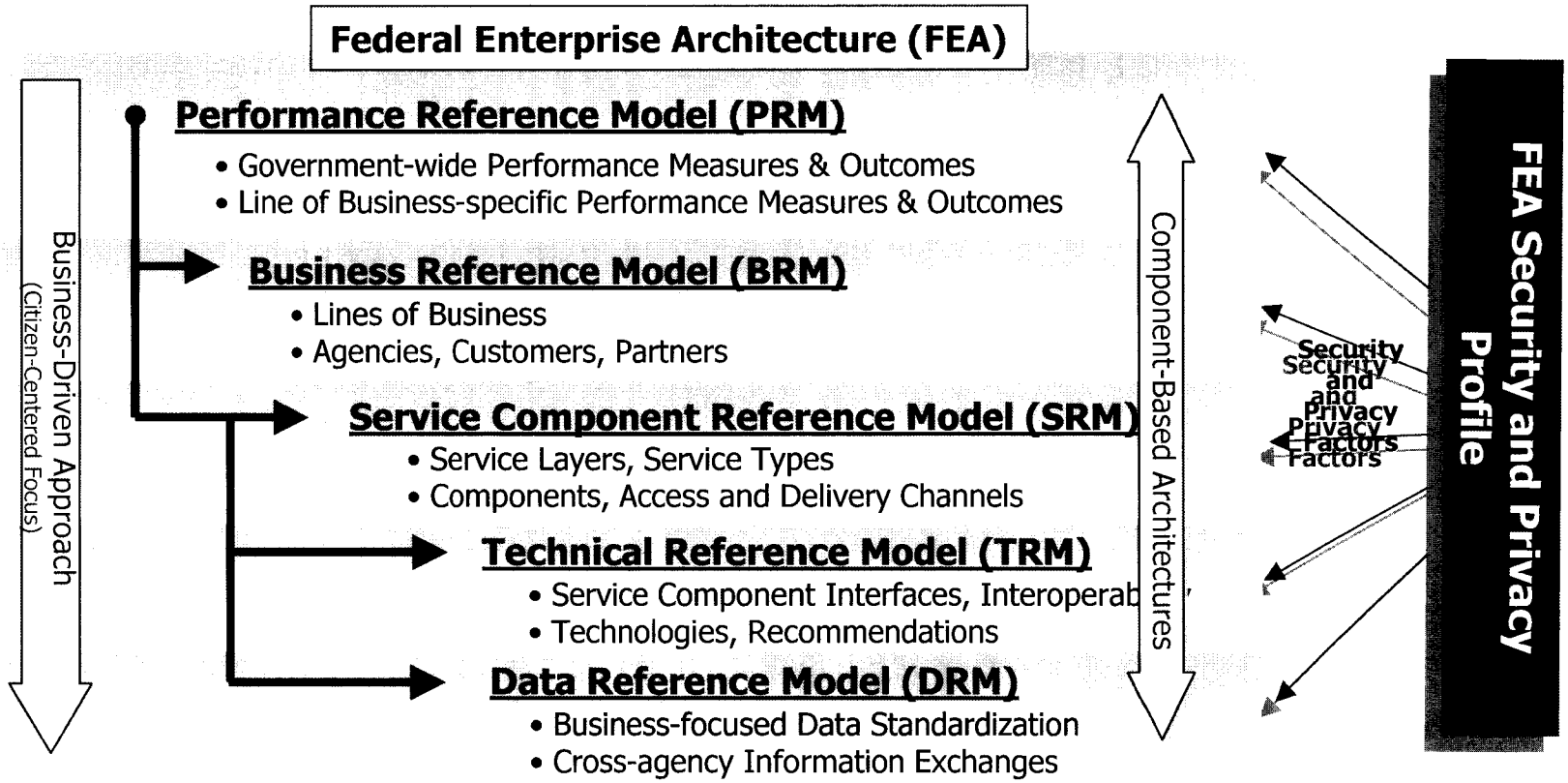
Federal Enterprise Architecture Security and Privacy Profile

Presented to:
Information Security and Privacy Advisory Board Meeting
September 2004

The Federal Enterprise Architecture (FEA) Consists of a Series of Interrelated Reference Models Designed to Facilitate Cross-agency Collaboration and Horizontal/vertical Information Sharing



There is a need for an additional view of the FEA that addresses and highlights information security and privacy

The FEA SPP is a multi-phase collaborative effort between Government and industry

- In June 2003, the Federal CIO Council began an effort to extend the FEA to address the important areas of security and privacy
- Booz Allen, MITRE and other industry organizations such as the IAC were enlisted to help develop the profile
- An initial document, "The FEA Security and Privacy Profile: Phase I," was finalized in July 2004
- THE CIO Executive Committee recommended that follow-on efforts (Phase II) should be undertaken to provide more detailed guidance on security and privacy for process owners, managers and other decision makers

Phase I addressed a need for an additional view of the FEA that addresses and highlights elements of security and privacy

- Intended to provide guidance to process owners, managers and other decision makers in designing and deploying security and privacy measures that ensure the protection and confidentiality of information
- Intended to serve as a uniform and repeatable methodology that applies to and leverages the FEA reference models to promote early identification of security and privacy issues
- Introduced the FEA Security and Privacy Profile and the key concepts of how security and privacy will "overlay" with the FEA reference models.

Phase II will further refine the SPP to provide a security and privacy roadmap for Federal IT investments

- Support risk-based executive decision making
- Leverage best practices in enterprise management of security and privacy (NIST, et al)
- Meet the agency needs for planning for security and privacy for information technology acquisition and to assist budget approval
- Provide the methodology to assist OMB for evaluating FISMA compliance
- Provide pragmatic full-lifecycle perspective for ongoing agency security and privacy requirement management
- Provide OMB validation that due diligence has been done for security and privacy prior to budget submission

Phase II initiative will leverage the NIST guidance and use a scenario to validate the FEA Security & Privacy Profile

Key Elements of Phase II FEA Security & Privacy Profile Initiative

FEA/NIST Bridge

- Outline a framework for agency or business owner to utilize the FEA reference models to identify security controls for their system

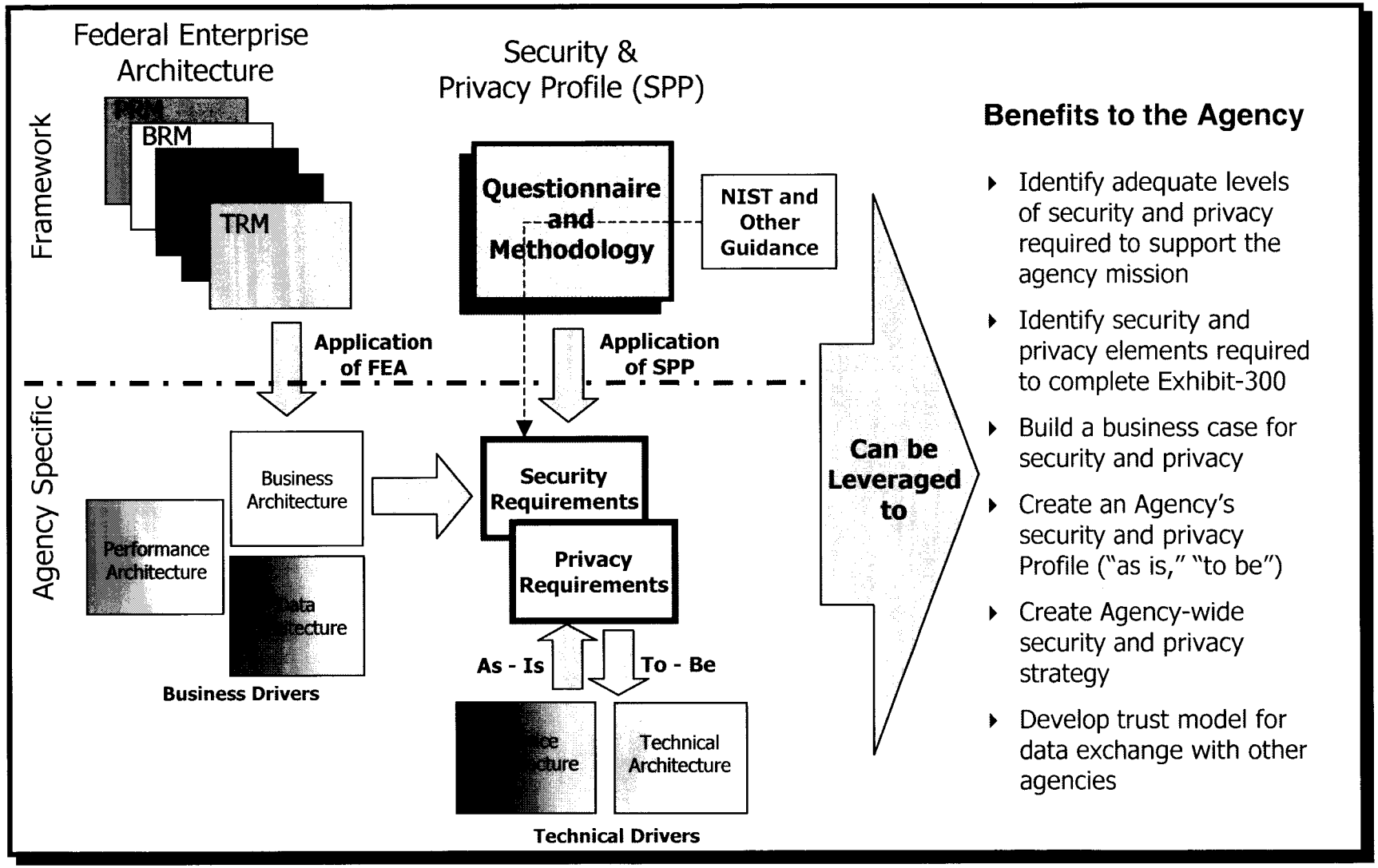
Privacy

- Describe how privacy fits within the models, provide privacy principles and privacy controls

Scenario

- Case study using the FEA Security Phase II framework to pilot the framework and to provide a "real world" example of the process described above. Could include several sub-components (I.e., trust model, privacy, etc.)

The notional concept of the SPP will use the architectures created from the FEA to generate high-level security and privacy requirements



Benefits to the Agency

- Identify adequate levels of security and privacy required to support the agency mission
- Identify security and privacy elements required to complete Exhibit-300
- Build a business case for security and privacy
- Create an Agency's security and privacy Profile ("as is," "to be")
- Create Agency-wide security and privacy strategy
- Develop trust model for data exchange with other agencies

Coordination strategy involves mechanisms to address three key objectives that are critical to the success of the project

Key Roles and Responsibilities

Governance Element	Key Objectives	Frequency	Mode	Primary Role
Governance Board (GB)	Provide strategic direction and resolve conflicts	Monthly	Checkpoint Sessions	• Provide oversight and guidance • Resolve conflicts • Approve deliverables
Point of Contact (POC)	Ensure relevancy of the deliverables to the agency	Bi-Weekly	Telecon	• Represent the interest of the organization • Coordinate review and agency feedback • Ensure agency buy-in to the approach • Brief the governance board members
Subject Matter Experts (SMEs) - Privacy - Security - E-Payment (Biz line) - … - …	Ensure technical correctness of the deliverables	As Needed	As Needed	• Provide technical expertise • Validate methodology and applicability of the framework

Lessons Learned

- Establish clear goals and objectives from the beginning
- Get buy-in from government representatives at all levels
- Establish a clear governance structure to get the correct participation
- Identify a senior visionary who will guide the activity