



Updates on the Federal Enterprise Architecture Program

(ISPAB Quarterly Meeting)

Dick Burk

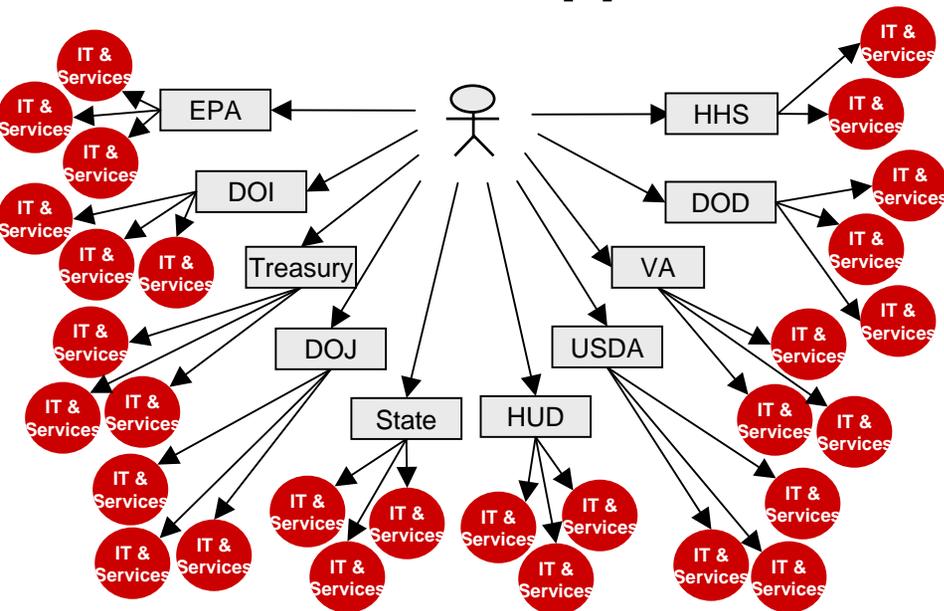
Chief Architect and Director, Federal Enterprise Architecture Program, OMB

December 7, 2005

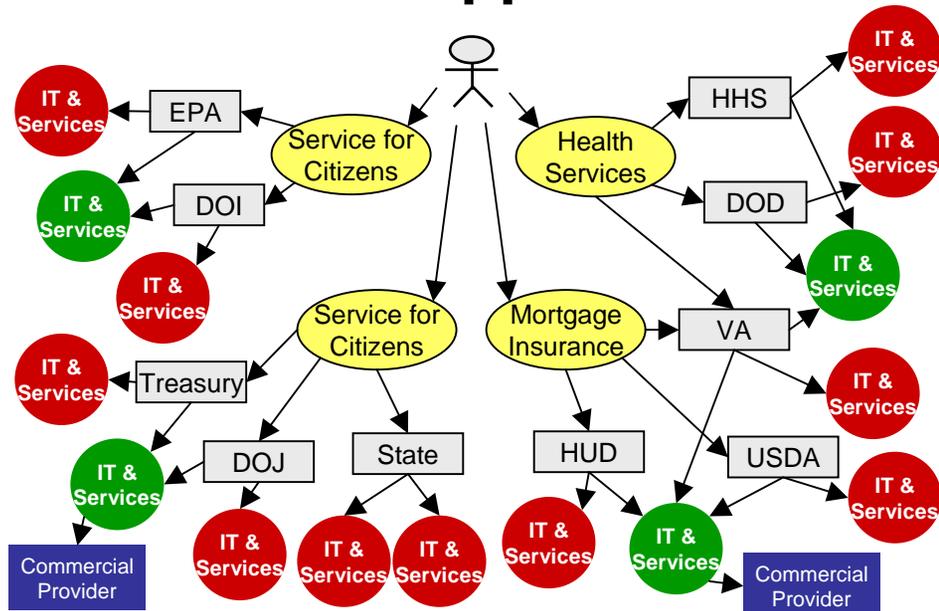


Future Direction: Citizen-Centered Services

The Historical Approach ...



The Future Approach ...



= Service for Citizens

= Agency-specific Service = Common Service

= Commercial Provider

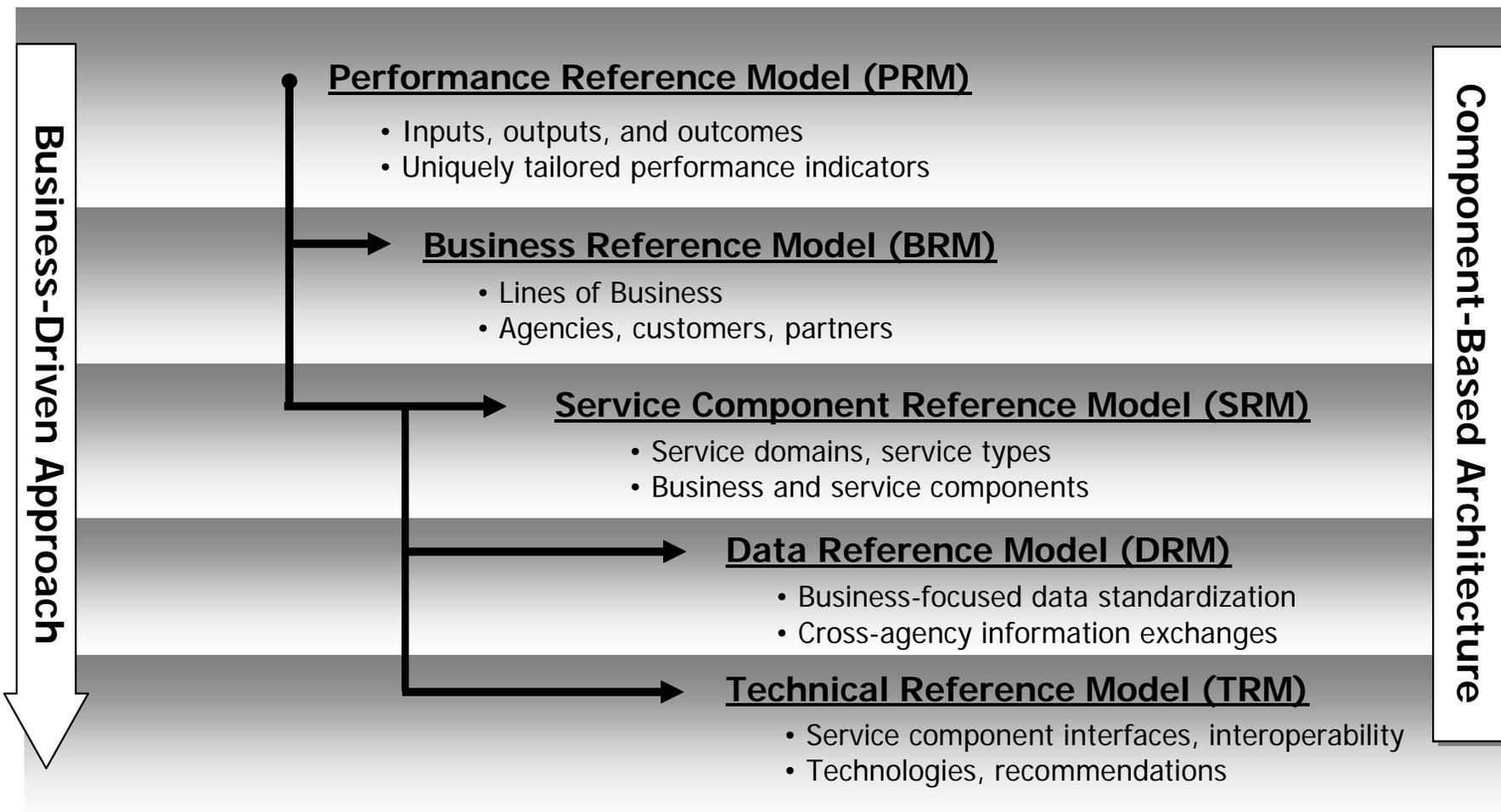


Transformation to Citizen-Centered Services

- OMB plays role to encourage agencies to become more effective and efficient
 - Public Sector does not have the discipline of profitability
- Agencies need to ask the question, “What functions are core to my mission?”
 - Defines what is fundamental to the organization
 - Build for Excellence, Buy for Competence

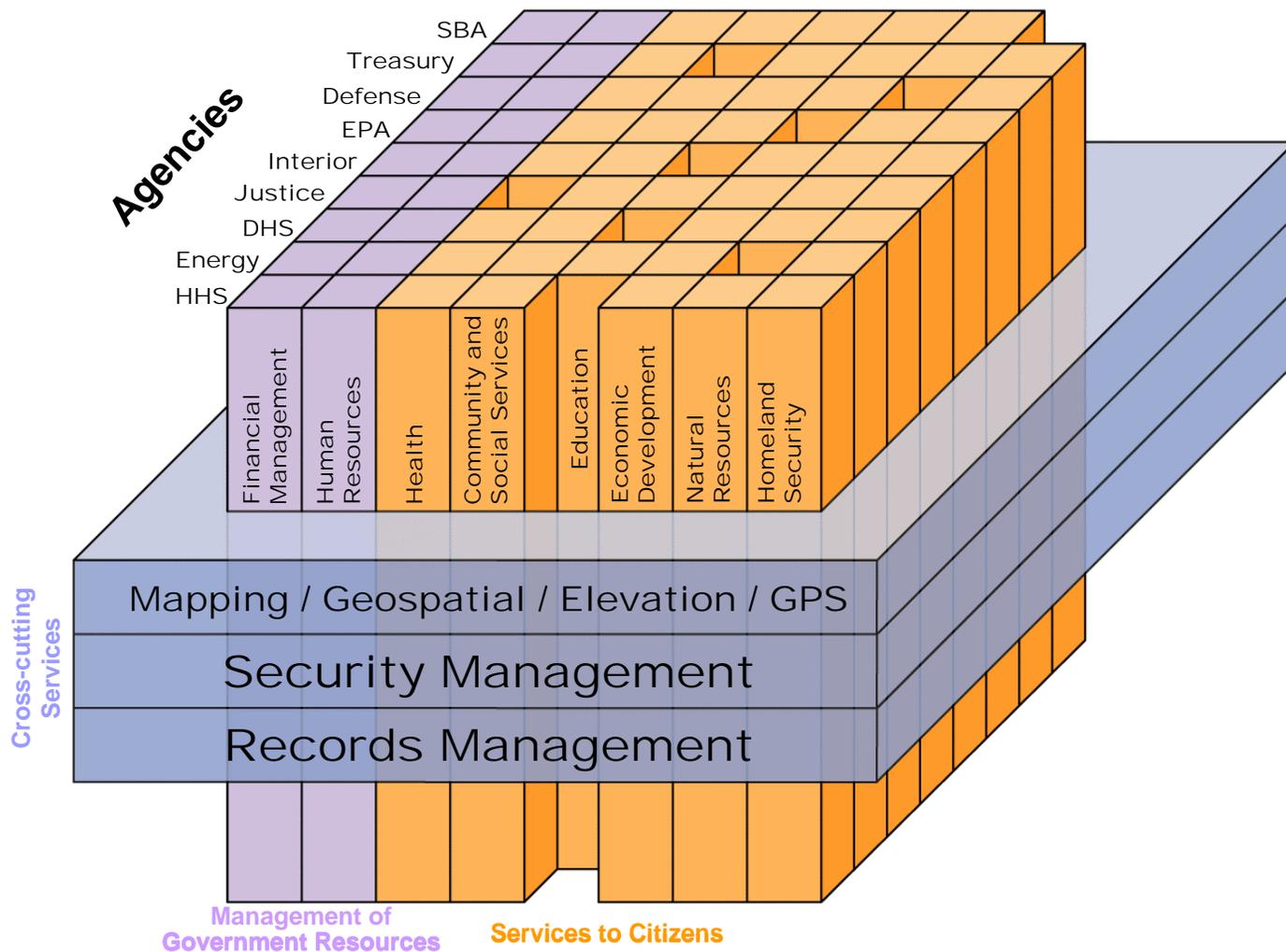


FEA Reference Models





LoBs and Services





CONOPS

ARCHITECT

- Develop and maintain enterprise architecture
- Review, reconcile and approve segment architecture for the agency's core lines of business and common IT services

Architectural Portfolio

INVEST

- Select IT initiatives to define the agency's IT investment portfolio
- Control IT investments
- Evaluate IT investments

Investment Portfolio

IMPLEMENT

- Develop and maintain segment architecture
- Develop IT program management plan
- Execute IT projects

Transition Strategy





E-Gov Status

Focus is on three main areas:

1. Lines of Business

Operational Phase

- Human Resources (HR) Management, Financial Management (FM), Grants Management (GM), Case Management (CM), and Federal Health Architecture (FHA)

Planning Phase

- Information Systems Security (ISS)

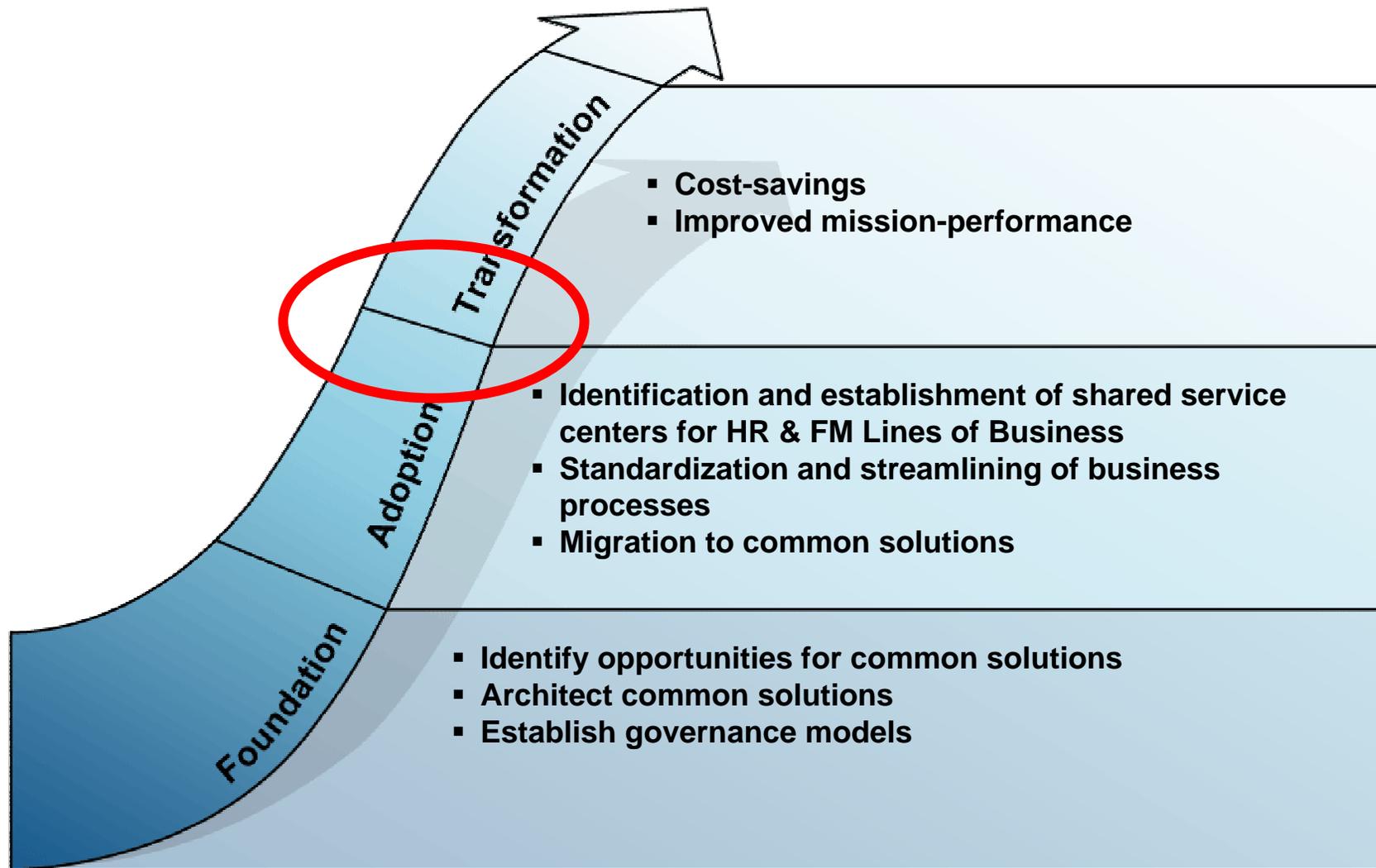
2. E-Gov Initiatives

- Driving toward usage and adoption by agencies
- Self-sustaining fee-for-service model

3. SmartBUY Agreements



E-Gov Future Direction





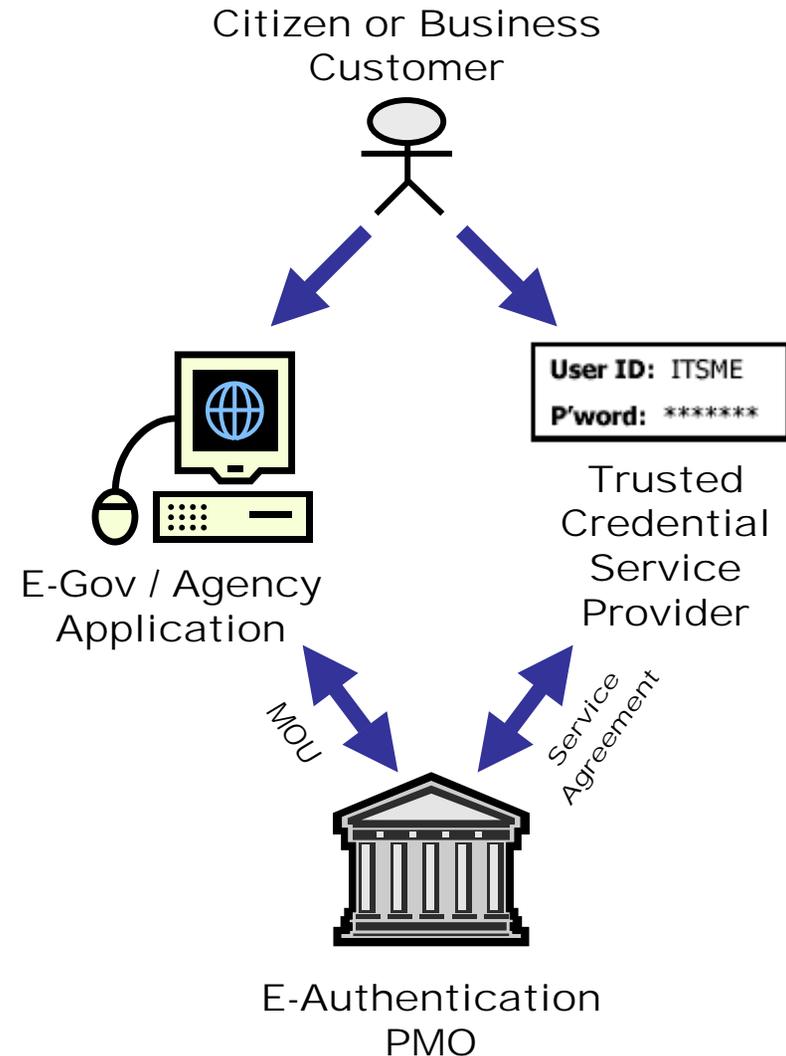
- CORE.gov
 - Repository for service components
 - Contains a collaboration tool

The screenshot shows the CORE.gov website interface. At the top left is the CORE.gov logo with the tagline "Component Organization and Registration Environment". To the right of the logo is a "User:" field. Below the logo is a navigation bar with tabs for "My pages", "Projects", and "Community". On the left side, there is a search box with a "Go" button and a link to "Advanced search". Below the search box is a "How do I..." section with a question mark icon, containing links to "View the CORE.GOV Index of Components as a PDF?", "View the CORE.GOV Index of Components in Word?", "Contact CORE.GOV?", and "Get help?". Below this is a "Links of Interest" section with links to "GSA", "FEAPMO", and "FirstGov". The main content area features a heading "Welcome to CORE.GOV - FEA's Center for Components" and a paragraph of introductory text. Below the text are three call-to-action buttons: "Request a Project Management Workspace", "Recommend a Component for Inclusion", and "Find a Component for Reuse". At the bottom of the main content area, there is a paragraph of text that includes a link to "Find a Component" and a link to "register" for an account on CORE.GOV.



CORE.gov Example: E-Authentication

- Provide standards-based authentication for Federal E-Gov applications
- Provide a uniform process for establishing electronic identity
- Eliminate the need for each initiative to develop a redundant solution for identity verification and electronic signatures
- Enable citizens and businesses to use credentials issued by commercial entities to conduct transactions with the government
- First component to be submitted to CORE.gov
- More info at www.cio.gov/eauthentication





IPv6 Implementation

OMB Memorandum 05-22 directs agencies to successfully transition their network backbone to Internet Protocol version 6 (IPv6) by June 2008, and....

1. Identify an IPv6 agency lead
2. Develop a network backbone transition plan for IPv6
3. Complete two (2) inventories of IP-aware devices and technologies
 - First is due in November 2005
 - Second is due in June 2006
4. Complete an IPv6 transition impact analysis
5. Complete an IPv6 progress report
6. Submit to OMB all of these items (with the exception of the second inventory) with their February 28, 2006 Enterprise Architecture assessment

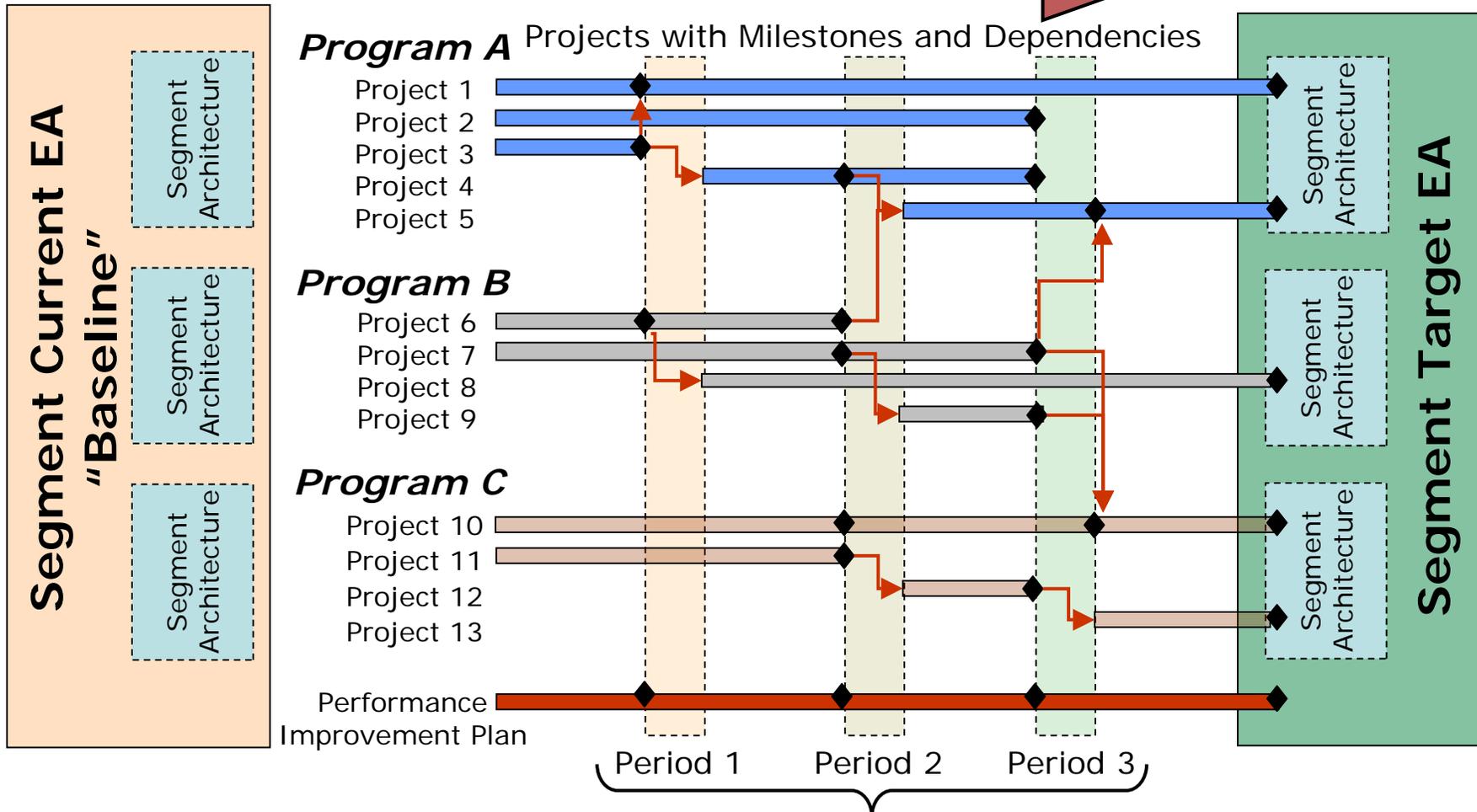


EA Assessment Framework 2.0

- Three Capability Areas
 - Completion
 - Use
 - Results
- EA Assessment Timeline
 - Annual Assessment Process
 - Quarterly Review Process



Transition Strategy





FEA Principle: Security and Privacy

- ***Security and Privacy are Design Standards***
 - Security and privacy are integral parts of government operations, and are designed into the architecture.
- **Rationale:**
 - Government must protect confidential information to increase public trust and improve the security of its resources.
- **Implications:**
 - Security and privacy requirements must be defined in the context of the business, and integrated into the entire architecture.
 - Security and privacy must be implemented consistently government-wide.



Business Reference Model (BRM)

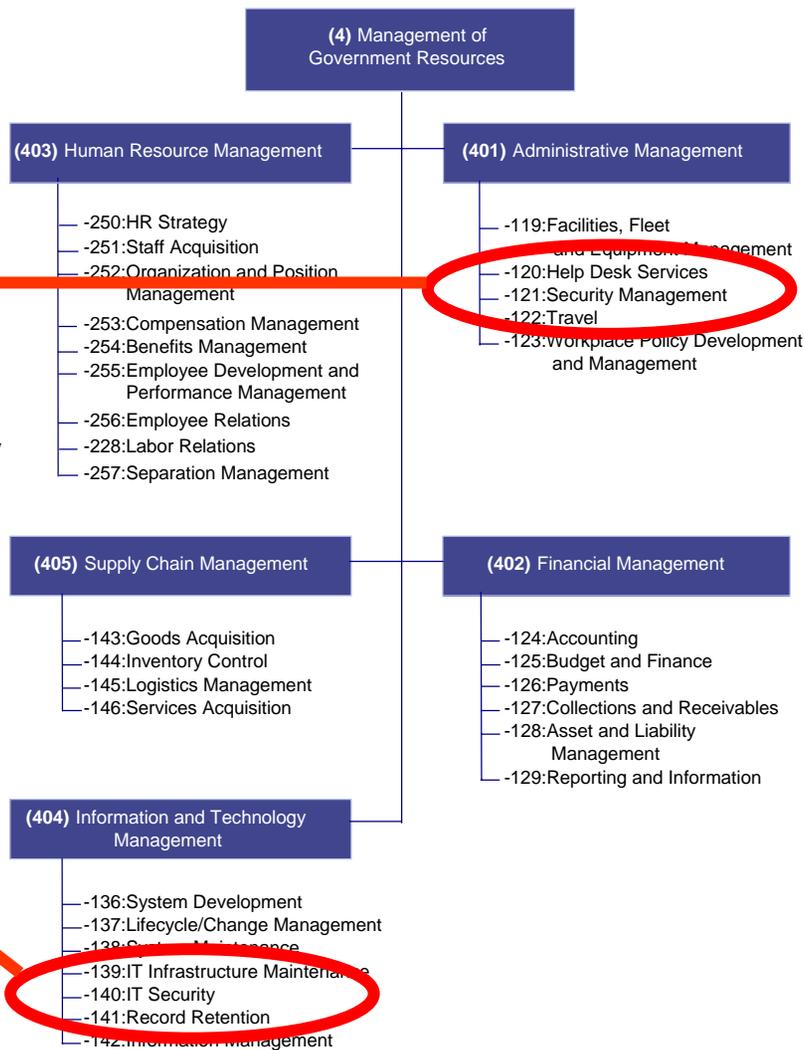
The Business Reference Model (BRM)





Management of Government Resources

- Administrative Management
 - Security Management
- Information and Technology Management
 - IT Security





Service Component Reference Model

Service Domains	Service Types
Customer Services	<ul style="list-style-type: none"> • Customer Relationship Management • Customer Preferences • Customer Initiated Assistance
Process Automation	<ul style="list-style-type: none"> • Tracking and Workflow • Routing and Scheduling
Business Management Services	<ul style="list-style-type: none"> • Management of Process • Organizational Management • Investment Management • Supply Chain Management
Digital Asset Services	<ul style="list-style-type: none"> • Content Management • Document Management • Knowledge Management • Records Management
Business Analytical Services	<ul style="list-style-type: none"> • Analysis and Statistics • Visualization • Knowledge Discovery • Business Intelligence • Reporting
Back Office Services	<ul style="list-style-type: none"> • Data Management • Human Resources • Financial Management • Asset / Materials Management • Development and Integration • Human Capital / Workforce Management
Support Services	<ul style="list-style-type: none"> • Security Management • Collaboration • Search • Communication • Systems Management • Forms Management



SRM: Security Management Service Type

Service Component	Definition
Identification and Authentication	Support obtaining information about those parties attempting to log on to a system or application for security purposes and the validation of those users
Access Control	Support the management of permissions for logging onto a computer or network
Encryption	Support the encoding of data for security purposes
Intrusion Detection	Support the detection of illegal entrance into a computer system
Verification	Support the confirmation of authority to enter a computer system, application or network
Digital Signature	Guarantee the unaltered state of a file
User Management	Support the administration of computer, application and network accounts within an organization
Role / Privilege Management	Support the granting of abilities to users or groups of users of a computer, application or network
Audit Trail Capture and Analysis	Support the identification and monitoring of activities within an application or system



Security and Privacy Profile

- Phase I completed in July 2004
- Phase II currently in progress
 - Being “piloted” at two federal agencies
 - Addresses other guidance released since Phase I
 - To be refined by Spring 2006
- Provides a methodology for agencies to define security and privacy requirements and investments within the context of EA



Security and Privacy Profile

In more detail, Phase II will include and reflect:

- An enterprise approach linking architectures and reference models to system-level security activities.
- Buy-in from CIOs and other agency stakeholders across the Federal Government.
- Useful implementation tools to assist agencies.
- Lessons learned from real-world implementation of the FEA SPP.
- Integration with FEA and other Federal guidance.



Information Systems Security (ISS) LOB

- Provide government-wide ISS services to be used across agencies
- Four common solution areas have been defined:
 - Training
 - FISMA Reporting
 - Situational Awareness and Incident Response (SAIR)
 - Security Solutions
- Plan is to establish 3 Centers of Excellence (COEs) for each of the 4 common solutions
- Required and optional common solutions will be phased in over 2 to 3 years



For Further Information:
www.egov.gov



E-Gov Results

Government to Citizen	Government to Government
<ul style="list-style-type: none">5.1 million taxpayers filed using Free-FileRecreation One-Stop provided easy access to 3,200 federal parks & other recreation sites	<ul style="list-style-type: none">51,000 users registered with DisasterHelp.govDisaster Management services used in 111 actual emergencies
Government to Business	Internal Efficiency & Effectiveness
<ul style="list-style-type: none">4.4 million electronic applications received for Employer Identification Numbers (EIN)6.5 million business tax forms filed electronically	<ul style="list-style-type: none">Job-seekers use USAJOBS to create between 90,000 and 100,000 resumes per monthE-Payroll consolidating payroll providers from 26 to 4

LoBs projected to save over \$5 billion dollars in the next 10 years.