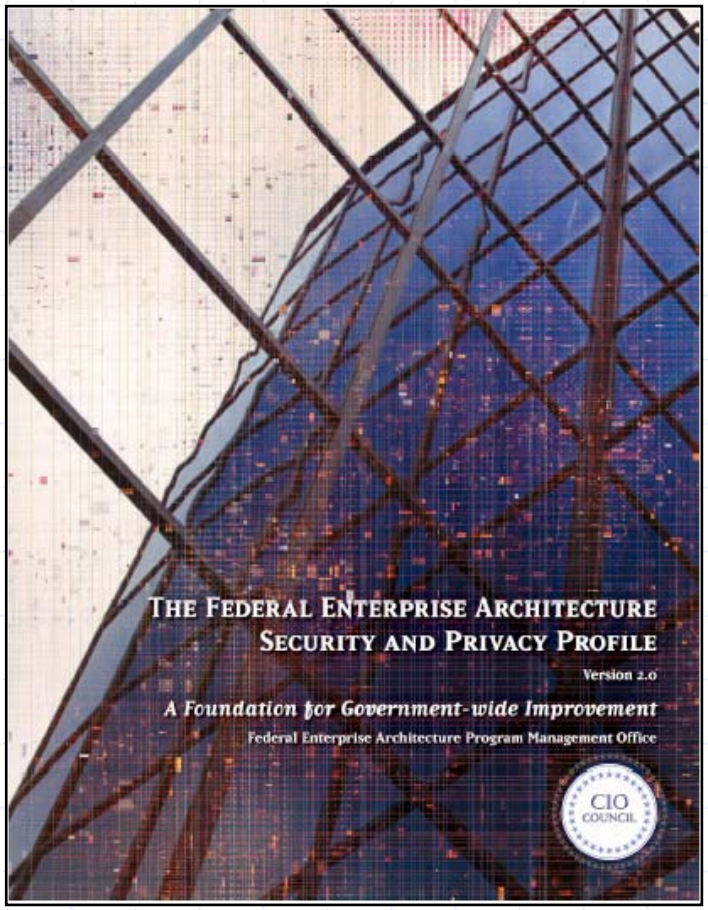
Defining the FEA-SPP

The FEA-SPP can help to develop effective information security and privacy solutions in the context of an agency's business requirements and architecture

Defining the FEA-SPP

The Federal Enterprise Architecture – Security and Privacy Profile (FEA-SPP) was developed by the Office of Management and Budget and the Federal CIO Council to provide best practices and recommendations that promote the successful incorporation of information 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.

FEA-SPP v2.0 was published in June 2006 and can be downloaded at:
http://www.whitehouse.gov/omb/egov/documents



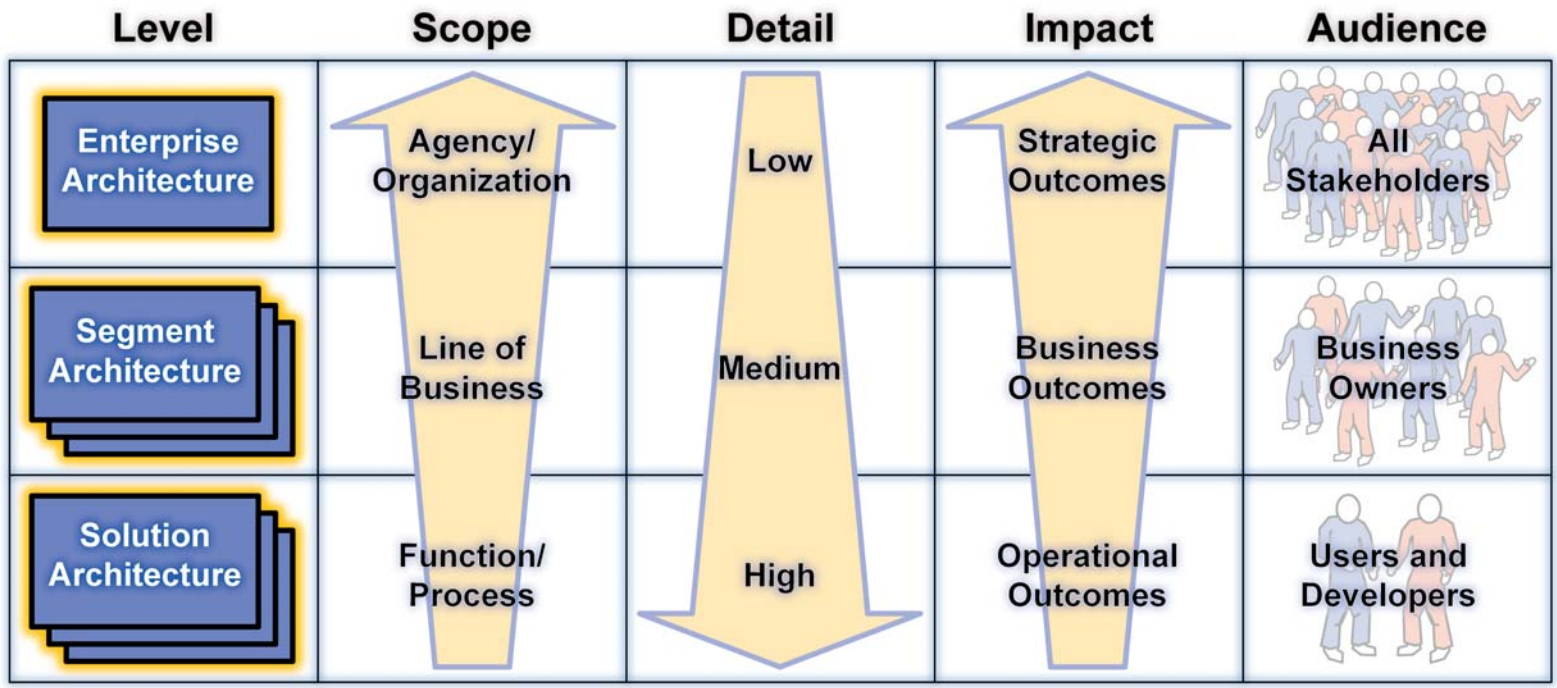
Defining the FEA-SPP

The FEA-SPP is voluntary and does not replace existing law or guidance regarding the classification or protection of federal information and systems, including the following examples:

Security / Privacy Topic	Law / Guidance
Legal requirements for the protection of Federal information and IT systems	Federal Information Security Management Act of 2002
Legal requirements to protect personal data	Privacy Act of 1974
Standards for Security Categorization of Federal Information and Information Systems	Federal Information Processing Standards (FIPS) Publication 199
Minimum Security Requirements for Federal Information and Information Systems	FIPS Publication 200
Management of Federal Information Resources	Office of Management and Budget Circular A-130
Recommended Security Controls for Federal Information Systems	National Institute for Standards & Technology Publication 800-53

Defining the FEA-SPP

All agencies seek to improve their mission performance. Architecture is a management practice to maximize the contribution of an agency's resources to achieve its mission. Architecture can establish a clear line of sight from investments to measurable performance improvements whether for the entire enterprise or a portion (segment) of the enterprise.



Defining the FEA-SPP

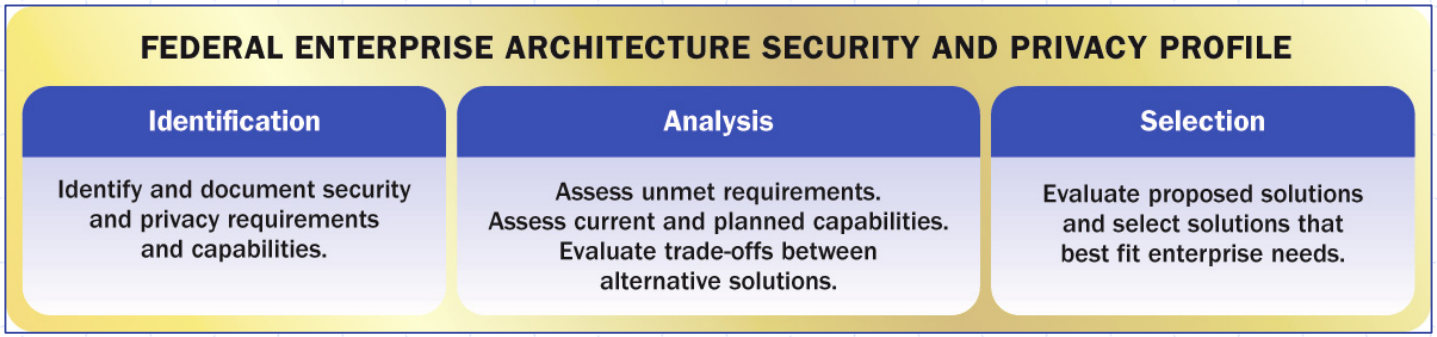
The figure below illustrates the relationship of architecture segments across multiple agencies. A single agency contains both core mission area segments and business services segments. Enterprise services are those cross-cutting services spanning multiple segments.

Segments can be leveraged within an agency, across several agencies, or the entire federal government.

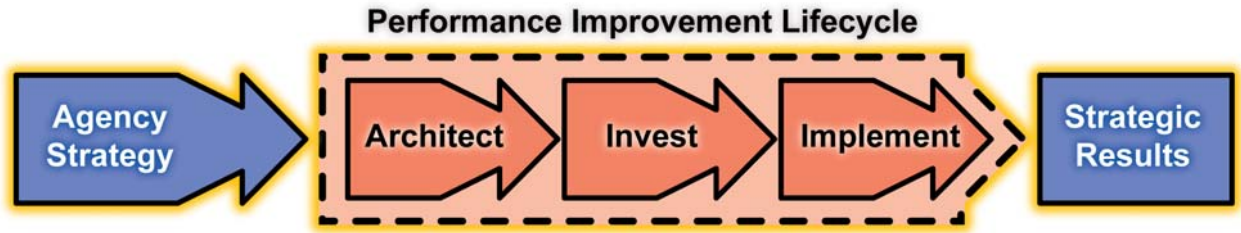
Security Management is an enterprise-level service, and the FEA-SPP is the OMB-recommended method to design and implement this type of service in enterprise and segment architectures.

Defining the FEA-SPP

FEA-SPP is a 3-stage method for developing enterprise-level information security and privacy solutions within and across architecture segments.



The FEA-SPP compliments existing law and guidance, and goes beyond program-level approaches by enabling an agency to capture information security and privacy requirements/solutions at an enterprise level through the agency's architecture and capital planning processes.



Defining the FEA-SPP

FEA-SPP provides an **enterprise level** approach to security and privacy solution development, which is different from **program-level** approaches

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 III—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?

An enterprise-level approach looks at workflow, information exchanges, services, systems, and infrastructure in the context of the agency's overall mission and goals

Defining the FEA-SPP

Examples of enterprise-level security and privacy solutions that can be enabled by the FEA-SPP:

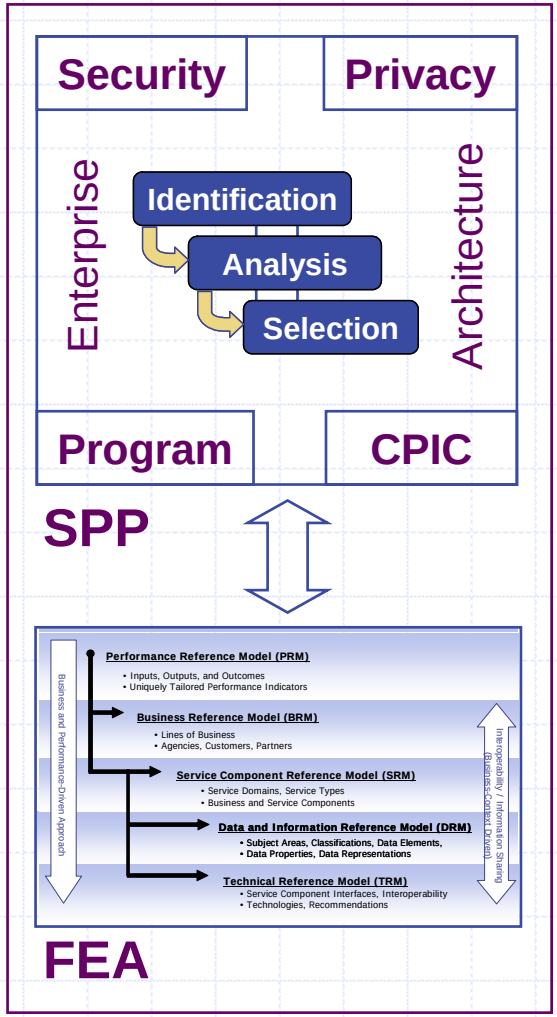
- Identifying security controls for a multi-agency grants management system with tie-ins to the Grants.Gov web portal…. then contributing a generalized version of the solution to Core.Gov for component re-use by other agencies
- Designing HIPPA-compliant data access controls for an electronic patient record system that serves multiple hospitals
- Establishing a common security buffer zone for an agency's internal networks
- Identifying requirements and solutions for the protection of personally identifiable information (PII) used during field inspections on laptops/PDAs
- Complimenting Service-Oriented Architecture efforts by designing reusable security controls for shared services across agency business units

The FEA-SPP works at all levels of the enterprise architecture

Defining the FEA-SPP

The FEA-SPP addresses information security and privacy from a business-centric enterprise perspective. The FEA-SPP integrates the disparate perspectives of program, security, privacy, and capital planning into a coherent process, using an organization's enterprise architecture for context and consistency.

The Federal Enterprise Architecture provides a common language for discussing security and privacy in the context of Federal agencies' business and performance goals, enabling better coordination and integration of efforts and investments across organizational or business activity stovepipes.



Visualizing an Architecture

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."

Visualizing an Architecture

Enterprise architecture (EA) is a technique for documenting, evaluating, and planning an organization's business objectives and the business activities, information, standards, and capabilities that support those objectives.[2] Agencies typically maintain two versions of their enterprise architecture. The version that portrays the existing enterprise, 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 and reuse existing assets and develop enterprise solutions with reuse and interoperability in mind. Understanding and establishing reusable components is an integral part of continuously improving an organization's IT portfolio management.[3]

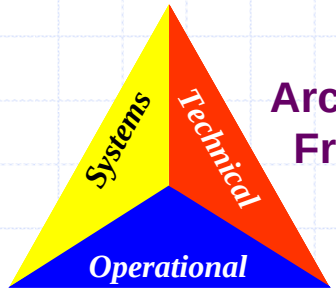
The enterprise architecture also describes the desired future state for an organization—called the *target* or *to-be* architecture. Like the *as-is* architecture, the *to-be* architecture defines business objectives and supportive activities in both business and technical terms. Organizations move from the baseline state to the target state through a *sequencing* or *transition* plan.

Source: SPP v2.0, page 5.

Visualizing an Architecture

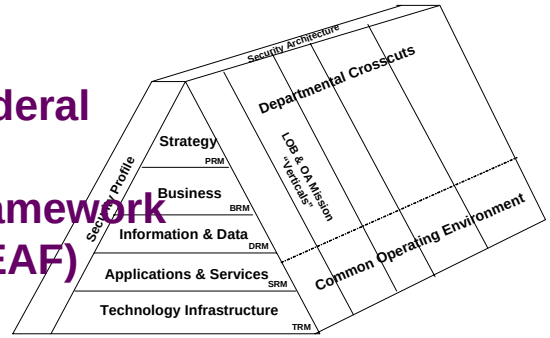
There are many approaches to modeling the current and future states of an enterprise. Federal agencies are free to select any approach; however, all Federal agency enterprise architectures must map to the Federal Enterprise Architecture's five reference models. This mapping facilitates cross-agency analysis and identification of gaps, duplicative investments, and opportunities for collaboration within and across agencies. The reference models are used to better understand current organizational activities and capabilities by describing them in standard terms that are recognized across the Federal government.

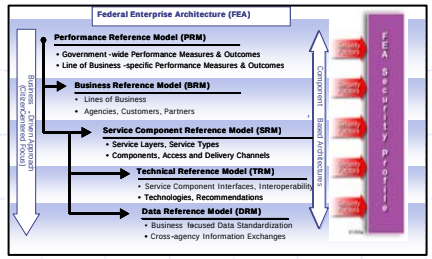
Source: SPP v2.0, page 6.



DoD Architecture Framework (DODAF)

Federal EA Framework (FEAF)



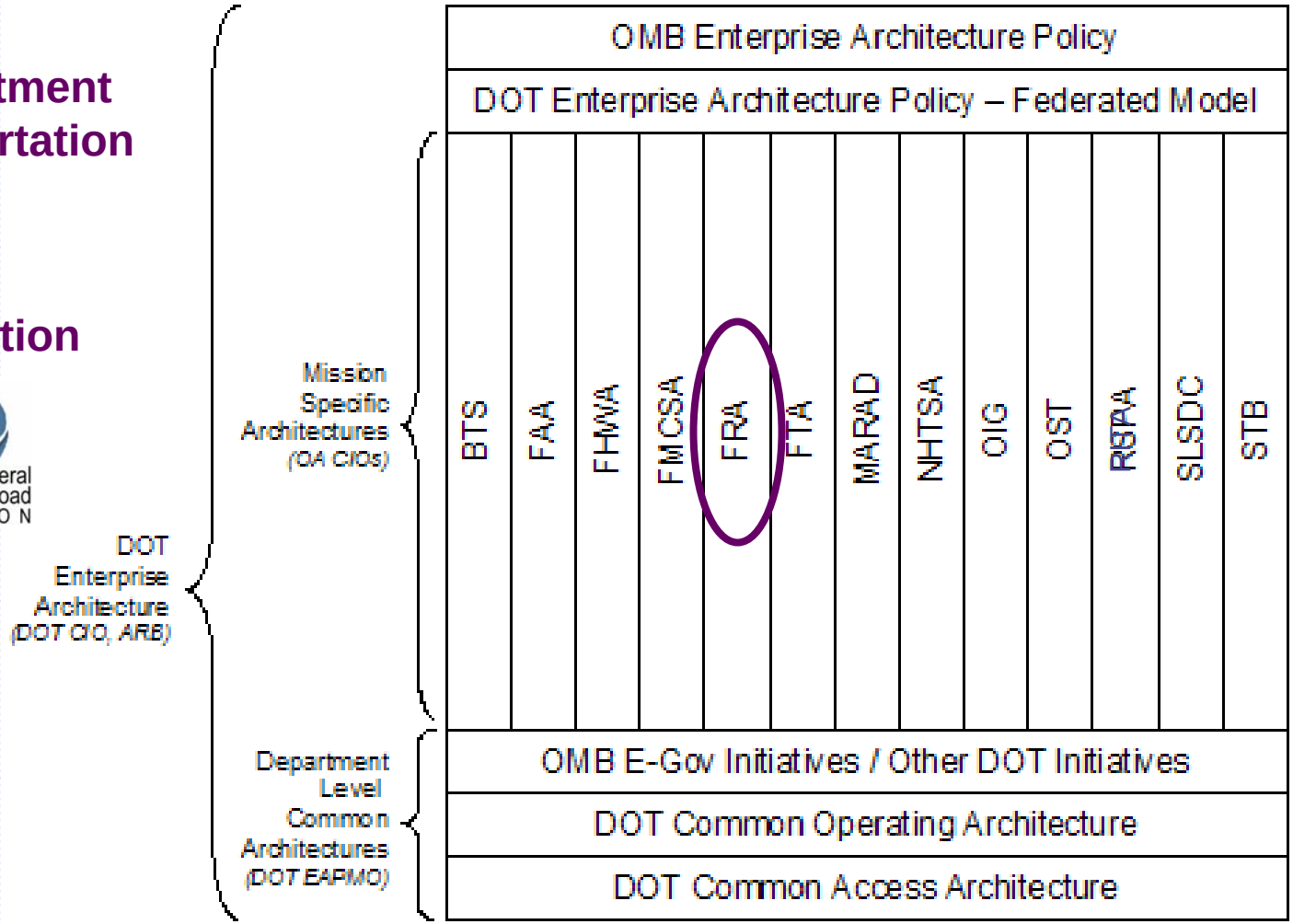


Federal EA Reference Models and Security & Privacy Profile

Visualizing an Architecture

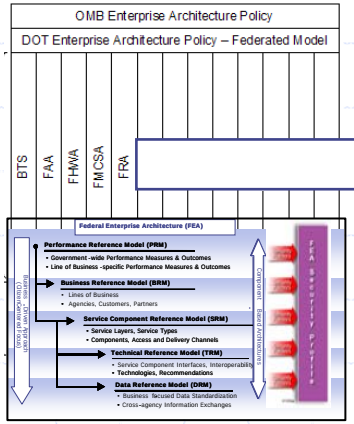
Example:
U.S. Department of Transportation

Federal Railroad Administration



Visualizing an Architecture

Federal Railroad Administration



FEA / SPP

Integrated Governance

Modernization Blueprint

Capital Planning and Budgeting

Human Capital Profile

Security Profile

Strategic Goals *PRM*

Business Processes *BRM*

Information and Data Flows *DRM*

Systems and Applications *SRM*

Technology Infrastructure *TRM*

Financial Mgmt. & Administration

Chief Counsel

Civil Rights

Policy

Public Affairs

Railroad Development

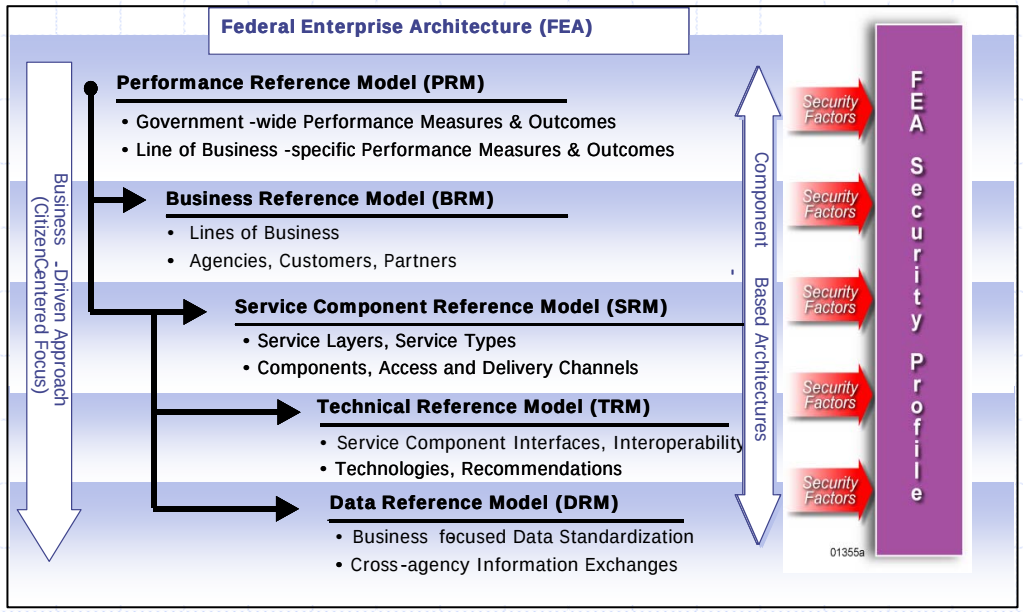
Safety

DOT & FRA Common Operating Environment

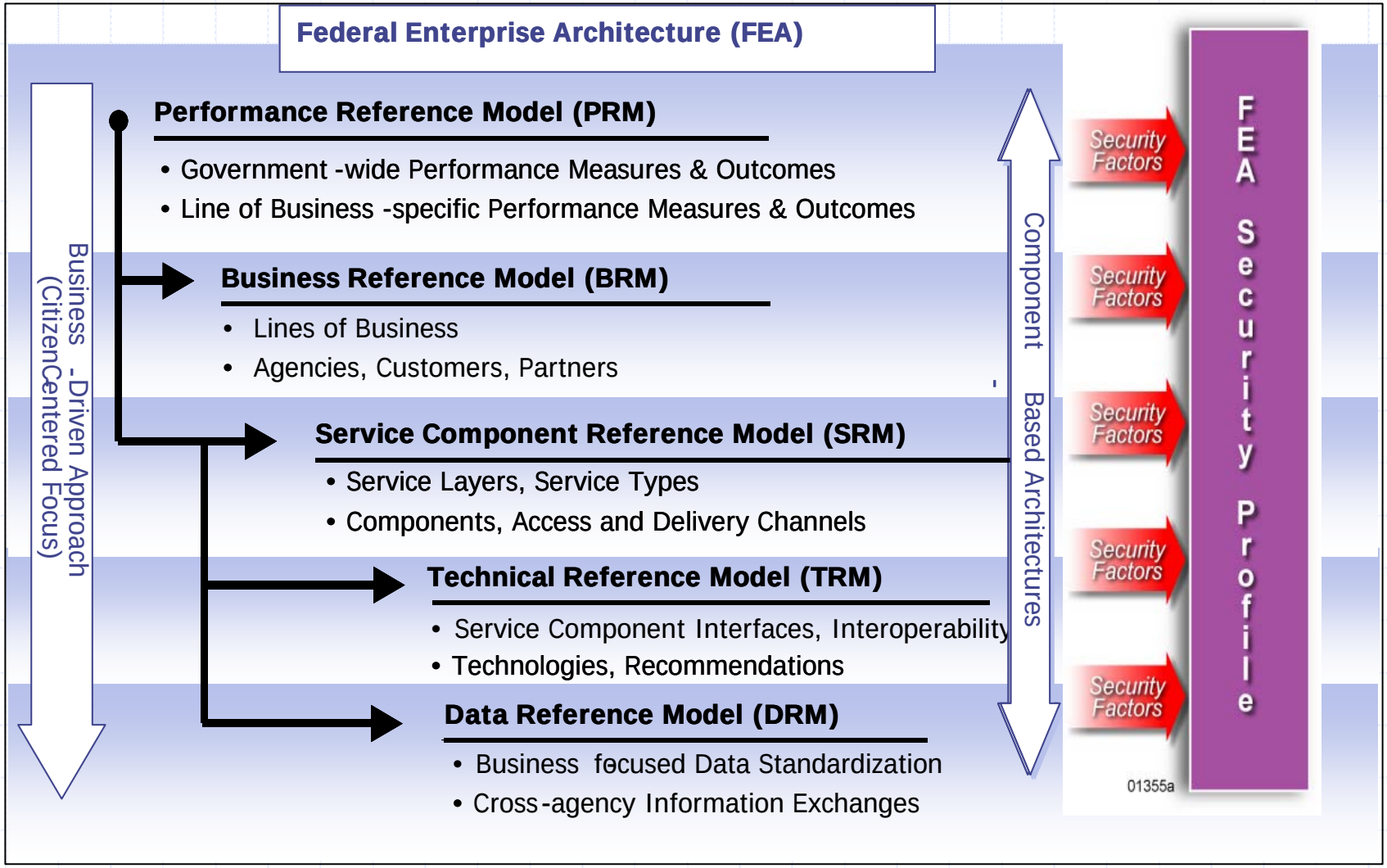
FEAF

Visualizing an Architecture

The Federal Enterprise Architecture (FEA) is a business-based framework for government-wide improvement. It describes the relationship between business functions and the technologies and information that support them. The FEA is being constructed through a collection of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across federal agencies. (OMB Circular A-11, Part 7)19

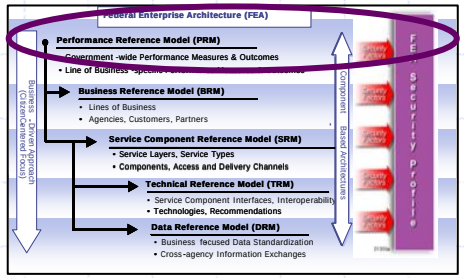


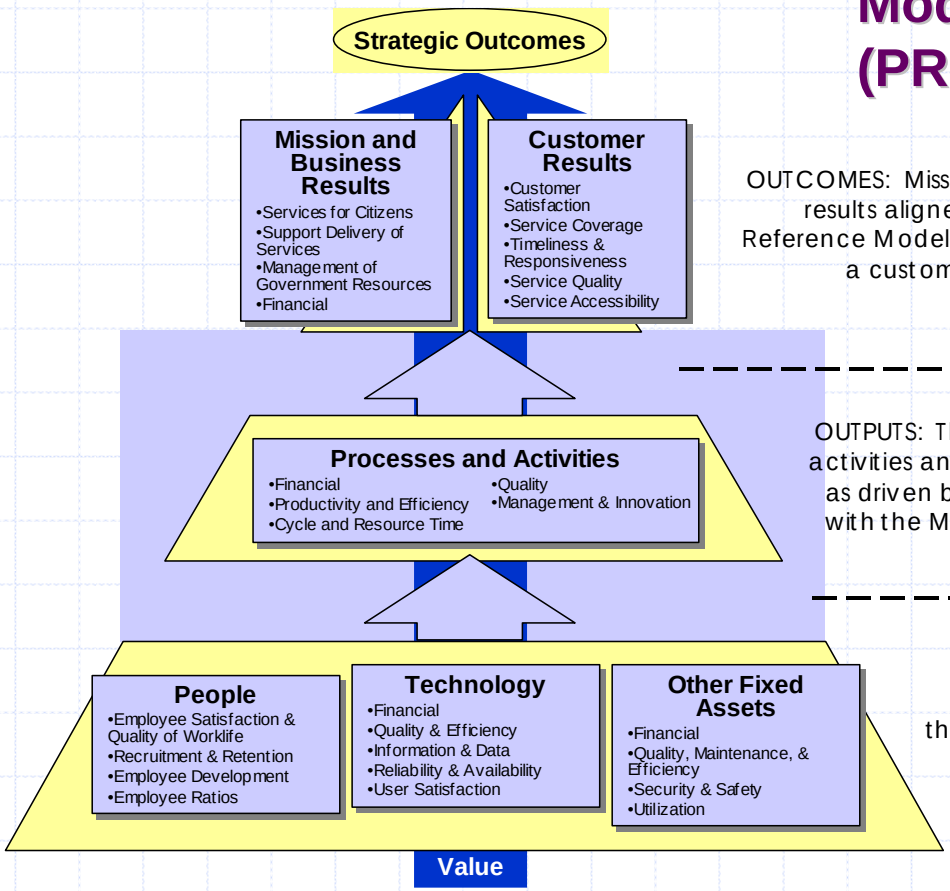
Visualizing an Architecture



Visualizing an Architecture

Performance Reference Model (PRM)





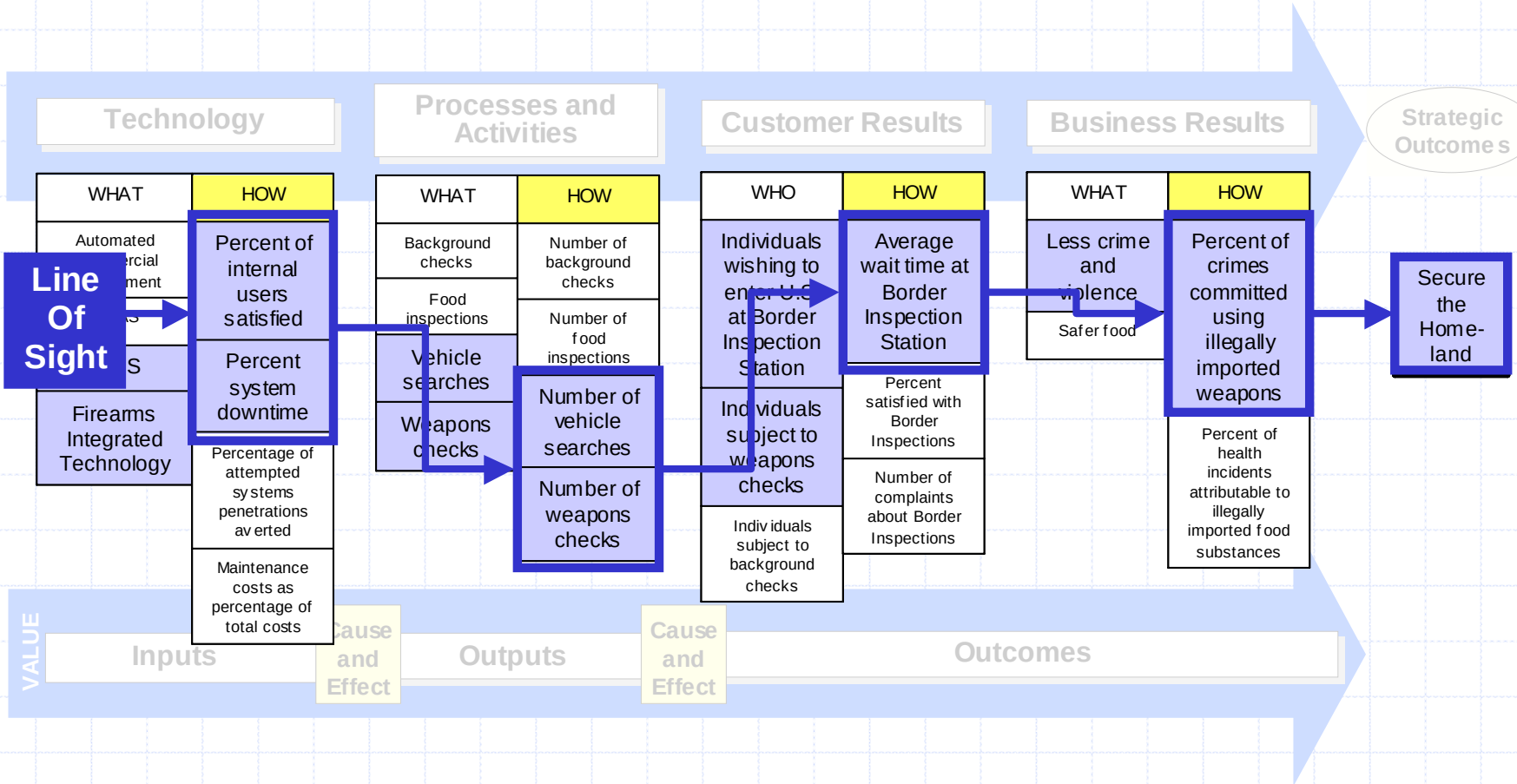
OUTCOMES: Mission and business-critical results aligned with the Business Reference Model. Results measured from a customer perspective.

OUTPUTS: The direct effects of day-to-day activities and broader processes measured as driven by desired outcomes. Aligned with the Mode of Delivery in the Business Reference Model.

INPUTS: Key enablers measured through their contribution to outputs – and by extension outcomes

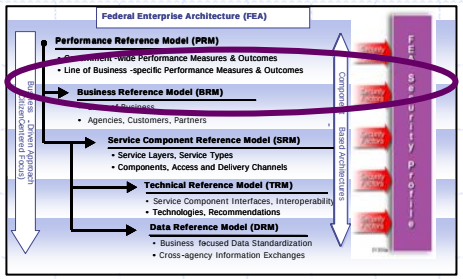
Visualizing an Architecture

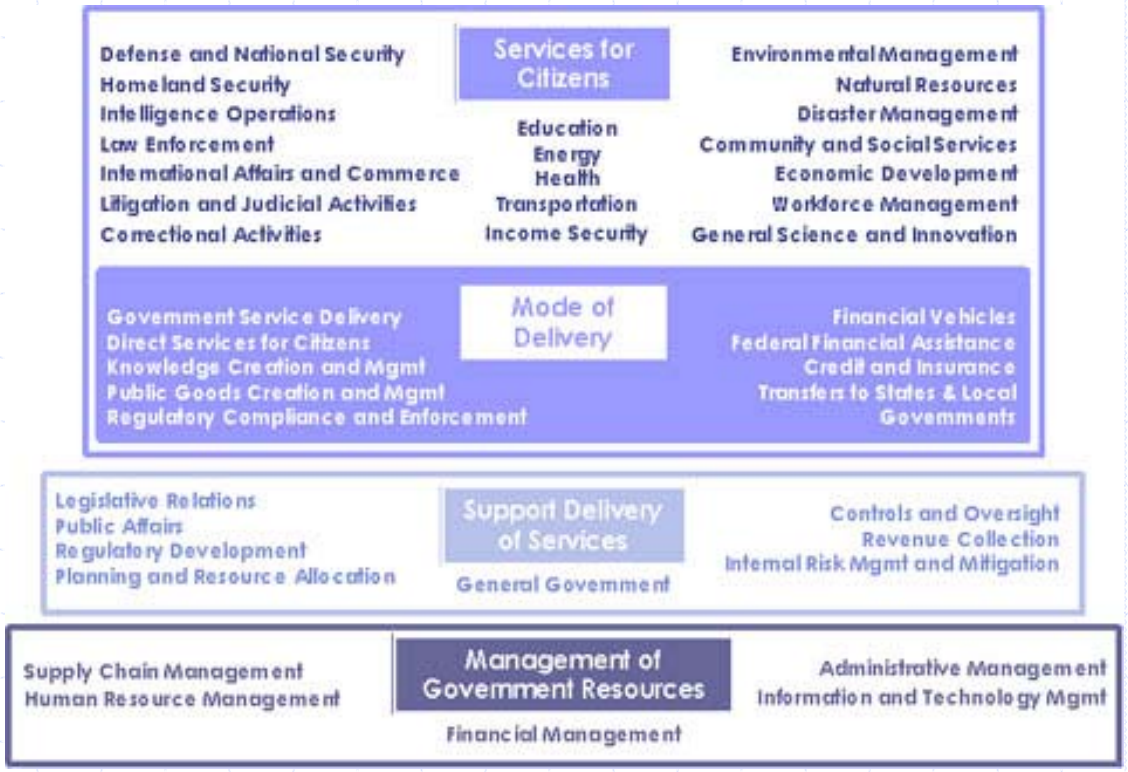
The PRM structure is designed to clearly articulate *Line of Sight* — the cause and effect relationship between inputs, outputs and outcomes



Visualizing an Architecture

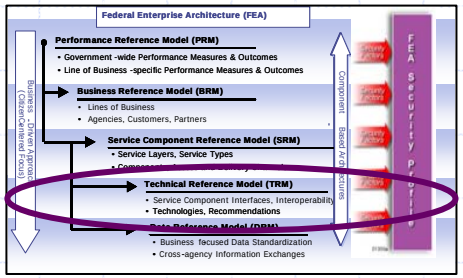
Business Reference Model (BRM)

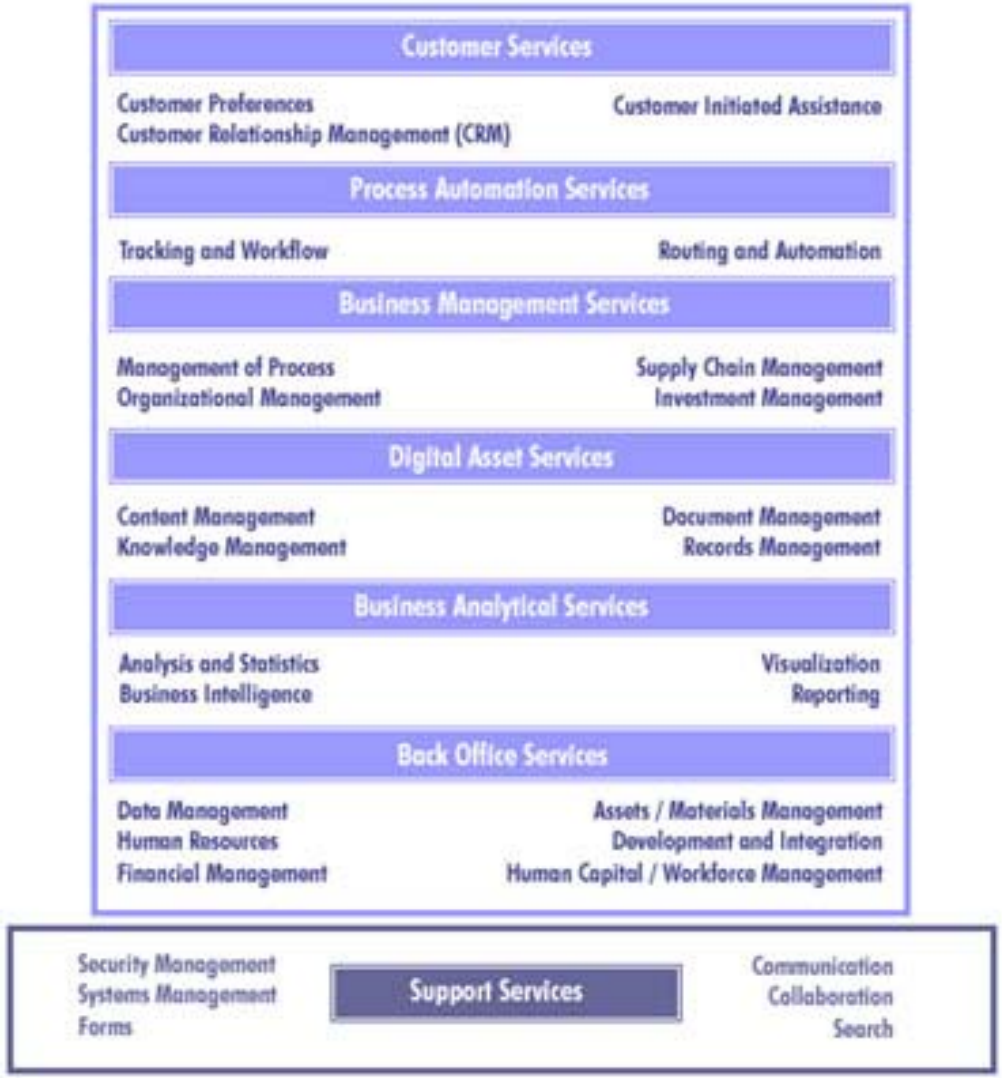




Visualizing an Architecture

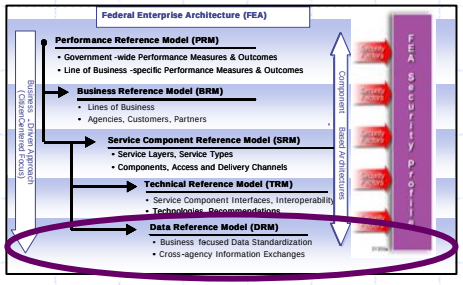
Service Reference Model (SRM)





Visualizing an Architecture

Technology Reference Model (TRM)



Service Access and Delivery

Access Channels	Delivery Channels	Service Requirements	Service Transport
Web Browser	Internet, Intranet	Legislative / Compliance	Network Services
Wireless / PDA Device	Extranet	Authentication / Single Sign-On	Transport
Collaboration / Communication	Peer to Peer (P2P)	Hosting	
Other Electronic Channels	Virtual Private Network (VPN)		

Service Platform and Infrastructure

Support Platforms	Delivery Servers	Hardware / Infrastructure
Wireless / Mobile	Web, Media	Servers / Computers
Platform Independent (J2EE)	Application	Embedded Technology Devices
Platform Dependent (.NET)	Portal	Peripherals
		WAN, LAN
Database / Storage	Software Engineering	Network Devices / Standards
Database	Integrated Development Environment (IDE)	Video Conferencing
Storage Devices	Software Configuration Management (SCM)	
	Testing Management, Modeling	

Component Framework

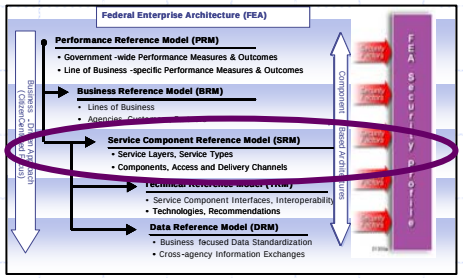
Security	Presentation / Interface	Business Logic	Data Management
Certificates / Digital Signature	Static Display	Platform Independent	Database Connectivity
Supporting Security Services	Dynamic Server-Side Display	Platform Dependent	Reporting and Analysis
	Content Rendering		
Data Interchange	Wireless / Mobile / Voice		
Data Exchange			

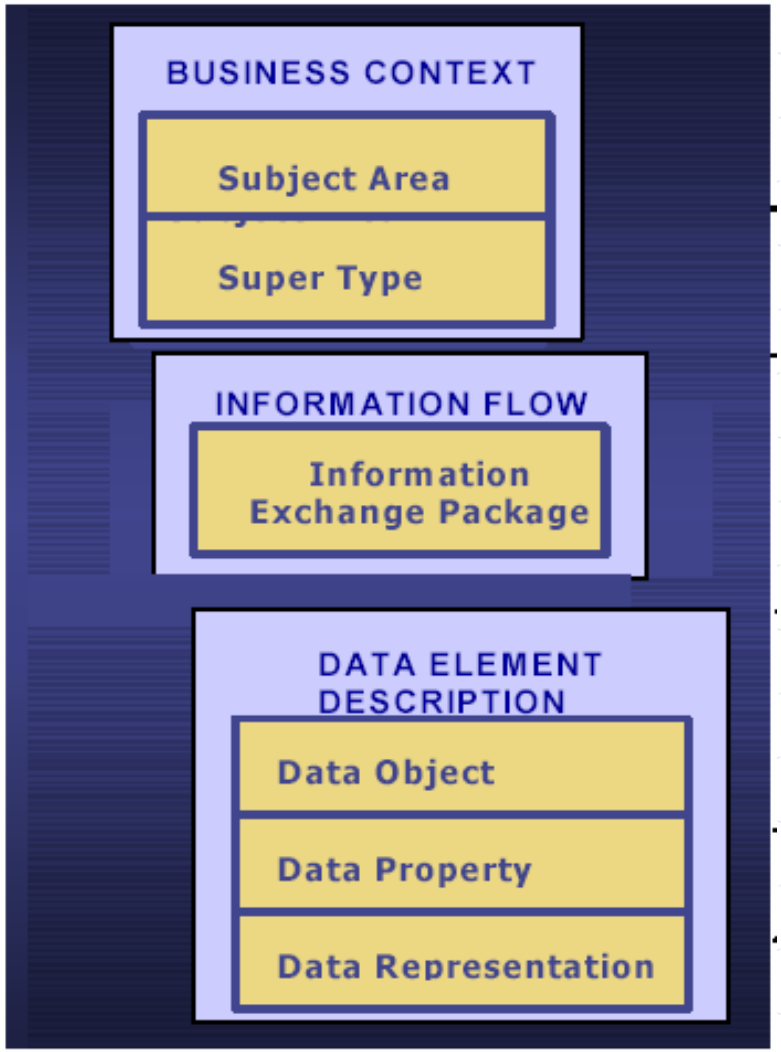
Service Interface and Integration

Integration	Interoperability	Interface
Middleware	Data Format / Classification	Service Discovery
Database Access	Data Types / Validation	Service Description / Interface
Transaction Processing	Data Transformation	
Object Request Broker		

Visualizing an Architecture

Data Reference Model (DRM)

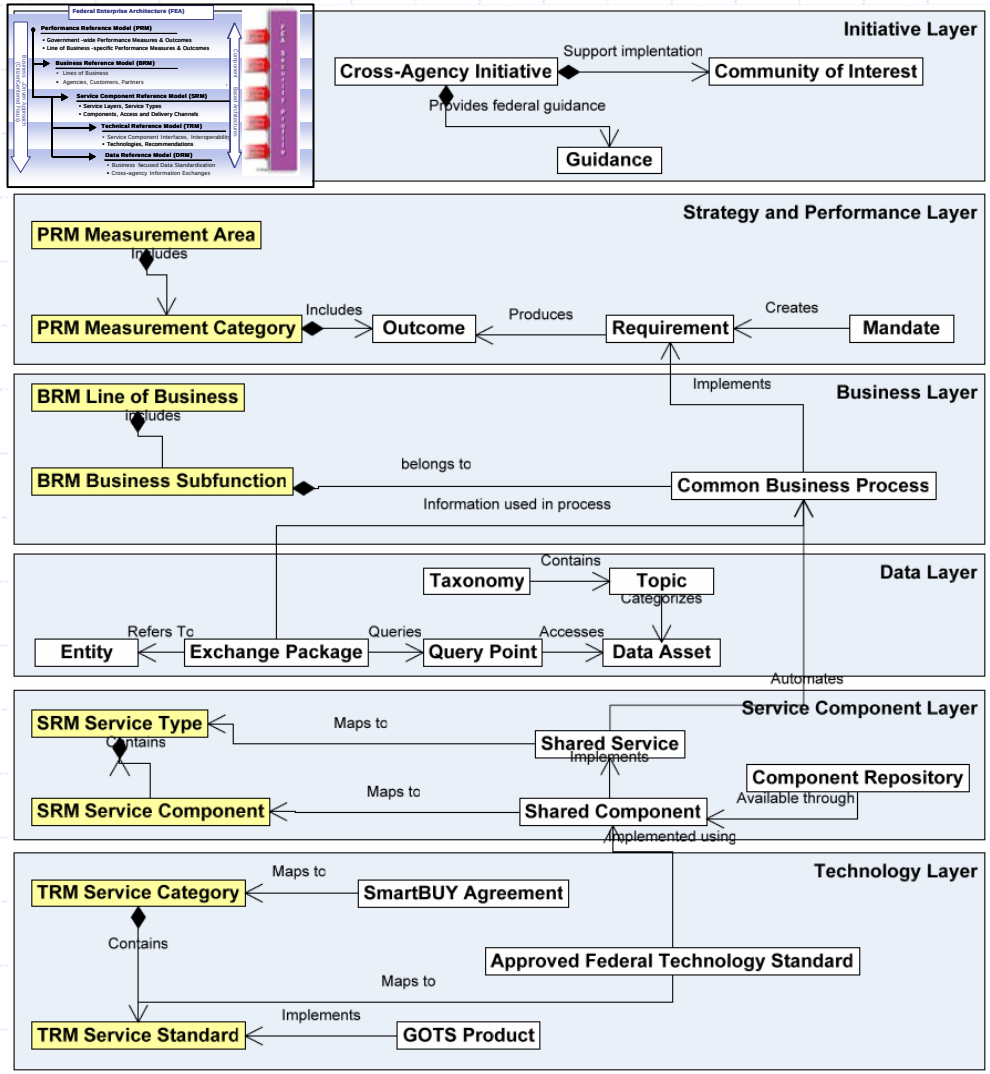




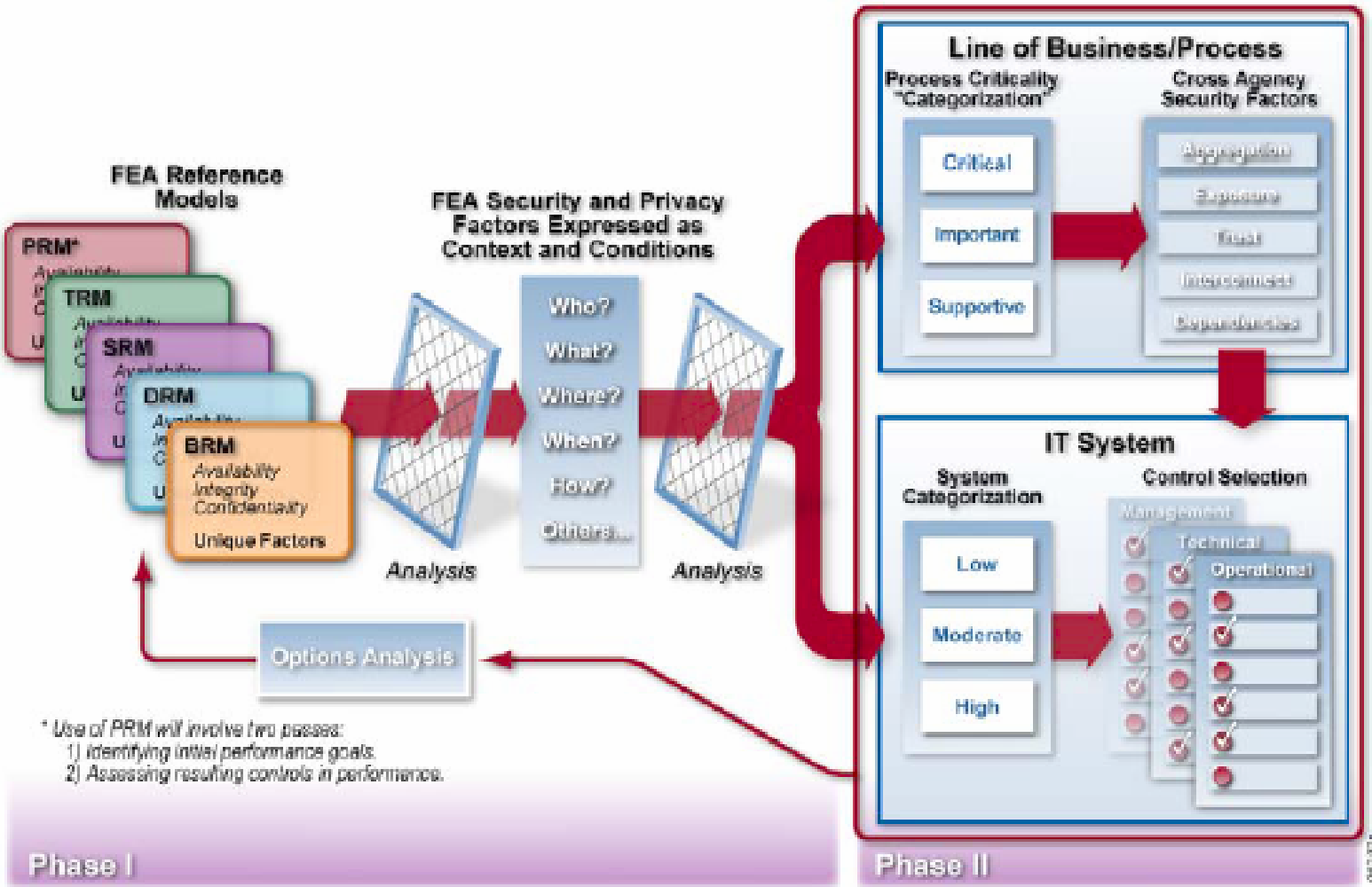
Visualizing an Architecture

Federal Transition Framework (FTF)

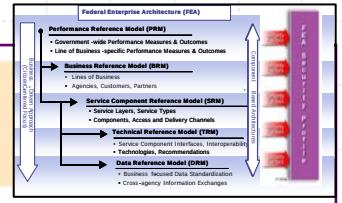
The FTF uses a simple, familiar and organized structure. It contains government-wide IT policy objectives and cross-agency initiatives including: OMB-sponsored initiatives, e.g., E-Gov and Line of Business initiatives, Government-wide initiatives such as Internet Protocol Version 6 (IPV6), Homeland Security Presidential Directive 12 (HSPD 12)



Visualizing an Architecture



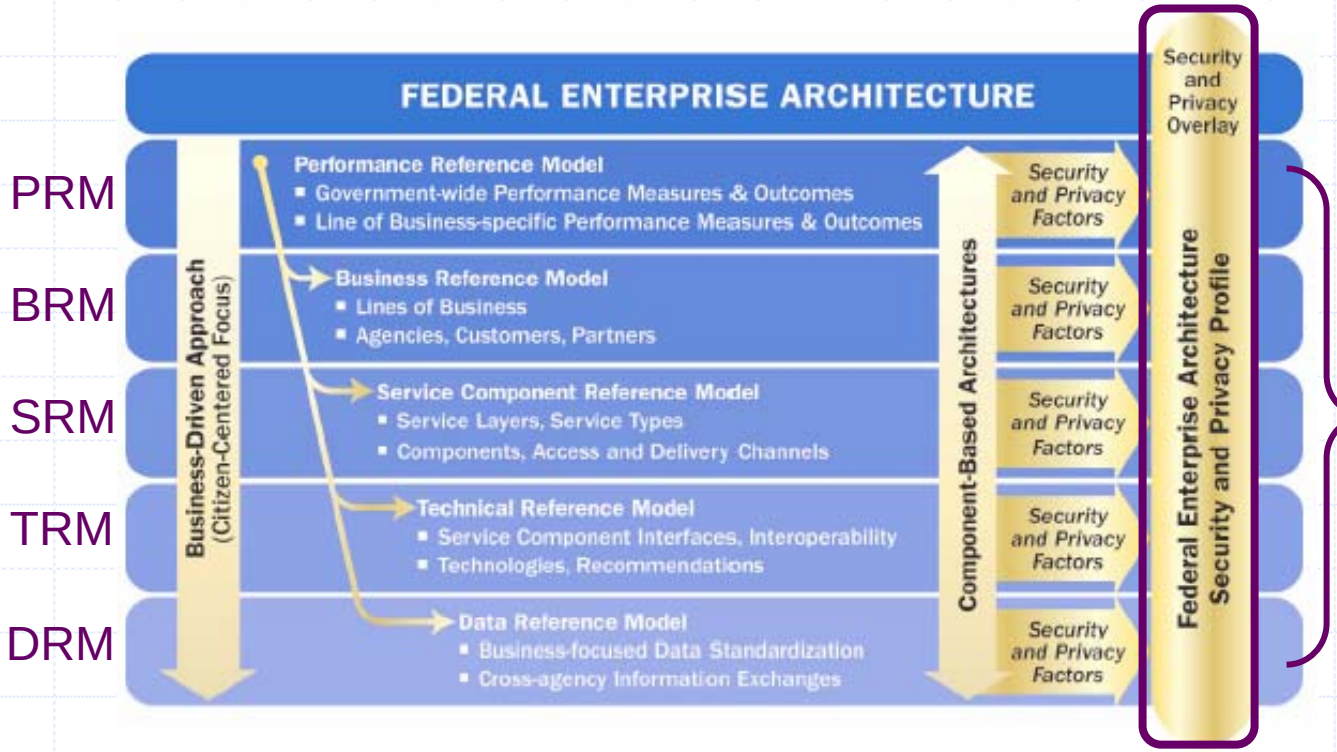
Visualizing an Architecture



FEA Reference Models	FEA Reference Model Description	FEA Security and Privacy Considerations
Performance Reference Model	Mission-related goals, objectives, and metrics	■ Describe security and privacy performance standards necessary for achieving mission performance standards and legal compliance.
Business Reference Model	Agencies' functions and sub-functions	■ Describe the security and privacy ramifications of agency business functions. ■ Describe security and privacy-specific support functions.
Service Component Reference Model	Mission-supportive processes and technologies	■ Describe the security and privacy requirements and features of mission-supportive processes and technologies. ■ Describe dedicated security and privacy processes and technologies.
Technical Reference Model	Categorizing relevant standards and technologies	■ Describe the security and privacy ramifications of deployed standards and technologies. ■ Establish enterprise standards for security and privacy delivery.
Data Reference Model	Standardizing data description, categorization, and sharing	■ Categorize data to identify mission-supportive and compliance-driven security and privacy requirements. ■ Evaluate data sharing behaviors to assess and address security and privacy ramifications.

Visualizing an Architecture

The FEA asks Federal agencies to look at their operations from common business, performance, service, technology, and data views; which are incorporated into Reference Models. The FEA-SPP works within and across all five of the FEA Reference Model areas to identify enterprise level information security and privacy requirements and solutions.



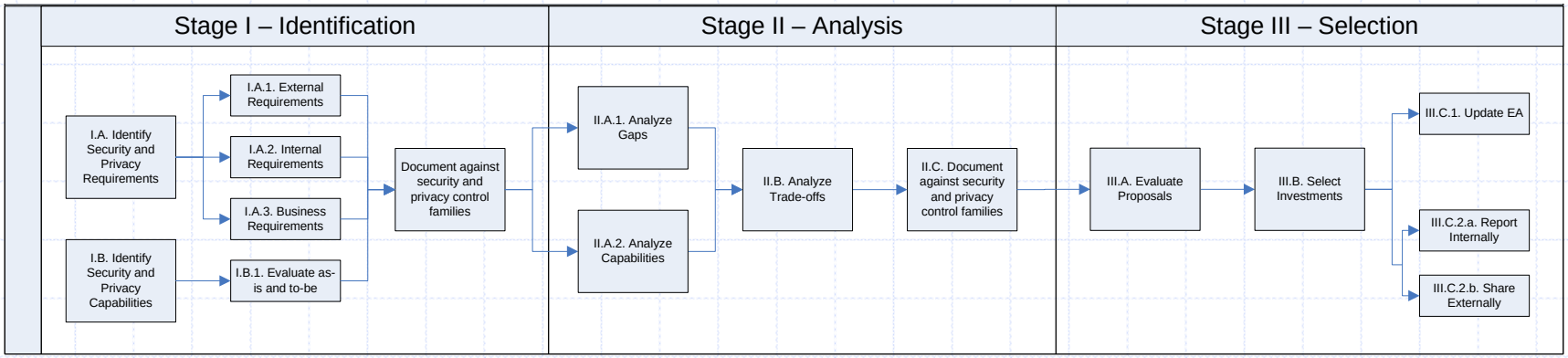
The FEA-SPP spans all five of the FEA Reference Models

The FEA-SPP Implementation Methodology

FEA-SPP Methodology

The FEA-SPP methodology uses a 3-stage, 16-activity procedure to produce enterprise-level information security and privacy solutions using the architecture and investment management processes.

Each stage has goals, objectives, implementing activities, and output products for inclusion in the agency's enterprise architecture.



Stage I	Stage II	Stage III
Identify security and privacy requirements, assess capabilities	**Analyze** capabilities and performance gaps, document proposed solutions	**Select** appropriate solutions, make investments, and share results

FEA-SPP Methodology

Stage I: Identification

Stage I is an identification of an agency's business-supportive security and privacy requirements and the existing or planned capabilities that support security and privacy. As a result of Stage I activities an agency will be able to:

- Fully identify program and enterprise-level security and privacy requirements, including previously unknown requirements
- Fully identify program and enterprise-level security and privacy capabilities, including current and planned future requirements
- Document requirements and capabilities in an agency's enterprise architecture using a nomenclature that is common across the Federal government

There are three activities in Stage I:

Activity I.A: Identify Security and Privacy Requirements

I.A.1: External Requirements I.A.2: Internal Requirements I.A.3: Business Requirements

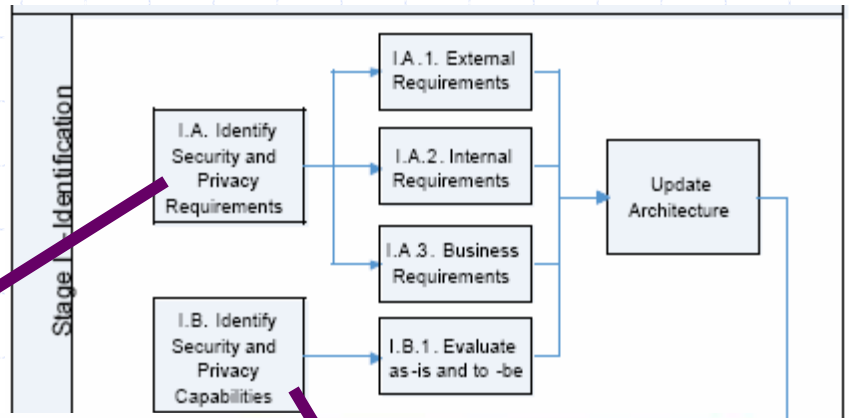
Activity I.B: Identify Security and Privacy Capabilities

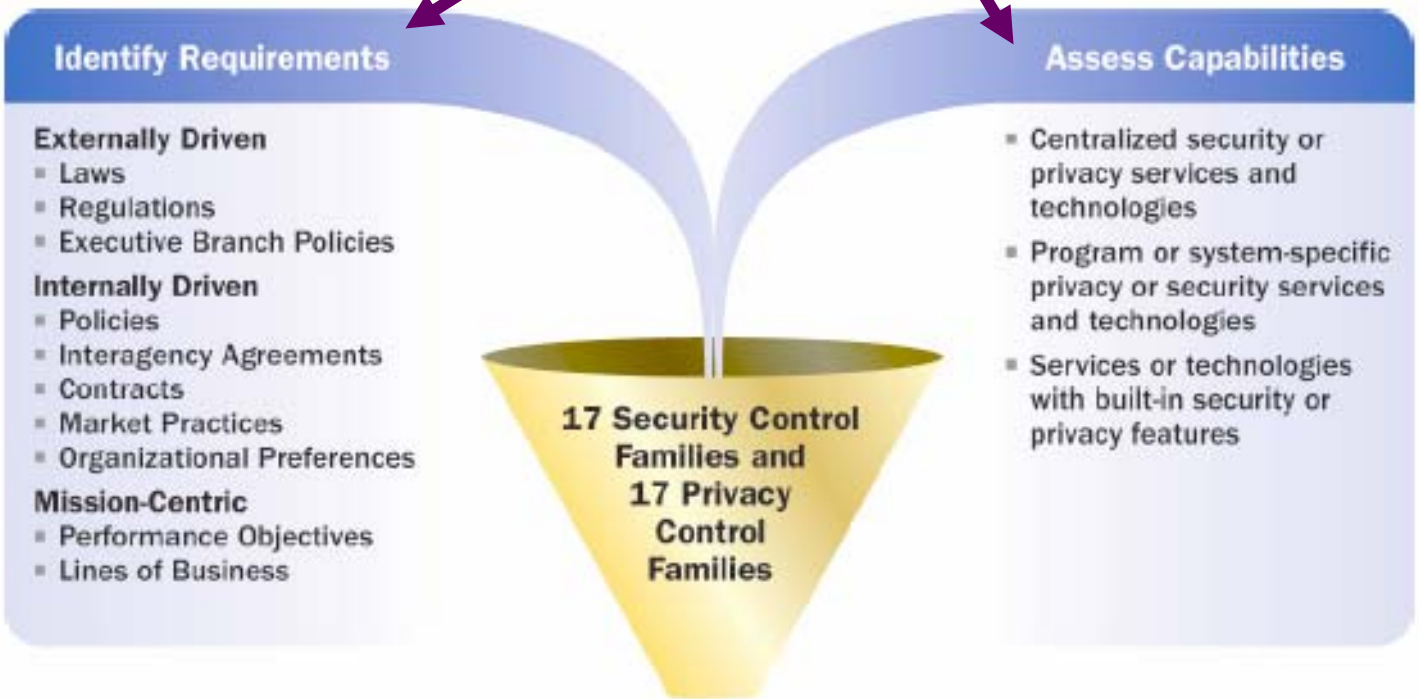
I.B.1: Evaluate as-is and to-be Capabilities

Activity I.C: Update Architecture

FEA-SPP Methodology

Stage I: **Identification**





FEA-SPP Methodology

The FEA-SPP uses 17 security and 17 privacy control families to:

- Describe business and compliance needs for security and privacy
- Capture security and privacy information across the agency's architecture
- Identify unmet requirements
- Identify redundant or non-standardized capabilities
- Select solutions that cost-effectively mitigate local and enterprise-wide risks
- Promote leveraging capabilities across agencies / Federal government

Security Control Families

Risk Assessment
System/Service Acquisition
Certification & Accreditation
Physical & Environmental
System/Info. Integrity
Awareness & Training
Audit & Accountability
Identification/Authentication
Systems/Comms Protection
Maintenance
Personnel
Planning
Media Protection
Incident Response
Contingency Plans
Configuration Mgmt
Access Control

Source: FIPS-199

Privacy Control Families

Policies and Procedures
Roles & Responsibilities
Monitoring & Measuring
Education, Awareness Training
Minimum Necessary
Accuracy of Data
Chain of Trust
Reporting and Response
Security Measures
Privacy Lifecycle
Public Disclosure
Notice
Consent
Acceptable Use
Individual Rights
Authorization
Risk Management

Source: FEA-SPP

FEA-SPP Methodology

Stage I - Identification Activities.

The FEA-SPP methodology is implemented through activities specified for each stage. The output of these activities is information that is integrated into the agency's enterprise architecture. For example, the table below lists the goals, objectives, activities, and output products for Stage 1 - Activity 1.A, which identifies an agency's information security and privacy requirements.

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
A. Identify Security and Privacy Requirements 1. Identify external requirements and incorporate into the agency's target (to-be) enterprise architecture. Security and privacy-related business processes should be highlighted in the agency's business architecture. System components providing security and privacy capabilities should be highlighted in the agency's system architecture. A clear understanding of performance requirements is the first step toward risk-management and compliance. An understanding of security and privacy requirements can be derived from business-specific documents as well as from security and privacy-specific documents.				
a. Identify those laws, regulations, and executive branch policies that establish business requirements.	Drivers[16]			
b. Identify those laws, regulations, and executive branch policies that establish security and privacy requirements.				
i. Evaluate key requirements for enterprise and programmatic security and privacy. Security examples include FISMA, OMB A-130, FIPS PUB 199, FIPS PUB 200, and others. Some privacy examples are cited in Appendix D.	Drivers			

FEA-SPP Methodology

Stage II: Analysis

In Stage II agencies analyze their business-supportive security and privacy requirements and the existing or planned capabilities that support security and privacy. Stage II's three analyses help agencies to:

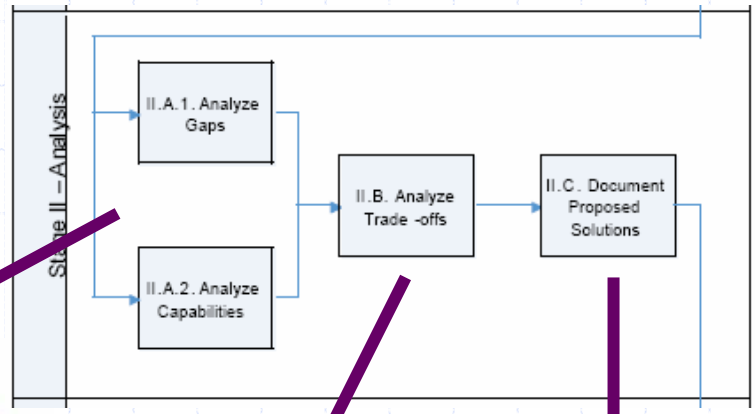
- Identify gaps between requirements and current or planned capabilities
- Identify opportunities to increase interoperability between or reduce costs of current or planned capabilities
- Propose solutions to address gaps or improve capabilities based on an informed trade-off analysis of alternatives

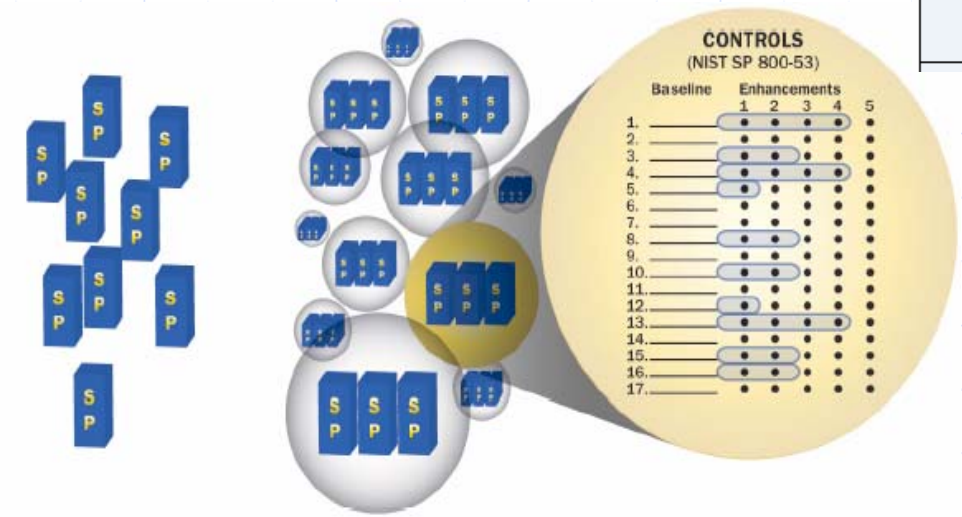
There are four activities in Stage II that support three types of analyses that address information security and privacy gaps, capabilities, and tradeoffs:

Activity II.A.1: Analyze Gaps
Activity II.A.2: Analyze Capabilities
Activity II.B: Analyze Tradeoffs
Activity II.C: Document Proposed Solutions

FEA-SPP Methodology

Stage II: **Analysis**

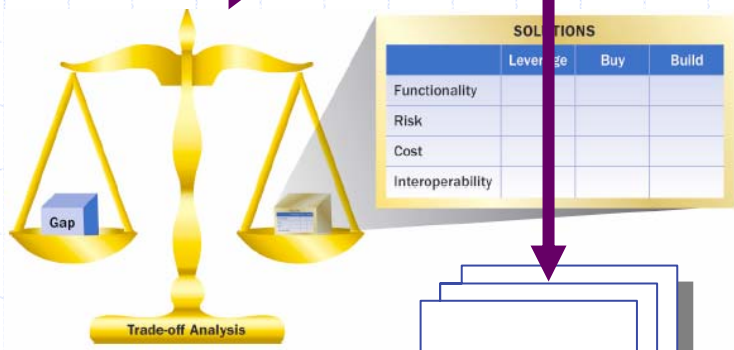




Assessments such as PIAs or FIPS 199 categorizations result in determinations of security and privacy characterizations of individual systems

Group similar systems by like security and privacy characteristics

Evaluate the groups' security and privacy requirements to identify divergence from standards or opportunities for consolidation



Proposed Security Solutions

FEA-SPP Methodology

Stage II - Analysis Activities.

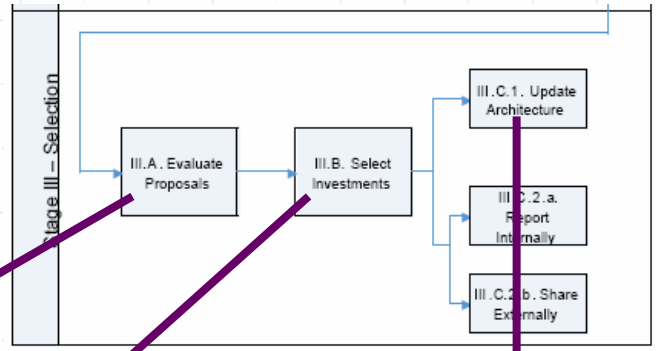
The following activities support the goals and objectives of Stage II's three types of analyses. For each activity, security and privacy information for the enterprise and/or program should be integrated into the agency's enterprise architecture.

The table illustrated below is a tool that can be used to determine where activities' outputs should be documented, identify the location where data is maintained, identify the owners of associated data, and document any corrective actions identified to improve the data or complete the activity.

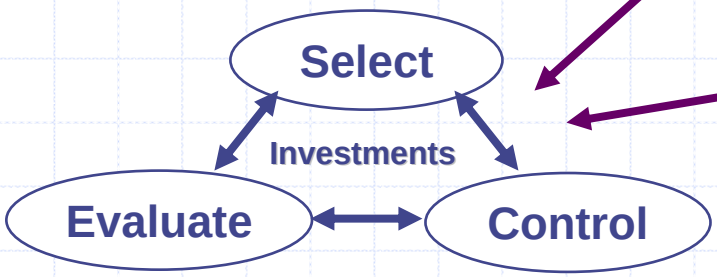
Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
A. Analyze Security and Privacy 1. Analyze Requirement and Capability Gaps. These activities determine where gaps exist between current requirements and the current or planned capabilities to meet those requirements. Unmet requirements are then assessed to verify if they must be met to appropriately manage security and privacy risks. a. Identify the gap between requirements and capabilities. i. Assess the gap between requirements and capabilities using the 17 security and 17 privacy control families. In Stage I, the FEA SPP implementation team maps requirements and capabilities to the control families. Conduct a family-by-family assessment to identify requirements that are not supported by a specific capability. Subsequent activities in Stage II address unmet requirements.	Baseline, Transition Strategy[19], Target[20]			

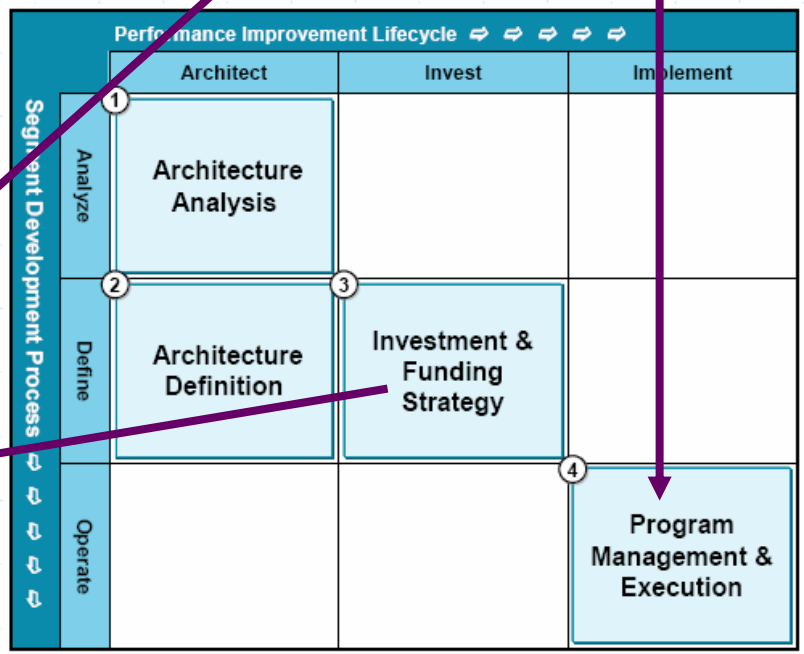
FEA-SPP Methodology

Stage III: **Selection**



SOLUTIONS	Leverage	Buy	Build
Functionality			
Risk			
Cost			
Interoperability			





FEA-SPP Methodology

Stage III: Selection

Stage III involves the enterprise-level evaluation of the information security and privacy solutions that were proposed in Stage II, as well as the selection of major investments to implement those solutions. Stage III activities include:

- An evaluation of individual security and privacy proposals so that each fully reflects the outputs of Stages I and II
- The selection of individual proposals that best support the business, security, and privacy needs of the agency
- Update of the to-be architecture and sharing of reusable components

There are five Stage III activities:

Activity III.A: Evaluate Proposals

Activity III.B: Select Investments

Activity III.C.1: Update Architecture

Activity III.C.2.a: Report Internally

Activity III.C.2.b: Share Externally

FEA-SPP Methodology

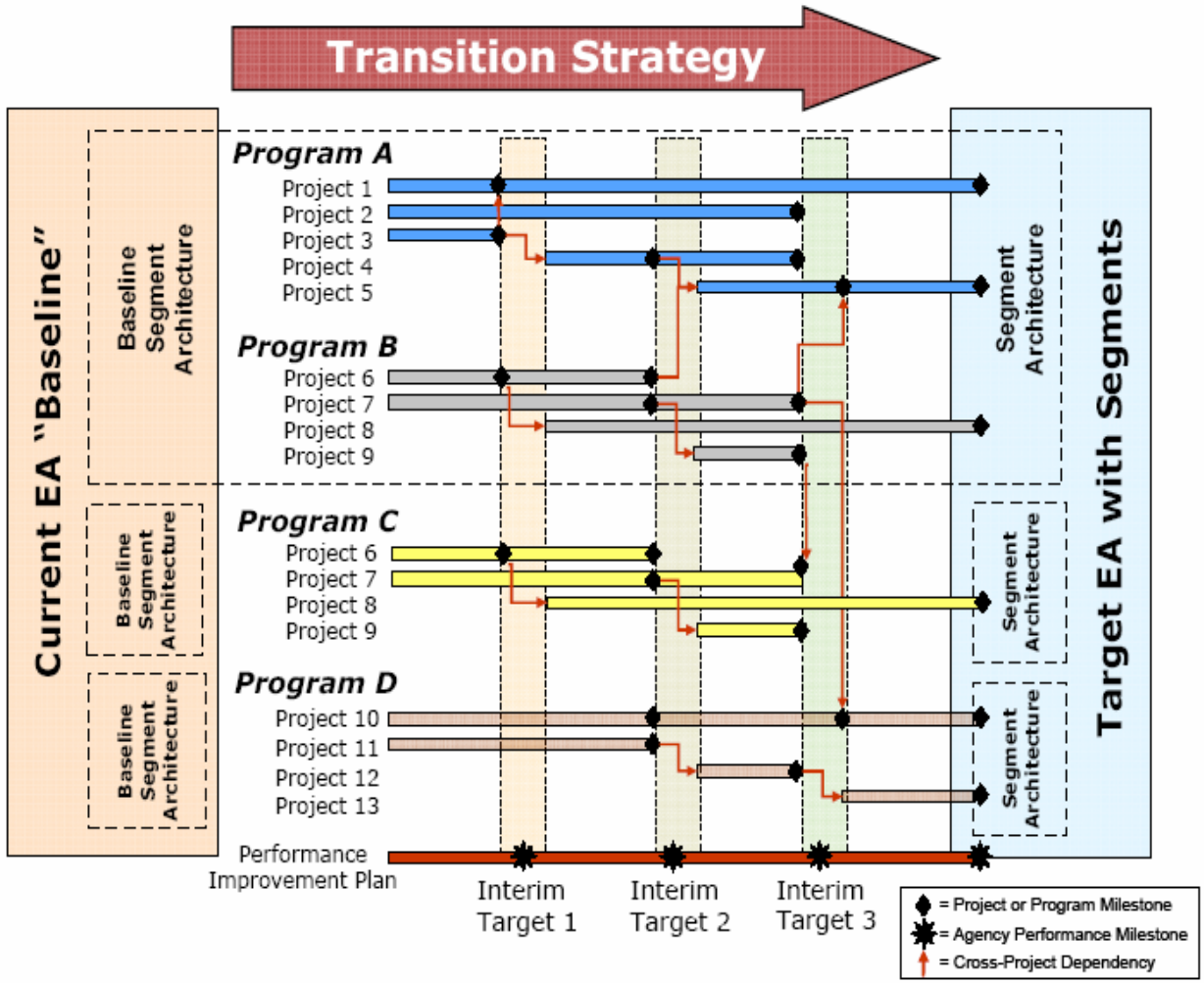
Stage III - Selection Activities.

The following table provides a tool to determine where Stage III activities' outputs should be documented, identify the location where data is maintained, identify the owners of associated data, and document any corrective actions identified to improve the data or complete the activity.

Goals, Objectives, Activities	EA Component	Information Location	Information Owner	Issues
A. Evaluate Individual Proposals 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.[24] a. Define minimally acceptable processes for assessing proposals.				
i. Validate the identification and mapping of security and privacy controls to the five enterprise architecture reference models.	All reference models			
ii. Validate the identification and mapping of security and privacy controls to the 17 security and 17 privacy control families.				
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.	Transition Strategy, Investment Portfolio[25]			

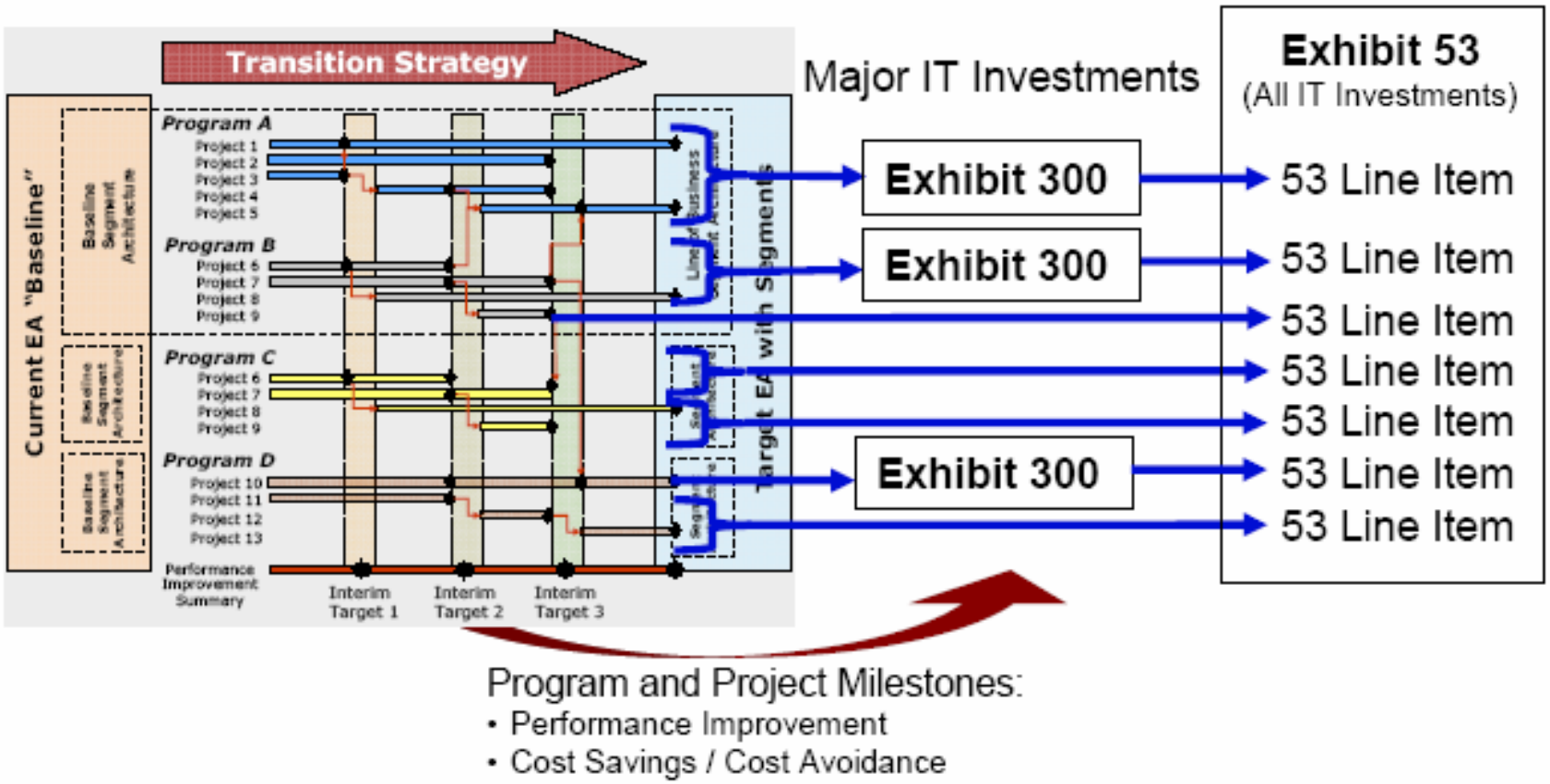
FEA-SPP Methodology

In the segment architecture transition strategy, individual programs and project level plans are defined for each segment architecture, while taking into account any dependencies that crossover into other segments. The FEA-SPP helps to identify security and privacy solutions within and between segments.



FEA-SPP Methodology

The EA transition strategy should include clear linkage between initiatives identified in the transition strategy and specific investments in the agency's investment portfolio, including security and privacy.



Validating
The FEA-SPP

FEA-SPP Validation

Validation testing was conducted at the Department of Justice (DOJ) and the Department of Housing and Urban Development (HUD).

- Each Department contributed a cross-functional team of 6-10 people
- Each Department's team participated in about 16 hours of facilitated sessions over the course of about four weeks.

External update activities consisted of reviews of related and recently published documentation. This included reviews of OMB, FEA, and NIST documentation. The validation activities resulted in the collection of the following recommendations:

- Clarify the general intent of the document
- More specifically describe activities and their outputs
- Make terminology less complex and discipline-specific
- Make stronger linkages to external OMB, FEA and NIST documentation and activities
- Allow for varying architectural maturity among implementing organizations

Recent Activities and Next Steps for the FEA-SPP

Recent Activities / Next Steps

Spring/Summer 2006

Validation testing completed at DOJ and HUD. Version 2.0 of the FEA-SPP was released by OMB.

Fall 2006

Scott Bernard of FRA/DOT was named as co-Chair with Sallie McDonald of DHS for addressing FEA-SPP issues and development via the Federal CIO Council's Architecture and Infrastructure Committee.

Winter 2007

Raising awareness of the FEA-SPP through presentations at security and architecture conferences / government meetings. Implementation working group of government and industry representatives to be formed.

Spring/Summer 2007

Agency implementation of FEA-SPP v2.0 begins. The Federal Railroad Administration plans to implement from Apr – Sep '07.

Points of Contact

Federal CIO Council
Architecture and Infrastructure Committee

FEA-SPP Co-Chairs:

Scott Bernard
Deputy Chief Information Officer
Federal Railroad Administration
Department of Transportation
scott.bernard@dot.gov

Sallie McDonald
Special Assistant to the Assistant Secretary,
Infrastructure Protection
Department of Homeland Security
sallie.mcdonald@dhs.gov