Coordinating Draft

The FEA Security and Privacy Profile Phase I Final

A Foundation for Government-wide Improvement

FEAPMO
FEDERAL ENTERPRISE ARCHITECTURE
PROGRAM MANAGEMENT OFFICE

ACKNOWLEDGEMENTS

For their dedication and commitment to the development of initial ideas and mature concepts contained in this document, the CIO Council would like to acknowledge the following:

Our government partners –

The Office of Management and Budget (OMB)

The National Institute for Standards and Technology (NIST)

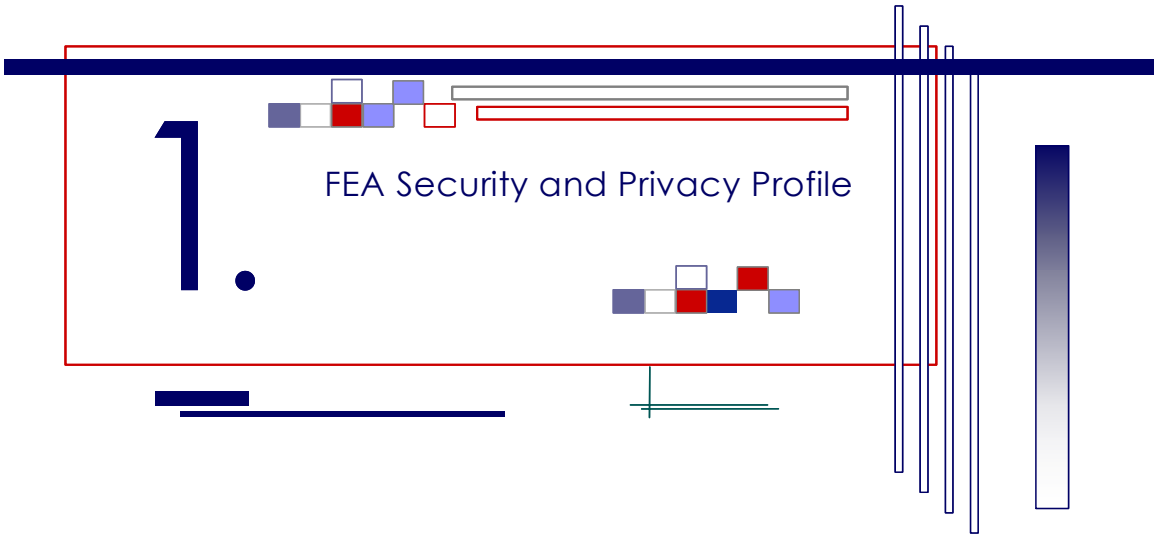
Our industry partners –

Booz Allen Hamilton

The Industry Advisory Council (IAC) Security Committee

MITRE

TABLE OF CONTENTS



INTRODUCTION

The Federal Government continues to enhance enterprise architecture implementation strategies in an effort to improve performance of information technology (IT) resources. To serve as a decision-making tool in developing IT investment strategies, the Federal Enterprise Architecture (FEA) has been established as the overarching architectural guide for the Federal Government. To complement and continue the process of developing the FEA, the Office of Management and Budget (OMB) and the Chief Information Officer (CIO) Council's Architecture and Infrastructure Committee have specified the need for an additional view of the FEA that addresses and highlights elements of security and privacy.[1]

The CIO Council envisions the FEA Security and Privacy Profile[2] as a tool for process owners, managers and other decision makers to ensure security and privacy are integrated within the FEA reference models, the nature of which are described in Section 2. The Security and Privacy Profile will provide guidance on designing and deploying measures that ensure the protection of information resources. These measures will be developed in accordance with legislative and regulatory security and privacy requirements, as well as from other applicable policies and guidelines.

To safeguard business data and information, trade-offs among three families of controls should be considered: management, operational, and technical. In addition, the benefits, costs, and risks associated with achieving adequate protection must be weighed. To accomplish this, a primary objective of the FEA Security and Privacy Profile is to provide a methodology for making risk-based decisions that will balance the critical need for information sharing between organizations with the prudent application of security policies and mechanisms.

To address the dynamic tension between security and information sharing interests, mission and business leaders can achieve a degree of balance if they employ a multi-attribute risk-based decision-making methodology. Information assurance specialists by themselves can no longer be charged to protect enterprise resources, especially when the enterprise extends along horizontal and vertical business lines. Enterprise executives must agree on security and privacy policies and control mechanisms that will be used to safeguard resources by integrating those decisions into their system acquisition and change management processes. To support this, a risk-based decision-making methodology must provide a set of options that help establish the right degree of data sharing, system access, resource security, and personal privacy. Such a methodology will help decision-makers achieve an acceptable balance between their mission and security objectives.

[1] See *Terms of Reference, Development of a Security Architecture Profile for the Federal Government.*
[2] The FEA Security and Privacy Profile provides an understandable, consistent, repeatable, scalable, and measurable methodology that uses relevant FEA reference model information (i.e., context and conditions) to help business owners accurately determine security categorization and establish an appropriate set of security controls in accordance with NIST guidance.

The FEA Security and Privacy Profile Phase I Final

This document responds to Phase I of the FEA Security and Privacy Profile as specified within the CIO Council's *Terms of Reference* (Appendix D). The concepts covered not only leverage proven examples of government information security architectures but also map an approach for addressing security and privacy in the FEA. Section 1 of this document provides scope, audience, background and objectives of this methodological effort. Section 2 introduces the FEA Security and Privacy Profile and the key concepts of how security and privacy[3] will "overlay" with the FEA reference models. Section 3 discusses the next steps and important considerations to be addressed in Phase II of this study, during which the Phase I concepts will be further developed and refined. During Phase II, the project team expects to work closely with the CIO Council, the Industry Advisory Council (IAC) Security Committee, and other industry organizations to facilitate development and refinement efforts.

SCOPE

The FEA Security and Privacy Profile is a *methodology* that allows agencies to establish an initial set of security controls for a given business process. Agencies will not find a set of controls for every line of business in this document. Instead, they will find an understandable, consistent, repeatable, scalable, and measurable methodology for deriving a set of controls that best meet their core and unique business needs.

The profile is designed to provide an overlay on each FEA reference model that can be used to:

- Assist agencies in first identifying security and privacy needs and then linking those needs to NIST guidance at the program and system levels in support of the line of business4
- Translate procedural security and privacy requirements found at the business level into the technical controls necessary at the system level
- Promote early identification of security and privacy issues
- Disclose possible risk exposure; type of controls needed to manage the risk; potential costs for controls, and possible ways to combine controls to achieve the same goal at a lower cost

AUDIENCE

The FEA Security and Privacy Profile is intended for all business owners who need to make informed decisions based on an options analysis to ensure services are provided, cost targets are met, and residual risk is managed effectively. The following individuals who collaborate with business owners may also find this Security and Privacy Profile useful:

- Officials at the CIO or chief information security officer (CISO) level who evaluate the impact of applying management, operational, and technical controls and present options and/or recommendations resulting in appropriate solutions
- Cross-agency service providers who look for consistent, repeatable methodologies that can be used by multiple agencies and service-providing partners to establish a common trust environment and ensure a level of protection for shared services and resources (e.g., data and systems).
- Officials at the privacy advocate or chief privacy officer (CPO) level who coordinate the development, implementation, and maintenance of a enterprise privacy strategy and ensure adherence to Federal privacy laws and regulations

[3] Privacy considerations will be more fully addressed in Phase II work. See Phase II Considerations (page 20).

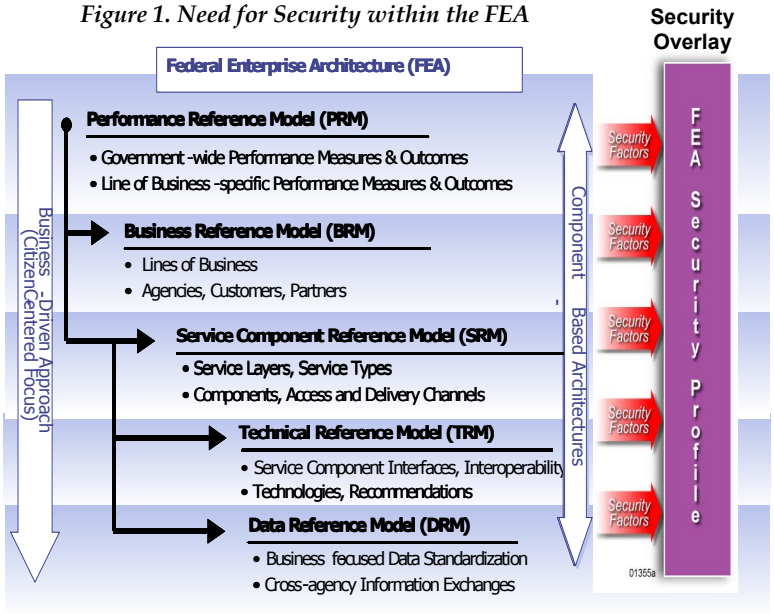
[4] FEA Security and Privacy profile Phase II efforts will include a review of the emerging standards and guidelines (e.g., NIST 800-60) to ensure consistency with the standards and guidelines and complement the guidelines where applicable.

While systems architects might find the FEA Security and Privacy Profile Phase I interesting, it is envisioned that the more detailed framework and sample use scenarios to be included in Phase II will be more applicable to their daily responsibilities.

BACKGROUND

As depicted in Figure 1, the FEA traditionally consists of five reference models: the Performance Reference Model (PRM), Business Reference Model (BRM), Service Component Reference Model (SRM), Technical Reference Model (TRM), and Data Reference Model (DRM). The significance of this representation is to demonstrate that these five models are designed to be interrelated and mutually supporting. Their purpose is to facilitate cross-agency collaboration in support of citizen-focused delivery of services.

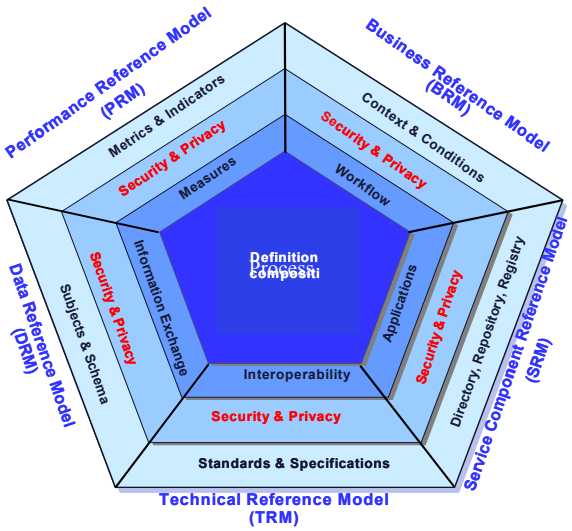
Figure 1. Need for Security within the FEA



It is a commonly held notion that each reference model contains vital information used by security practitioners to understand and shape a protection environment in support of the operational objectives envisioned in the BRM. Therefore, information should be identified, extracted, and presented in a way that communicates the nature, urgency, and scope of business requirements to appropriately define corresponding protection strategies. The business needs to share information in order to achieve a common set of reusable services. This must be a key factor that drives the security and privacy policies, mechanisms, and agreements.

Key components of the reference models must be assessed to effectively overlay security and privacy. Figure 2 illustrates the components of each reference model and shows a security and privacy layering requirement for each model. The PRM defines factors of business success and relates those measures to relevant technical metrics. The BRM outlines the basic Lines of Business (LOB) of the Federal Government and provides the "context and conditions" in which IT must operate. The SRM identifies IT components that can be used to support business activities. The TRM defines technical standards that should be used in government IT systems. Finally, the DRM defines the high-level data types that are used in government business processes. Together, the five models contribute to defining and building cost-effective IT support for government business processes. (Additional information on the FEA reference models can be found on the FEA Program Management Office Web site at www.feapmo.gov.)

Figure 2. FEA Components



The FEA Security and Privacy Profile Phase I Final

The role of the FEA Security and Privacy Profile is to identify, extract, and communicate reference model data to business owners and security and privacy practitioners (e.g., security stakeholders) so that appropriate protection responses can be proposed.

PRIVACY IN THE FEA SECURITY AND PRIVACY PROFILE

The FEA Security and Privacy Profile describes privacy considerations and requirements for controls. The concept of privacy and its associated issues is important for several reasons:

1. **Privacy is a significant issue.** For several years, OMB has required agencies to include privacy assessment information in capital planning activities as part of Form 300B. The E-Government Act of 2002 requires that Privacy Impact Assessments (PIA) be conducted before one of the following actions is undertaken: (a) developing or procuring IT that collects, maintains, or disseminates information in identifiable form from or about members of the public; or (b) under the Paperwork Reduction Act, initiating an electronic information collection process for 10 or more persons.

2. **Privacy is important to industry partners in implementing a robust E-Government program.** In fact, the IAC E-Government Shared Interest Group is currently sponsoring a study of E-Government privacy best practices.

3. **Privacy is closely linked to security.** Security is the necessary foundation for ensuring that privacy and security controls can be leveraged. To support this concept, controls can be grouped into four major categories:

   - *Direct support controls* are most critical to providing the security needed to ensure privacy requirements are met (i.e., personnel security, physical security, data integrity)

   - *Indirect support controls* are necessary for ensuring the system is adequately secure, able to operate when needed, and can be recovered if an incident occurs (i.e., risk management, contingency planning, incident management)

   - *Complementary controls* overlap to a high degree. The idea that some privacy elements may be covered by current security controls requirements (i.e., security control review, policy documentation, security awareness, training and education)

   - *Unique privacy controls* are unique to privacy legislation (i.e., data use, notice/choice, consent/authorization)

Defining Privacy

The definition of privacy in the United States is building around acceptable privacy principles dealing with Information in Identifiable Form (IIF). Emerging principles include:

- ***Accountability*** - assigned roles and responsibilities to assure application of privacy principles to IIF.

- ***Notice*** – openness regarding the authority for collecting IIF; the purpose of the collection; the location of the entity maintaining the IIF; with whom the IIF may be shared and why; rights an individual has in IIF; and the entity's polices, procedures, standards, and practices with regard to IIF.

- ***Minimum Necessary*** – collection of IIF should be limited to entity's legal authority and minimum necessary IIF the entity needs to perform the defined legally permitted task.

- ***Consent*** – an entity's collection of IIF should be contingent upon first obtaining an individual's consent to collection.

- ***Authorization*** – an entity does not collect, use, or disclose IIF in a manner inconsistent with its Notice unless it has first obtained the individual's written permission for the use or disclosure.

- ***Individual Rights/Individual Participation*** – an individual should be: Afforded the ability to access and copy the IIF an entity acquired or maintains; obtain an accounting of disclosures that the entity made; request an amendment of the information an entity maintains and, if such amendment is not undertaken, request that the information be notated; and, retrieve a confidential communication of IIF collection.

- ***Limited Use/Acceptable Use*** – use and disclosure of IIF should be limited to the legal purpose set forth in an entity's Notice and then only to that which is minimally necessary to complete the legally permitted task. All other uses should be prohibited.

- ***Data Accuracy/Data Integrity*** – when possible, an entity relies first on the IIF it collects directly from the individual and it monitors access and modifications.

- ***Security Safeguards*** – an entity implements the appropriate management, operational, and technical controls to preserve the privacy, confidentiality, integrity and availability of IIF.

4. **Value can be gained by providing guidance on privacy at the due diligence or standard of care level.** Adopting privacy controls will serve to raise awareness and inform enterprise architects of their responsibilities and perhaps even cause privacy officers to be included sooner rather than later in the design decisions.

OBJECTIVES FOR THE FEA SECURITY AND PRIVACY PROFILE

The CIO Council envisions that the FEA Security and Privacy Profile will provide stakeholders with an understandable, consistent, repeatable, scalable, and measurable process for identifying security and privacy controls. This process will support stakeholders in identifying and implementing the level of protection necessary to mitigate or manage threats, risks, exposures, and vulnerabilities. To achieve this vision, the council has established four objectives for developing the FEA Security and Privacy Profile:

1. Ensure the same management rigor that is applied to each FEA reference model is equally applied to security and privacy.

2. Address security and privacy throughout the decision-making process.

3. Facilitate early identification and understanding of essential security factors and establish a set of security and privacy services and patterns that can be trusted and shared among the government community.

4. Ensure the approach integrates with National Institute of Standards and Technology (NIST) guidance thus fostering the integration of information assurance with enterprise life cycle management practices.

Objective 1: Ensure the same management rigor that is applied to each FEA reference model is equally applied to security and privacy.

The FEA is a business- and performance-based framework supporting cross-agency collaboration, transformation, and government-wide improvement. It provides OMB and Federal agencies with a new, consistent method for describing, analyzing, and improving the Federal Government and its ability to serve the private citizen. Until now, consistency in describing FEA-level security information decisions was lacking. One objective of the FEA Security and Privacy Profile is to address this shortfall, thereby facilitating understandability, consistency, repeatability, and scalability by using a clearly documented process that includes audit trails of key stakeholder decisions and desired/expected outcomes.

The FEA Security and Privacy Profile will benefit stakeholders by helping them to—

- Understand security and privacy-related context and conditions and relate them to the value-benefit of information sharing within the business line context (e.g., relevant factors)

- Recognize risk exposures of the environment, including internal and external influences

- Identify a set of controls that will influence the types of technologies and resources deployed, which ultimately affects cost

- Point to business and information exchange partners and the level of trust required to effectively perform business and exchange information in a protected manner

- Provide performance measures as a means for monitoring outcomes to ensure decisions align with stakeholder and business line partner expectations

- Define an ongoing process to supply additional information over time in making adjustments to initial decisions reflecting changes in needs, uses, and the emergence of new threats

Objective 2: Address security and privacy at the beginning of the decision-making process.

The FEA Security and Privacy Profile is meant to encourage Federal organizations to address security and privacy at the beginning of the business process/IT systems development effort when high-level requirements are being defined. Changes in the way Federal agencies are interacting with other agencies, the public, and their industry partners are driving them to implement and rely on new technologies and business processes. Integrated services and information sharing provide improvements that are needed to attain the goals of delivering services faster, better, and more cheaply. Without proper planning, they can frequently introduce risks and vulnerabilities that could jeopardize the data and processes that support an agency's services and, ultimately, its mission. Therefore, responsibility and decision-making discussions around security and privacy should occur at the earliest possible stage and at the highest levels of decision-making.

The key is to achieve a balance by maximizing the benefits, i.e., reducing risk, supporting key business strategies, and achieving return on investment (ROI), while optimizing the investments in security and privacy initiatives.

Objective 3: Facilitate early identification and understanding of essential security and privacy factors.

The FEA Security and Privacy Profile will assist agencies in defining four variables that support well-informed, risk-based decision-making.

1. **Initial Risk Exposure.** By analyzing information from the FEA reference models, stakeholders can develop an initial estimate of the risk exposure associated with any given business process[5] by examining security patterns based on threats-risks-security and privacy mechanisms and the development and operational cost of applying that mechanism. Alternatives should be defined based on the risk versus ease-of-use attributes of the alternatives. If the initial estimate is too high, business owners can save both time and money by looking for other options earlier in the process.

2. **Range of Controls.** The FEA Security and Privacy Profile will allow stakeholders to initiate discussions early in the process by addressing the range of controls that may be available to support security and privacy goals. The methodology helps business owners understand the nature, extent, and impact that controls have on LOB, business processes, or IT systems. Knowing the range of controls provides stakeholders the ability to determine alternative approaches in mitigating risk, with alternatives being fundamental to the decision-making process.

3. **Relevant Potential Costs.** The FEA Security and Privacy Profile will also provide information to derive potential costs associated with controls. As with risk exposure, these costs will be projected at the "rough order-of-magnitude" (ROM) level, rather than the precise determinations that will be developed when the system's physical design has begun. Identifying financial impacts early may help avoid costly redesign or unexpected costs later in the process.

4. **Options Analysis.** Finally, the FEA Security and Privacy Profile helps business owners in risk-based decision-making achieve security objectives by establishing a range of options. In the options analysis, business owners specify the level of service performance desired, view an initial set of security controls providing a level of residual risk, and determine if the associated cost is acceptable. The result is an ROM cost estimate that can be analyzed against a predetermined

5 A formal risk assessment should be conducted once the actual system design begins. See NIST Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems.

budget or cost feasibility plan. If the initial estimates are too high, business owners can reassess—or reduce—the types of controls needed to mitigate risk, thereby increasing residual risk yet reducing cost. Thus, within the options analysis, stakeholders can begin to prioritize mitigation strategies in determining the most effective balance of benefit, cost, and risk factors.

In addition, the FEA Security and Privacy Profile methodology paves the way for establishing trust among partners. By using a common approach and documenting decisions that result from an options analysis decision, business partners (government-to-government or government-to-business) will be able to better understand what decisions were made, why a given set of controls was adopted, and whether any changes should be made to protect a similar or interconnecting LOB.

Objective 4: Ensure the approach integrates with NIST guidance.

While FEA reference models are at the line of business (LOB) level, NIST guidance addresses the program and system levels. The proposed FEA Security and Privacy Profile will assist agencies in first identifying security and privacy needs for LOB and then in linking those needs to NIST guidance at the program and system levels in support of LOB. For example, a particular LOB may achieve its business objectives by using a variety of systems; however, it is the process that sets them apart. An agency would first use NIST SP 800-60 and FIPS 199 to determine what the impact of loss of systems would be for each specified LOB. However, it may be necessary to decompose LOB further to the sub-function and process level to achieve a level of detail necessary to engage the process or business owners and partners in determining specific elements of risk. This additional information will allow accountable officials to make informed risk based decisions to drive the selection of appropriate security and privacy controls, also leveraging NIST SP 800-30.

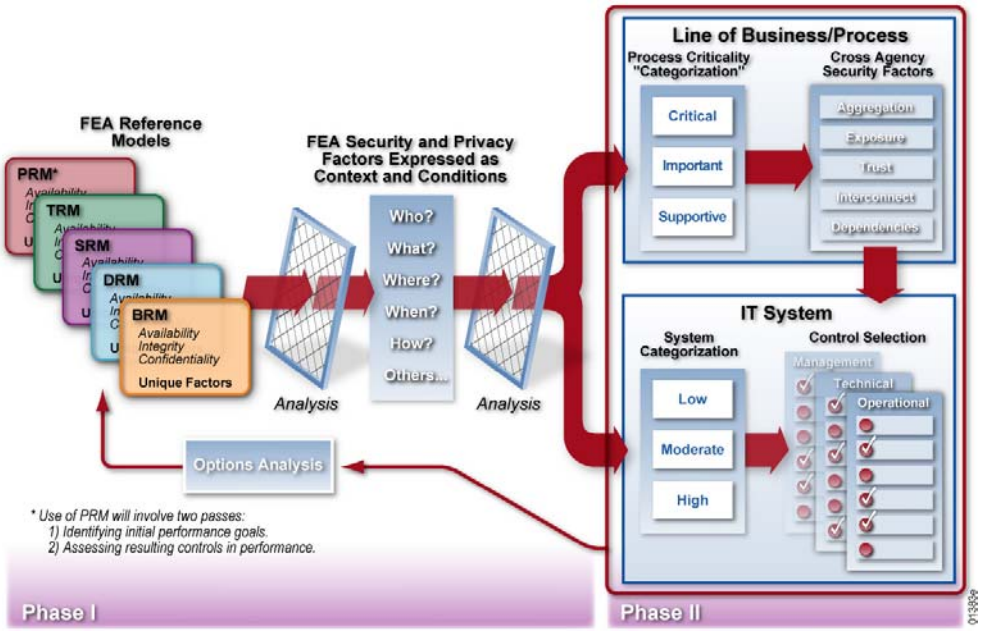
This objective does not signal a replacement of NIST by the FEA Security and Privacy Profile, but rather demonstrates a complementary integration that guides accountable decision makers in risk based decision-making. The shared security and privacy concerns can be documented as part of the baseline agreements in information and data sharing that cross traditional organizational boundaries. Stakeholders will benefit through their ability to make well-informed decisions, thus leading to highly accurate, effective IT capital planning and increased coordination between stakeholder counterparts (e.g., business managers, infrastructure operators). The resulting guidance ensures that IT security and privacy priorities are tied to business and mission needs and may support identification of a common, initial set of security and privacy controls for systems sharing the same categorization within a given LOB

2 Security and Privacy in the FEA Reference Models

OVERVIEW OF THE FEA SECURITY AND PRIVACY PROFILE

The purpose of the FEA is to ensure the provision of sound government investment in information technology. By integrating the FEA Security and Privacy Profile with the five models/components— Performance Reference Model (PRM), Business Reference Model (BRM), Service Component Reference Model (SRM), Technical Reference Model (TRM), and Data Reference Model (DRM)— businesses can develop and implement essential IT-related data, requirements, processes, standards, and controls to help achieve their business objectives.

Figure 3. FEA Security and Privacy Profile Overview



As depicted in Figure 3, the FEA Security and Privacy Profile provides a methodology for extracting relevant security and privacy information from each FEA reference model, proposes and identifies a set of appropriate security and privacy controls, and provides corresponding security factors on residual risk to the business owner.

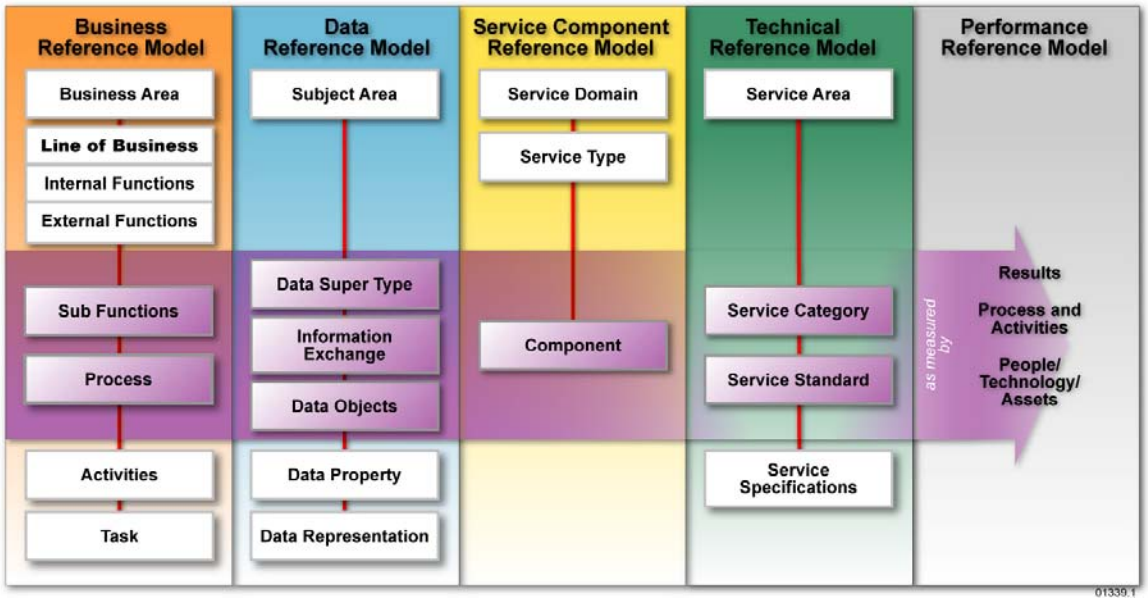
The methodology for the FEA Security and Privacy Profile begins with the business owner's careful analysis of each reference model to determine the nature, scope, and content of the services to be provided. Information and data are identified using common terms aligned with security objectives, such as confidentiality, integrity, and availability, as well as terms that specifically address each business process. This information can then be transformed into "context and condition" data through a series of relevant questions and answers that assist business owners in understanding the risk exposure of the processes they are designing. Whenever new services are established or significant changes are made to existing services, the impact to security should be assessed. This methodology can be used by the business owners and stakeholders who participate in the decision-making and option analysis processes.

Determining the feasibility of this approach is the main objective of Phase I of the FEA Security and Privacy Profile study. This section discusses how the methodology, security, and privacy information, otherwise referred to as "context and conditions," can be derived from each reference model. It also presents a high-level view of how the resulting information can help the user determine an appropriate set of security and privacy controls to provide options to the decision maker through the options analysis mechanism.

IDENTIFYING SECURITY AND PRIVACY INFORMATION

As Section 1 described, the FEA has an interrelated, mutually supportive structure composed of five reference models. Each reference model has several levels ranging from general (upper-most levels) to detailed/specific (lower levels) that describe the elements and information unique to the model, as depicted in Figure 4. Relevant information on security and privacy is provided at different levels within each reference model. The shaded arrow displayed across the five reference models in Figure 4 indicates the level within each model at which sufficient security and privacy information can be formulated.

Figure 4. Components of FEA's Reference Models Yield Security and Privacy Information



Relevant security and privacy information obtained from the respective level for each reference model is presented below, followed by a notional example depicted in Figure 5.

Business Reference Model (BRM)

The BRM provides information that relates business processes to an organization's mission. This information helps prioritize systems and guides decisions related to "how much" security is needed. Potentially, a minimum level of security is needed for business processes and/or IT systems less critical to the mission. The BRM provides very general information at its higher levels and identifies four business areas, including Service to Citizens, and 53 internal and external lines of business. However, as the model's subfunctions and processes become more refined, sufficient information can be extracted to begin providing security and privacy guidance.

Data Reference Model (DRM)

The DRM defines the types of data used in supporting business processes and associated systems. Laws and regulations require protection of some data super-types. The DRM can be augmented to provide guidance on data sensitivity that also contributes to understanding how much security is needed. It is necessary, however, to refine the data super-type until enough detail is available to identify laws and regulations that affect data sensitivity. The data model must address the protection of the security- and privacy-related data elements including the security and privacy policies, the security and privacy mechanisms used and their locations, the security and privacy roles and authorization information, and any vulnerabilities and breaches that have occurred. Data security and privacy assessments must define the critical information based on laws, regulations, and business needs.

Service Component Reference Model (SRM)

The SRM defines components that can be used to provide specific services required by the user. Because these services will support the mission, and potentially process sensitive data, the SRM can facilitate their use by identifying the security capabilities of available components. Further, the SRM can catalog components that are available to provide security services. Service component definitions are needed to provide sufficient information to address security and privacy context and conditions. A set of services for security and privacy components, perhaps as derived from a service oriented architecture implementation, will be the basis for controls used by horizontal and vertical business lines.

Technical Reference Model (TRM)

The TRM presents technologies that can be used in building systems. As with the SRM, the technologies will either have or require security capabilities or additional technologies to augment the systems depending on the business process and data supporting the mission. The TRM will also identify security technologies that can be used to meet security needs. Both the SRM and TRM guide decisions on "what" security is needed and "where" it should be deployed. Service standards are the level of detail at which security guidance can be provided.

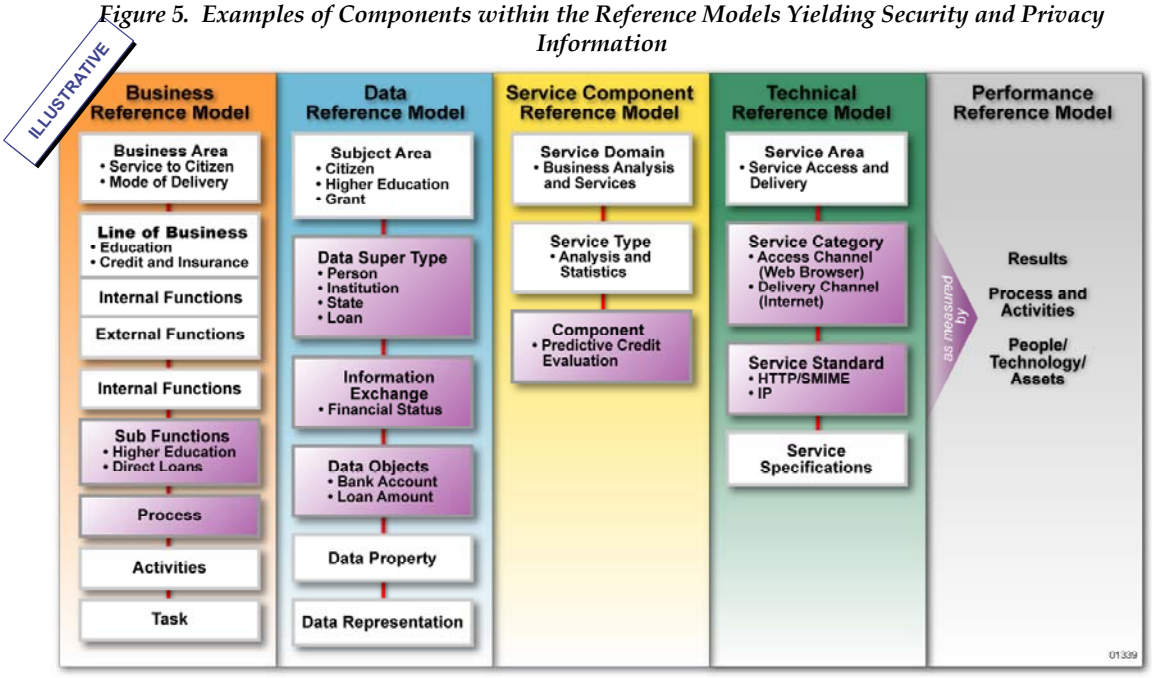
Performance Reference Model (PRM)

The PRM defines measures of success related to business outcomes. The security services in a business process/IT system should support these measures. Hence, measures will need to be developed for the security services that link them to successful business outcomes. Ultimately, information from all of these models builds toward the development and implementation of safe and effective business processes to serve citizens. Security and privacy attributes and assessment and improvement goals will be included as one of the critical elements in the performance model, along with the ability to recommend improvements based on emerging threats and protection technologies.

IDENTIFYING SECURITY AND PRIVACY INFORMATION—A NOTIONAL EXAMPLE

Figure 5 illustrates how security and privacy information can be derived from the FEA reference models. This graphic depicts a notional example based on promoting higher education by providing direct government loans to students who attend college. While not intended to reflect an actual government service, the example illustrates an activity that is consistent with information in the FEA reference models and identifies applicable security and privacy information associated with the activity.

Figure 5. Examples of Components within the Reference Models Yielding Security and Privacy Information



The narrative that outlines the notional example is contained in Table 1 - Example Setup. In this outline, different levels of each reference model are used to "mine" relevant context and condition information that are useful in determining the corresponding set of security and privacy controls.

TABLE 1. EXAMPLE SETUP

Business Reference Model
A service to citizens will be provided in the Education line of business dealing with Higher Education. This service will be provided via the Mode of Delivery business area through the Credit and Insurance LOB using Direct Loans. From this information, business owners can begin early in the process to identify the security and privacy factors affecting the objectives of the LOB. Examples include the motivations of adversaries that may attempt to disrupt this business activity or actions by some citizens who might try to fraudulently obtain loans for purposes other than pursuing higher education.

Data Reference Model
Certain data super-types and information exchanges can be hypothesized as necessary to support issuing direct loans. The loan applicant must be identified to perform credit checks and to collect loan payments; hence, personal identity information must be collected. Privacy concerns will require that confidentiality protection be applied to this data. Furthermore, privacy concerns require that only the minimum amount of personal information be collected.

Financial information and the name of the higher education institution to be attended will also be required. As financial information is sensitive and requires protection, each data type may have specific security guidance associated with it. Furthermore, aggregations of multiple data types may require additional protection beyond that required of individual types.

Unique factors that influence security and privacy will need to be addressed. For example, the Federal Education Rights and Privacy Act (FERPA) allows students to restrict access to the name of the particular college they attend. Therefore, systems supporting the loan process will have to provide mechanisms for applicants to control this information.

Service Component Reference Model
As part of the loan application process, the government will need to determine whether applicants are creditworthy. Because the government operates many loan programs, existing components might already perform predictive credit evaluation. If such components are available, the description of those components will have to include the security and privacy services they provide. Since financial data processed by the evaluation component is sensitive, service components used in loan processing need to provide appropriate protection for the data.

Technical Reference Model
Business may want to collect loan applications via particular access and delivery channels, such as a Web-based application delivered via the Internet. Selection of particular service standards from the TRM (such Internet-based delivery) may suggest additional security concerns that would not be present with other service standards.

Performance Reference Model
Finally, information from the models will suggest measures of effectiveness for the security controls. The business objective of a new loan program might be to increase the number of applicants for Federal higher education aid from particular citizen groups. To accomplish this, business managers may feel that the application system needs to be available 24/7. To achieve this level of availability, particular security controls would be included. This suggests that actual availability should be measured. Further, factors that contribute to availability, such as security controls, should be implemented. Once the system has been deployed, reliability and contributing information can be measured to ensure the application system agreed on meets its expectations in contributing to the overall business objective.

FEA CONTEXT AND CONDITIONS

Fundamental to the FEA Security and Privacy Profile is its capability to provide business owners and security practitioners with the tools for developing a straightforward set of questions that clearly define risk. NIST SP 800-60 and FIPS 199 provide business owners with initial considerations for security categorization and security controls based on LOB and information type. Using this as a starting point, the FEA Security and Privacy Profile helps a business owner develop a set of "20 questions" that can be used to support the "risk exposure" determination. This additional information will, in turn, assist them in fine tuning this initial set of controls based on specific business "context and conditions"

Context and condition questions, resulting from an organization's implementation of the FEA, will provide an understandable "state of the operating environment" that should be easily articulated by the business owner. Thus, it will be the business owners who initially identify and frame the context and conditions from each of the reference models deemed applicable to the environment under consideration. Validation of the initial set of context and conditions will be one objective of the participating stakeholders, such as the Privacy Advocate or Security Practitioner. Stakeholders can modify the set of questions by adding to the unique security factors set, thereby capturing an individualized representation of the business environment and system requirements. Stakeholders will be able to catalogue questions and responses to be later reviewed, validated, and measured by performance metrics. This approach provides a more objective means of determining the final set of controls. The responses are developed in such a way as to permit quantification of the corresponding level of risk associated with each question.

Figures 6 and 7 provide an illustrative set of questions from the BRM and DRM, respectively, along with scaled responses. Though both models address confidentiality, integrity, and availability, the questions in Figure 6 address the "availability" security objective, while Figure 7 addresses "confidentiality."

Figure 6. Illustrative Set of Questions from the BRM Addressing Availability

This Business Reference Model Example of the "20 Questions" and Responses Help Determine the Security Objective on Potential Impact Required by NIST 800-60 and FIPS 199.

FIPS 199 Security Objective	FEA Context and Conditions	Levels of Risk/Response: Low (limited impact)	Medium (serious impact)	High (catastrophic impact)
Availability: Core Factors	Source: BRM — What is the relationship of your process to the Mission?	*Supportive*	*Important*	*Critical*
Criticality / *Citizen Use/Availability* / *Threats to Outcome* / *Interconnections*	Source: BRM — What downtime is acceptable to sustain normal operations?	*Extended (Weeks)*	*Limited (Days)*	*Immediate (Hours)*
	Source: BRM — How likely is the service to be exploited (what is the level of attractiveness to disrupting productivity or embarrassing the gov't)?	*Low*	*Moderate*	*High*
	How many other services does this rely on? How many other services rely on this?	*No Critical Systems*	*Few Critical Systems*	*Many Critical Systems*
Availability: Unique Factors / *Unique Legislative Requirements*	To what extent does legislation impose unique security requirements?	Low	Moderate	High

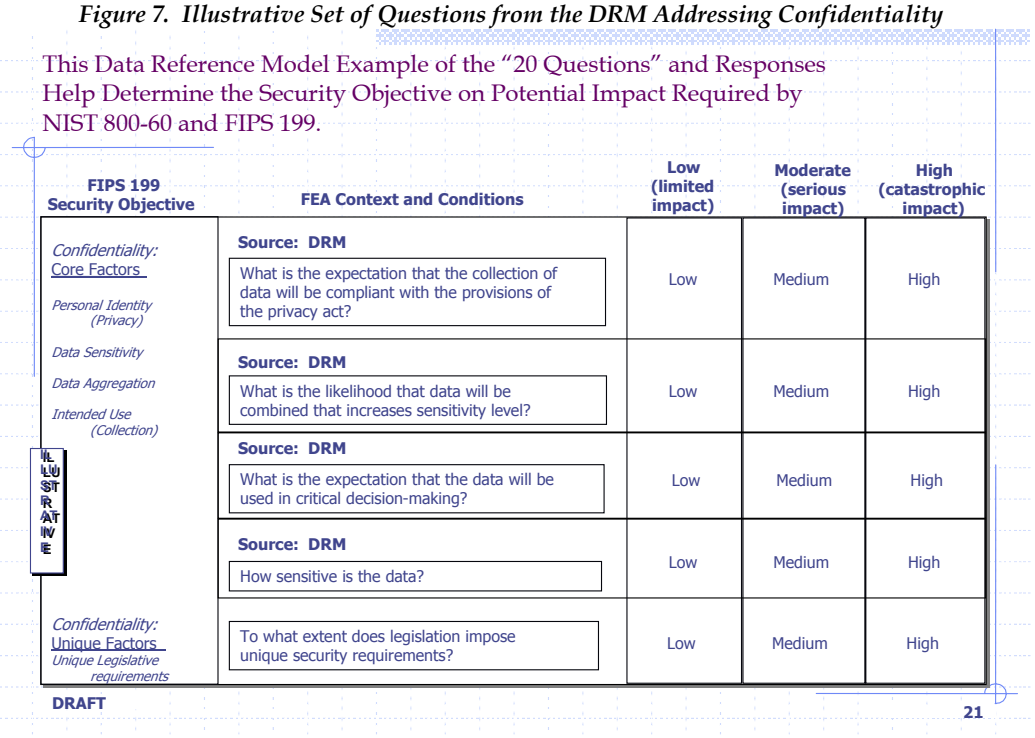
ILLUSTRATIVE

DRAFT

20

The next step in the process is to bind the FEA Security and Privacy Profile with NIST categorization and security controls framework. Before doing this, however, it is necessary to describe the alignment between the FEA Security and Privacy Profile and NIST guidance.

Figure 7. Illustrative Set of Questions from the DRM Addressing Confidentiality



SYNCHRONIZATION BETWEEN FEA SECURITY AND PRIVACY PROFILE AND NIST

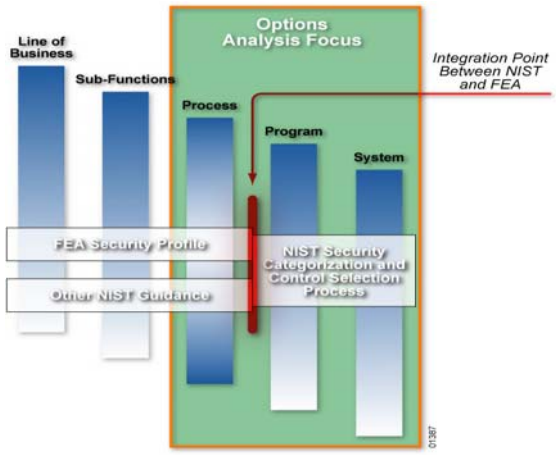
Another important concept is how the FEA Security and Privacy Profile interfaces with and complements existing and emerging NIST guidance. To be successful, the profile must link to the body of NIST guidance currently being implemented by most government agencies. As mandated by Congress, NIST is preparing a series of new regulations and guidance documents that will fundamentally change the way the Government protects critical data, processes, and resources. This emerging documentation, which includes FIPS 199 and NIST SPs 800-37, 800-53/53a, and 800-60,[6] will establish the framework in which agencies identify, apply, and verify their implementation of security controls. Accordingly, the FEA Security and Privacy Profile must synchronize with this evolving body of work so that well-defined, consistent, repeatable, scalable, and measurable guidance is provided to Federal stakeholders and their partners.

To describe the synchronization process effectively, the different activity levels within each process must first be defined (see Figure 8). The FEA categorizes high-level activity as lines of business, subfunctions, and processes. The process layer is a key focal point of the FEA Security and Privacy Profile because it describes and bounds a common set of services and behaviors that multiple agencies need to understand to share services or data. Processes also rely on multiple systems to produce expected results and required products or services. NIST guidance has been focused primarily at the program and system levels. Current and future guidance is aimed at assisting system owners and agency-level security program developers with the framework necessary to apply and validate security controls that are commensurate with the level of incurred risk. The purpose of the synchronization between the FEA Security and Privacy Profile and NIST guidance is to address the different perspectives between the FEA process and the NIST program/system layers without introducing unproductive and confusing overlaps.

6 Refer to NIST SP 800-53a, "Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems"; NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"; NIST SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Objectives and Risk, Levels."

Figure 8 depicts a shaded area called the Options Analysis Focus, which indicates the options analysis concept is at the process-to-system levels, i.e., useful information required to make effective trade-offs is available primarily at the process, program, and system levels. Seamlessly linking the FEA Security and Privacy Profile to NIST guidance is crucial to facilitate trade-off analysis that takes place in the options analysis space.

Figure 8. Integration Point Between NIST and the FEA



THE UTILITY OF OPTIONS ANALYSIS—A HOME CONSTRUCTION ANALOGY

During the early stages of life-cycle development for a new or reengineered business process, limited information is available beyond a vision of the desired service outcome and a conceptual design. It is at this point, however, that security stakeholders must begin evaluating risk so that the formulation of options around the conceptual design approach can be more meaningful. Options analysis, therefore, becomes relevant to decision-makers as a forum to help establish their option selection processes. This process is quite similar to the scenario that most people encounter in building a house. A home construction analogy may serve to shed light on the utility of this options analysis concept. At each interval of the analogy (in the shaded box), links to key elements in the process as described in Phase I will be reviewed.

Analogy Setup

A person owns a lot of a particular size and requests that a contractor provide a cost estimate for the construction of a five-bedroom home. Without any other design specifications, the contractor can only respond "a lot." The person then asks, "How much for a four-bedroom home?" Again, the contractor can only respond "not as much."

This home building scenario depicts the limitations of the types of decisions that can be made based on available information at the early stage in the decision-making process. So too, at the early stages in the FEA Security and Privacy Profile, only levels of commitment (e.g., "a lot" or "not as much") can be known about cost and risk. It is not until the corresponding security categorization is performed and an initial set of controls are identified that more insightful information can be made available. As the decision-making process continues, additional information will better inform decision makers and influence outcomes, as seen in the next example.

Analogy Refinement

On the basis of additional discussions held between the contractor and the prospective buyer, the contractor can gain a better understanding of the buyer's basic (core) and desired (unique) housing needs. As a result of the new information, the contractor can provide a choice of several models that will meet the buyer's needs. The prospective buyer then asks, "How much for each model?" The contractor's response is "$250K to $325K for model A, $300K to $400K for model B, and $375K to $500K for model C." The price range reflects premium features (e.g. different elevations, sunroom) or upgrades (e.g., carpets, appliances) that are available for each model.

Cost is a key decision driver for building a home, and cost will influence the types of features and upgrades selected by a prospective buyer. Now that more information is available, more meaningful decisions can be made. By using options analysis, the buyer can begin to weigh cost versus options when selecting the model.

Similarly, a business owner requires more information to begin determining whether the benefit of the control is commensurate with cost and risk. It is not until corresponding security controls (e.g., firewall, firewall and intrusion detection; or, firewall, intrusion detection, and load balancing and backup) are

identified that ROM costing information is available and the business owner can begin to perform an options analysis.

Analogy Conclusion
Originally, the contractor had only limited information on the different types of models available to build that would meet the buyer's needs. After selecting a model, the buyer now needs to decide on the desired options to fit within a certain budget (e.g., hardwood floors and carpet upgrades). Once the options are selected, the contractor can provide a final cost.

For the business owner, options analysis can be used to perform trade-offs between the selection of security options that determine residual risk and the cost of those options. As the decision-making process continues along the life-cycle development path, more relevant and accurate information is available at each succeeding stage. In the end, the utility of the options analysis approach is to give decision makers the ability to, for example, weigh the benefit of having 99-percent system availability against the costs associated with security controls to enable that performance level. If the cost is too high, two options are available: either an optional control can be evaluated to meet that particular service requirement, or the service requirement can be modified. The objective is to evaluate options using the best information available until a balance is achieved among benefit, cost, and risk.

APPLYING THE FEA SECURITY AND PRIVACY PROFILE—A SCENARIO

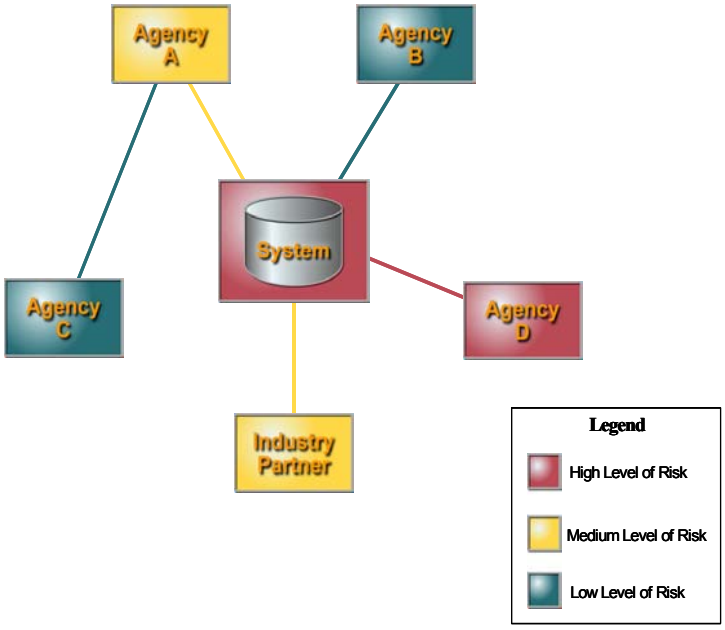
In this section, a notional initiative, "eConsolidate" (eCon), is used to illustrate the potential use of the Security and Privacy Profile. The eCon program requires the development of a system to automate a particular LOB/subfunction business process as well as the consolidation of LOB/subfunction data into a centralized location with interconnectivity between agencies and/or industry partners participating in the initiative. While providing a more efficient use of government resources, the major part of the design will incorporate security and privacy concerns and implementation of the eCon program. Each organization's security posture will have varying levels of risk and individual security policies, processes, and controls. Therefore, the eCon program will need to accommodate different levels of risk associated with participating organizations to provide an effective decision-making and system development process.

Business owners and security practitioners will thus be faced with the following security issues:

- How will the eCon program address associated security risks when more than one organization consolidates data?
- What security and privacy controls may be added or may be subtracted from the set identified in 800-53 to account for specific context and conditions obtained from the reference models?
- How can we use relevant data from the reference models to help decision makers understand the risk exposure inherent in the prescribed set of controls?
- How can context and condition data be useful in making the business case to support adjusting the prescribed set of security and privacy controls to increase or reduce risk commensurate with the business owner's risk tolerance ?
- How will the eCon program capture the initial risk exposure and budget for potential costs to mitigate exposures?

Figure 9 represents a possible representation of how the risk determination of a new service (e.g., eCon) would be determined without the application of the FEA Security and Privacy Profile. In this scenario, the new service would be focused at the system level with the risk determination being aligned with the risk classification of the highest trading partner, in this case Agency D. In this configuration several large issues arise. First, obtaining agreement from each of the trading partners that the new service will have a risk level of High will be difficult. Agency D will not be willing to share its resources unless the risk level and control structure of the new service achieve the standard established by Agency D. At the same time, Agencies A, B, C, and the Industry Partner may not be willing to participate in the new service if the cost outweighs the benefits. Second, partners not willing to share information with the new service may get the information from a previously established relationship with another agency, such as between Agency A and Agency C, as illustrated in Figure 9. Third, participants may focus too much on the technology that implements the system and may not adequately capture other critical aspects of the service.

Figure 9. Before Appling the FEA Security and Privacy Profile



In the next section, concepts discussed in this document, such as context and conditions identified from each reference model, stakeholder validation, and options analysis, are leveraged to demonstrate a potential application of the FEA Security and Privacy Profile. In addition, information in Figure 9 will be modified to reflect the impact that the FEA Security and Privacy Profile will have on the decision-making process.

APPLICATION OF THE FEA SECURITY AND PRIVACY PROFILE

In keeping with the FEA Security and Privacy Profile methodology, security and privacy stakeholders from each participating organization would meet to consider security and privacy factors from each reference model and develop a straightforward set of questions that can clearly yield an effective picture of residual risk. The following table illustrates potential security-related questions that can be gleaned from the reference models.

TABLE 2. APPLICATION QUESTIONS

Potential Business Reference Model Questions	➢ What is the relationship of your process to the mission? ➢ What downtime is acceptable to sustain normal operations? ➢ How likely is the service to be exploited? ➢ How many other services does this rely on? ➢ To what extent does legislation impose unique security requirements?
Potential Data Reference Model Questions	➢ How sensitive is the data? ➢ What is the expectation that the collection of this data will be compliant with the provisions of the Privacy Act? ➢ What is the likelihood that the data will be combined in a way that increases sensitivity level? ➢ What is the expectation that the data will be used in critical decision-making? ➢ To what extent does legislation impose unique security requirements?
Potential Technical Reference Model Questions	➢ What is the level of trust in the delivery channel? ➢ What is the expected/perceived level of vulnerabilities in the technology being used? ➢ What is the expected/perceived level of maturity in the technology being used? ➢ What is the degree of complexity for integrating/maintaining the current system within the environment?
Potential Service Reference Model Questions	➢ What is the compatibility of the service to the line of business? ➢ Are there unique features of the host infrastructure that impact system integration or operations?

This exercise will result in a set of standard security context and conditions potentially agreed upon by all participants. The context and conditions should be reviewed, validated, and in many cases, measured using performance metrics. The resulting information may provide early support for the options analysis that will bring into view the level of security and privacy commitment to be incurred by the owners of eCon (in the earlier home construction analogy, this is the "a lot" or "not as much" stage). More specifics on cost and risk will become available when stakeholders refine decision-making data in the manner to be proposed in the FEA Security and Privacy Profile to Phase II.[7]

The next step is to apply the security context and conditions to determine the FIPS 199 system security categorization. After categorization, NIST SP 800-53 can be used to identify an initial set of security controls that will provide the security stakeholders with a foundation for performing trade-off analysis. This analysis will enable them to define the final set of security controls that might be needed by the business processes and supporting systems. The options analysis will consider benefit, cost, and risk in an effort to determine the best system approach.

By following this process, the eCon program owners would have established the beginnings of a common trust model where they know, with some level of certainty, what application controls have been implemented to facilitate the business process. A gap/fit analysis should be performed to determine additional controls (i.e. compensating controls) that may be imposed to facilitate the implementation of a data sharing activities. In addition, owners could refer to their respective agencies and, in using the same methodology, be able to determine if their infrastructure or other interconnected systems would support the level of security required. Figure 10 illustrates how the application of the FEA Security and Privacy Profile would potentially affect each trading partner.

Several key points to note about Figure 10:

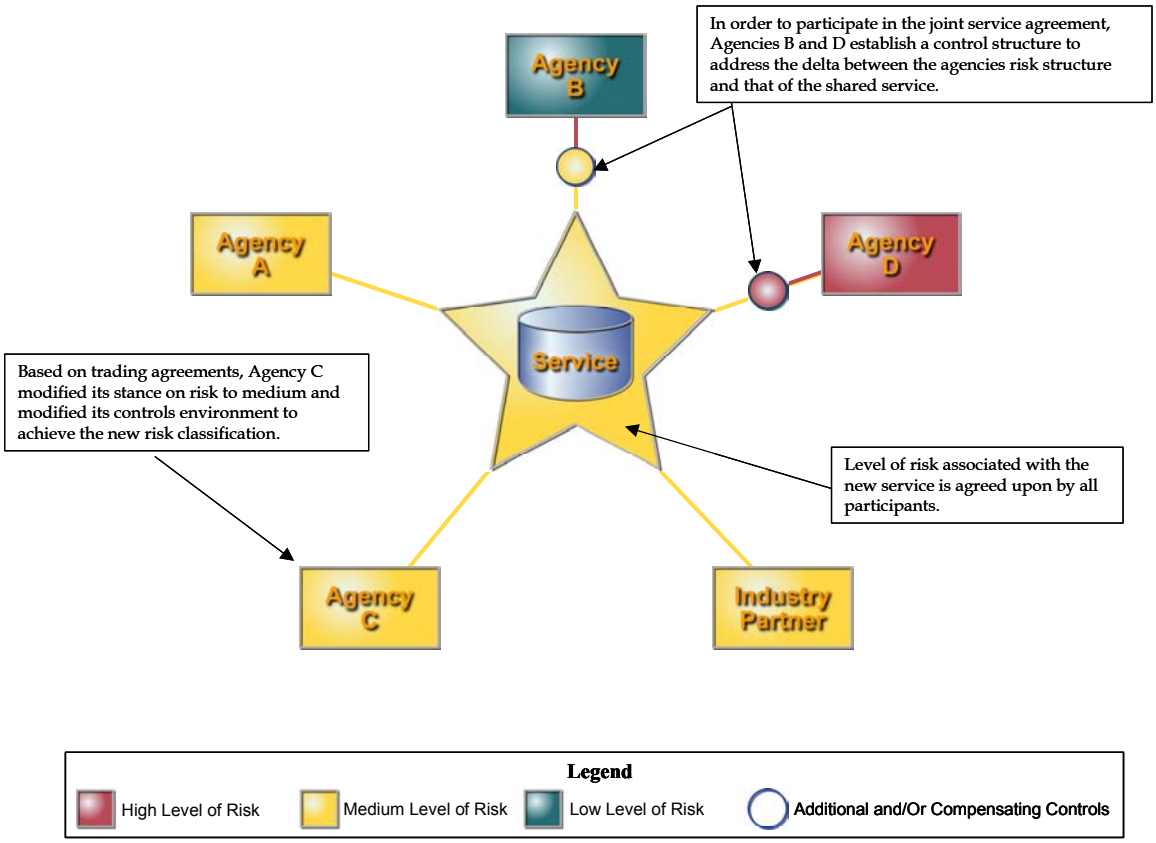
[7] The methodology approach will be examined in Phase II of the FEA Security and Privacy Profile study.

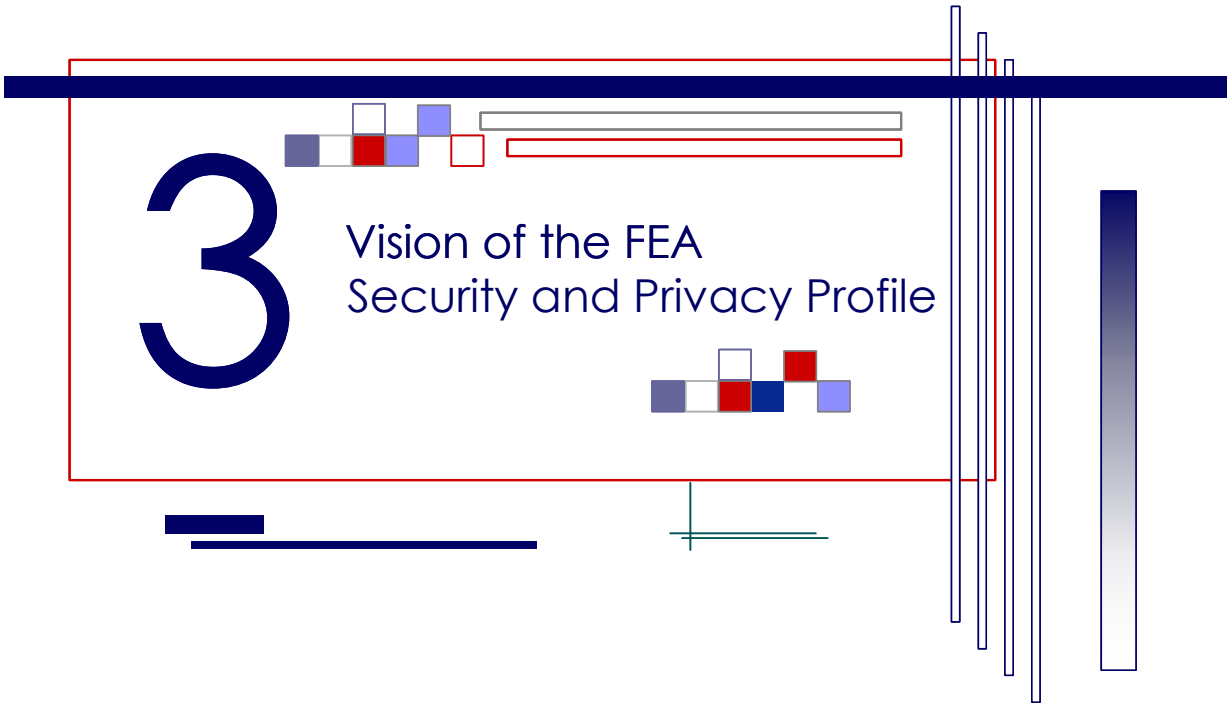
1. Focus of this activity is elevated from the system level to the cross-agency shared services level. In addition, based on validated context and conditions, an agreed upon shared services risk level is reached that is other then system/agency high. This concept is illustrated by the Star Symbol.

2. Leveraging the concept of Option Analysis and applicable guidance, the beginnings of a common trust model is established enabling the identification of a common or agreed upon set of controls. Thus, agencies are able to perform a gap fit analysis to implement additional compensating controls and establish data sharing activities. This is illustrated by representations of Agencies B, C, and D.

3. Partners are more inclined to agree to and operate within the established network and share information directly with the service instead of each other. This is illustrated by representation of Agency C.

Figure 10. Application of the FEA Security and Privacy Profile





PHASE II CONSIDERATIONS

The concepts presented in this paper respond to Phase I of the FEA Security And Privacy Profile study. They represent a methodology aimed at meeting the CIO Council's objective of providing an integrated approach for incorporating security and privacy into the FEA. As outlined in this section, important considerations must be addressed in Phase II of this study.

- **Phase I Comments:** Because Phase I concepts will result in the receipt of comments from a variety of stakeholders, it is important to ensure that anticipated users of the FEA Security and Privacy Profile have the opportunity to contribute knowledge and experience that will assist in shaping the direction of the profile. Thus, comments received will be carefully considered for future revisions of the FEA Security and Privacy Profile.

- **Privacy Considerations:** Privacy, in conjunction with security, must be considered early in the decision-making process. Additional analysis is needed to identify controls that directly or indirectly support privacy requirements. A use-case scenarios will be employed to illustrate the interaction between security and privacy.

- **Synchronization of NIST and the FEA Viewpoints:** Current NIST's focus on security is at the system level, such as in the performance of risk management activities, identification and implementation of controls, and system categorization. The FEA reference models focus on the line of business level. Thus, a success factor of the FEA Security and Privacy Profile will be to establish a firm linkage between NIST guidance and the FEA. This process will require more extensive development in Phase II.

- **Selection of Controls:** Phase I introduced terms such as "options analysis," "common trust model," and "security factors," which are critical elements of the FEA Security and Privacy Profile. Each of these is intended to assist decision makers in selecting an appropriate set of controls for implementing sufficient security and privacy within the business process and IT system. Phase II will refine these concepts and ensure they are fully integrated with NIST guidance on security controls. A set of specific information assurance activities that are integrated with Enterprise

Architecture (EA) and related enterprise life cycle elements such as portfolio management and capital investment planning will be developed. These activities will include a close evaluation of the set of emerging security and privacy technologies against a set of security-privacy needs-threats scenarios and security and privacy patterns that can be used to integrate EA practices into information assurance.

- **The FEA Security and Privacy Profile's Association with other Industry Projects:** A significant amount of work is being done by industry to address security, privacy, standards based and service oriented architectures, web services, etc. that need to be further reviewed. The objective of this analysis will be to determine integration points, clearly state differentiations, and identify the boundaries between current industry projects and the FEA Security and Privacy Profile.

- **Build Detailed Implementation Scenarios:** Based on the concepts presented in Phase I and some real working examples in the government and industry, various scenarios will be developed to assist agencies in using the FEA Security and Privacy Profile to plan and implement appropriate security and privacy programs.

APPENDIX A - REFERENCES

National Institute of Standards and Technology SP 800-53, "Recommended Security Controls for Federal Information Systems," Initial Public Draft, October 2003.

National Institute of Standards and Technology SP 800-53a, "Techniques and Procedures for Verifying the Effectiveness of Security Controls in Federal Information Systems," Draft—Not Released To the Public.

National Institute of Standards and Technology SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," June 2003.

National Institute of Standards and Technology SP 800-60, "Guide for Mapping Types of Information and Information Systems to Security Objectives and Risk Levels," Draft—Not Released To the Public.

National Institute of Standards and Technology, FIPS PUB199, "Standards for Security Categorization of Federal Information and Information Systems," May 2003

The Federal Enterprise Architecture Program Office, *The Business Reference Model*, June 2003.

The Federal Enterprise Architecture Program Office, *The Services Component Reference Model*, June 2003.

The Federal Enterprise Architecture Program Office, *The Technical Reference Model*, August 2003.

The Federal Enterprise Architecture Program Office, *The Performance Reference Model*, September 2003.

APPENDIX B - ACRONYMS

BRM	Business Reference Model
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DRM	Data Reference Model
ECon	eConsolidate
e-Gov	e-Government
FEA	Federal Enterprise Architecture
FERPA	Federal Education Rights and Privacy Act
FIPS	Federal Information Processing Standards
IAC	Industry Advisory Council
IT	Information Technology
LOB	Line of Business
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PRM	Performance Reference Model
ROI	Return on Investment
ROM	Rough Order of Magnitude
SDLC	System Development Life Cycle
SP	Special Publication
SRM	Service Component Reference Model
TRM	Technical Reference Model

APPENDIX C - GLOSSARY

Architecture
A set of design artifacts or descriptive representations that are relevant for describing an object such that it can be produced to requirements (quality) and be maintained over the period of its useful life (change).

Capital Planning and Investment Control (CPIC) Process
A process to structure budget formulation and execution and to ensure that investments consistently support the strategic goals of an agency.

Enterprise
An organization supporting a defined business scope and mission. An enterprise comprises interdependent resources (people, organizations, and technology) that should coordinate its functions and share information in support of a common mission (or set of related missions).

Enterprise Architecture
1. A strategic information asset base that defines the business, the information necessary to operate the business, the technologies necessary to support the business operations, and the transitional processes necessary for implementing new technologies in response to the changing business needs; a representation or blueprint. 2. The set of primitive, descriptive artifacts that constitute the knowledge infrastructure of the enterprise.

Enterprise Life Cycle
The integration of management, business, and engineering life-cycle processes that span the enterprise to align IT with the business.

Methodology
A documented approach for performing activities in a coherent, consistent, accountable, and repeatable manner.

Model
Representations of information, activities, relationships, and constraints.

Principles
A component of the strategic direction. In terms of the Federal Enterprise Architecture, principles are statements that provide strategic direction to support the Federal vision, guide design decisions, serve as a tie breaker in settling disputes, and provide a basis for dispersed, but integrated, decision-making.

Options Analysis
Outlines the active and continual process of balancing security factors in making risk-based decisions on "how" and "to what extent" security and privacy must be implemented.

Repository
An information system used to store and access architectural information, relationships among the information elements, and work products.

Security and Privacy Profile
Provides an understandable, consistent, repeatable, scalable, and measurable methodology that uses relevant FEA Reference Model information (i.e., context and conditions) to support business owners in accurately determining security categorization and establishing an appropriate set of security controls in accordance with NIST guidance.

System
A collection of components organized to accomplish a specific function or set of functions.

Systems Development Life Cycle (SDLC)
Guidance, policies, and procedures for developing systems throughout their life cycle, including requirements, design, implementation, testing, deployment, operations, and maintenance.

APPENDIX D - CIO COUNCIL TERMS OF REFERENCE

Development of an Information Security Architecture Profile for the Federal Government

OBJECTIVE: The Federal Government is moving forward aggressively to leverage architecture as a primary basis for making decisions on IT investments as well as to use architecture to guide the development of implementation strategies for information technology capabilities. The Federal Enterprise Architecture (FEA) serves as the overarching architectural guide for the Federal government and consists of five models: Business Reference Model; Performance Reference Model, Systems Components Reference Model; Data Reference Model; and Technical Reference Model. There is a need for an additional view of the FEA that addresses and highlight elements of the FEA that address information security. The target Information Security Architecture Profile would overlay the existing reference models and provide managers and systems architects with guidelines regarding the design and deployment of appropriate measures to ensure protection of information resources. The objective of the task described in these terms of reference is to develop an Information Security Architecture Profile that will become a part of the FEA.

APPROACH: The CIO Council Architecture and Infrastructure Committee (AIC) will work with industry to leverage work that has been done within the Federal agencies and industry in the area of security architectures. Successful security architectures will be evaluated for potential applicability across the Federal government. A suitable set of architectural principles and guidelines will be assembled from the existing FEA reference models, government agencies, as well as private companies to quickly produce an initial version of an Information Security Architecture Profile that will be available for use by Federal agencies and used to guide future updates to the FEA reference models. The Information Security Architecture Profile will also include a brief outline of the roles of various organizations in ensuring protection of Federal information resources.

PARTICIPATION: The CIO Council Architecture and Infrastructure Committee will oversee the development of the Information Security Architecture Profile. The Governance Subcommittee of the AIC will manage the work. The Governance Subcommittee will identify a full time leads for the effort as well as other appropriate participants from a range of Federal agencies, and in particular the National Institute of Standards and Technology and the Department of Homeland Security. The AIC Co-Chairs and the CIO Council Security Focal Point will provide executive sponsorship and oversight for the effort. The CIO Council will engage with recognized industry leaders in the field of information security architecture to produce the Security Profile. In particular, the Booz Allen Hamilton Corporation and the Mitre Corporation will be asked to participate in a rapid Phase I of the effort to be delivered by August 2003. Phase I will leverage recognized experts in the area of government information security architecture as well as proven examples of government information security architectures and profiles. In Phase II, the Industry Advisory Council (IAC) Security Committee, as well as other industry organizations as appropriate, will be asked to participate by providing experts in the area of information security architecture to help review, refine and expand the Phase I product. As the draft product is developed, it will be shared with an increasingly broader set of government and industry participants to solicit additional inputs and comments.

TIMEFRAME: The Architecture and Infrastructure Committee and industry team will develop a draft (Phase II) product for review by the full AIC by October 2003.

LEADERSHIP: Two selected members of the Governance Subcommittee will lead the Information Security Architecture Profile effort.

RESOURCES: The sponsoring government and industry organizations will provide the necessary resources to complete this effort.