Federal Enterprise Architecture Security and Privacy Profile Version 3

Federal Enterprise Architecture
Security and Privacy Profile
Version 3.0 (May 5, 2009)

Sponsored By:
National Institute of Standards and Technology
Office of Management and Budget
Architecture and Infrastructure Committee, Federal Chief Information Officers Council

Working Draft

Table of Contents

1. Acknowledgements
2. Introduction
   2.0 Overview
   2.1 Target Audience
      2.1.1 Enterprise Infrastructure Role Support
      2.1.2 IT Capital Planning Role Support
      2.1.3 FISMA Compliance Role Support
      2.1.4 Senior Agency Official for Privacy Role Support
   2.2 Enterprise Architecture
   2.3 Relationship to FEA Reference Models
   2.4 Relationships to NIST Standards and Guidance
3. Understanding the History of the FEA SPP
   3.0 Background
   3.1 FEA SPP Version 1.0
   3.2 FEA SPP Version 2.0
4. The FEA-SPP Methodology
   4.1 Integrating with the Risk Management Framework
5. The Security and Privacy Framework
   5.1 FEA-SPP Framework Concept
6. Security and Privacy Segment Architecture
6.1 The Federal Segment Architecture Methodology
6.2 Using the FSAM To Implement Security and Privacy Controls

7. Appendix A
A.1 THE FEA-SPP Security Control Assessment Tool

8. Appendix B
B.1 Recipe for filling out SPP

9. References
R.1 Laws
R.2 Executive Policy
R.3 Federal Standards
R.4 International Guidance
R.5 Guidance
R.6 Other Resources

1. Acknowledgements

The 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 the public and private sectors, doing so in the context of the Federal law and guidance on enterprise architecture, information security, data privacy, capital planning, project management, and records management.

The FEA-SPP Working Group was co-led by Dr. Scott Bernard of the U.S. Department of Transportation's Federal Railroad Administration and Dr. Ron Ross of the National Institute of Standards and Technology. Members of the Version 3 FEA-SPP core writing group for included:

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marian Cody</td>
<td>Environmental Protection Agency</td>
</tr>
<tr>
<td>Waylon Krush</td>
<td>Lunarline, Inc.</td>
</tr>
<tr>
<td>John McCue</td>
<td>Executive Office of the President</td>
</tr>
<tr>
<td>Kenneth P. Mortensen</td>
<td>Attorney at Law (formerly Department of Justice)</td>
</tr>
<tr>
<td>Scott Ward</td>
<td>GiniCorp</td>
</tr>
</tbody>
</table>

Thank you to each of the FEA-SPP Working Group members and to those who provided input and feedback on the
various drafts of Version 3.0, this document could not be completed without the help of these people.

_______________________________
Ron Ross, Ph.D.
Manager, FISMA Implementation Project
National Institute of Standards & Technology

_______________________________
Scott Bernard, Ph.D.
Deputy CIO/Chief Enterprise Architect/ISSO
Federal Railroad Administration

2. Introduction

2.0 Overview

The Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) is a scalable and repeatable conceptual methodology for addressing information security requirements that support privacy from a business-centric perspective at the enterprise, segment, and solution levels of an agency’s enterprise architecture. The FEA-SPP supports the identification and evaluation of those security requirements that provide a foundation for appropriate privacy protections throughout the architecture planning framework using the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and the FEA-SPP Tool; both of these support the development and implementation of baseline security controls using NIST procedures and FEA guidance. The FEA-SPP provides 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 an agencies’ strategic planning and investment decision processes.

The FEA-SPP:

• Promotes an understanding of an organization’s security requirements that support privacy protections, its capability to meet those requirements, and the risks to its business associated with failures to meet requirements.

• Integrates the NIST Risk Management Framework (RMF) and System Development Life Cycle (SDLC) security planning into an organization’s enterprise, segment, and solution architectures to ensure relevant security privacy requirements for privacy are baked in.

• Helps program executives understand how security and privacy requirements fit within the EA planning framework, while leveraging standards and services that are common to the enterprise or the Federal government as appropriate.
• Improves agencies’ processes for incorporating privacy and security into major investments and selecting solutions most in keeping with enterprise needs.

The FEA-SPP evaluates security and privacy at an enterprise-level in the context of the Federal Enterprise Architecture (FEA). The FEA asks Federal agencies to look at their operations from common business, performance, services, technologies, and data views. Agencies capture information in those categories using the appropriate enterprise architectural reference model, which enables the agency to understand to understand how its organization operates today, how it intends to operate in the future, and the changes that must take place if it intends to transition to that future state. The FEA-SPP illustrates how to adapt enterprise security objectives of confidentiality, integrity, and availability, and the privacy objectives that ensure appropriate management of and protection of personal information. The government needs to create systems to protect their information yet make that information available to the appropriate people, set forth in a variety of Federal laws and regulations.

The FEA-SPP demonstrates how to incorporate security and privacy considerations that support privacy protections—when developing an Enterprise, Segment, or Solution architecture using approved Federal guidance and standards. The FEA-SPP integrates the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and the System Development Life Cycle (SDLC) planning principles to provide users with the ability to understand and manage risks associated with organizational information at the enterprise level, at the segment level, at the information system level, while at the same time controlling the risks to the individual’s information.

This document will provide a step-by-step methodology, illustrating how to select security and privacy controls, and scenarios for the use and implementation of the EA SPP. This whitepaper will also outline how the EA SPP aligns with the six-step RMF and the five-step SDLC.

2.1 Target Audience

The FEA SPP is a cross-disciplinary methodology that requires support and participation of experts from security, privacy, enterprise architecture, capital planning, and organizational business functions. It is written at a high level to make it understandable to a wide audience. Success of the FEA-SPP methodology hinges on understanding of each domain and their combined contribution toward mission accomplishment of an organization. Agencies should document those insights in the enterprise architecture and use them to promote the objectives of security and privacy across all enterprise activities and investments.

2.1.1 Enterprise Infrastructure Role Support

Those individuals in the role of supporting the infrastructure of the enterprise have the responsibility to establish and maintain the networks and systems in accordance with specified operational requirements, including those related to protecting the information assets of the organization from compromise by improper distribution, from damage caused by attack or system failure, or from mishandling that may break the proper chain of custody for the life of the data.

2.1.2 IT Capital Planning Role Support

The individuals in the role of supporting IT capital planning have the responsibility to apply a systematic approach to selecting, managing, and evaluating information technology investments in order to fund projects that advance the organization’s mission and presidential directive. The FEA-SPP provides a methodology for planning systems that provide the security for proper functioning of the organization in line with the objectives of management.
2.1.3 FISMA Compliance Role Support

The individuals in the role of supporting FISMA compliance have the responsibility for ensuring compliance with the Federal Information Security Management Act (FISMA) guidelines for IT systems security. FISMA provides a set of specific guidelines for federal agencies to plan for, budget, implement, and maintain secure systems.

2.1.4 Senior Agency Official for Privacy Role Support

The officials in the role of the agency official providing privacy policy and compliance support must have the ability to impact the development of information technology system on an enterprise-level. The Senior Agency Official for Privacy (SAOP) is responsible for ensuring that an agency applies the fair information practices as set out in the Privacy Act of 1974 into that agency’s collection, use and disclosure of personal information. The FEA-SPP provides a framework to integrate the SAOP’s mission with those roles at the agency focused on information technology and security.

2.2 Enterprise Architecture

2.3 Relationship to FEA Reference Models

2.4 Relationships to NIST Standards and Guidance

3. Understanding the History of the FEA SPP

3.0 Background

3.1 FEA SPP Version 1.0

3.2 FEA SPP Version 2.0

4. The FEA-SPP Methodology
4.1 Integrating with the Risk Management Framework

5. The Security and Privacy Framework

5.1 FEA-SPP Framework Concept

6. Security and Privacy Segment Architecture

6.1 The Federal Segment Architecture Methodology

6.2 Using the FSAM To Implement Security and Privacy Controls

7. Appendix A

A.1 THE FEA-SPP Security Control Assessment Tool

An assessment tool has been developed that helps users to determine the types of security and privacy controls that are needed for an information system or architecture segment based on the following four factors:

- The categorization of the enterprise, segment, or solution
- The sensitivity of data that is processed, stored, transmitted, managed, or reviewed in accordance with FIPS 199 (Civilian Federal), DoD 8500.1 (DoD), or CNSS 1199 (Intelligence Community)
- The phase of the system development lifecycle or acquisition phase the system or process is in
- The type of assessment method being used (NIST (Civilian Federal), DIACAP (DoD), NSS (IC))

- The FEA-SPP Tool integrates the National Institute of Standards and Technology (NIST), National Security Systems (NSS), Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), Risk Management Framework (RMF). The NIST and RMF support 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 controls relevant to the system or process risk associated with the mission of the Agency.

• The FEA-SPP Tool works under the assumption that the system or process has undergone a preliminary security categorization in accordance with (IAW) Federal Information Processing Standard (FIPS) 199, DoD 8500.1 or CNSS 1199. 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.

This tool was developed using Microsoft Access but installs without Microsoft Access being present on the information system. Subsequent versions of the tool will be platform and product neutral and include XML and web-based capability. The tool 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. The point of contact for evaluation copies of the tool is waylon.krush@dot.gov.

8. Appendix B

B.1 Recipe for filling out SPP

http://www.whitehouse.gov/omb/e-gov/fea/

9. References

R.1 Laws

Clinger Cohen Act of 1996. (Clinger Cohen Act)


Federal Acquisition Streamlining Act of 1994. (FASA)


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

Privacy Act of 1974. (Privacy Act)

R.2 Executive Policy


R.3 Federal Standards


R.4 International Guidance


R.5 Guidance


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

R.6 Other Resources


