# Security and Privacy Profile for the Federal Enterprise Architecture

## Achieve Effective and Cost-Efficient Security and Privacy

***How will you address increasingly complex security and privacy requirements while accomplishing mission objectives?***

The Federal Enterprise Architecture Security and Privacy Profile (FEA SPP) offers a business-driven approach to turning these requirements into effective and efficient solutions by:

- Documenting security and privacy requirements and capabilities using the Federal Enterprise Architecture framework.
- Leveraging system level security and privacy activities.
- Defining a governance approach to discover and reconcile disparate mission, security, and privacy requirements.

### Who created the FEA SPP?

The Office of Management and Budget and the Federal Chief Information Officers Council developed the FEA SPP. Assessments of policies and guidance related to enterprise architecture, security, privacy, and capital planning documents ensured that the FEA SPP is relevant and complementary to current activities. The FEA SPP was field tested through validation exercises at the Department of Housing and Urban Development and the Department of Justice. During these exercises, senior cross-functional teams walked through the FEA SPP methodology to ensure its usability and applicability. Although limited in duration and scope, these exercises led to meaningful changes in the Departments' business processes.

### How does the FEA SPP work?

The FEA SPP documents a step-by-step, multi-disciplinary approach to ensure that an agency or business segment's security and privacy investments meet business requirements, are reflective of federal policy, and are cost-effective.

## The FEA SPP Methodology

| | Objectives | Benefits |
|---|---|---|
| **Stage 1: Identification** | Identify security and privacy requirements and capabilities, documenting them in the enterprise architecture. | Develop an enterprise perspective on security and privacy needs and capabilities. |
| **Stage 2: Analysis** | Assess unmet requirements. Assess current and planned capabilities. Evaluate trade-offs between alternative solutions. | Recommend security and privacy solutions with a better understanding of enterprise-wide mission impacts. |
| **Stage 3: Selection** | Evaluate proposed solutions, selecting those that best fit enterprise business needs. | Optimize the security and privacy investment mix in a manner that best meets enterprise-wide mission, security, and privacy requirements. |

# The FEA SPP applies existing enterprise architectures to develop an enterprise view of security and privacy

| 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.<br>■ 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.<br>■ 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.<br>■ 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.<br>■ Evaluate data sharing behaviors to assess and address security and privacy ramifications. |

## Links to the Federal Enterprise Architecture

The FEA SPP links system and program-level security and privacy activity to agency architectures through the FEA reference models. It describes how to document security and privacy requirements and capabilities within architectures, and how to leverage that documentation to inform business and investment decisions.

Enterprise decision-making necessitates the use of consistent language when describing system and program-level security and privacy requirements and capabilities. With regard to security, the FEA SPP leverages the seventeen security control families set forth in FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*. With regard to privacy, the FEA SPP introduces seventeen privacy control families. Similar to the security control families, the privacy control families provide a common framework for discussing and comparing the privacy features of disparate systems and programs.

### For More Information

Download the FEA SPP by visiting the Architecture and Infrastructure Committee web site at http://www.cio.gov/ or the Federal Enterprise Architecture website at http://www.whitehouse.gov/omb/egov/.