Logistics Management Institute

A Practical Approach to Integrating Information Security into Federal Enterprise Architectures

IR229T1

October 2002

John DiDuro
Robert Crosslin, Ph.D.
Debra Dennie
Paul Jung
Christopher Louden
David Shepherd

LMI®

A Practical Approach to Integrating Information Security into Federal Enterprise Architectures

IR229T1

October 2002

John DiDuro
Robert Crosslin, Ph.D.
Debra Dennie
Paul Jung
Christopher Louden
David Shepherd

LOGISTICS MANAGEMENT INSTITUTE
2000 CORPORATE RIDGE
MCLEAN, VIRGINIA 22102-7805

Executive Summary

Security is a critically important consideration in government today. The security of business or mission-critical information has many facets. These range from the contents of personnel policies and hiring practices, to internal controls of functions such as approval processes, data access and update rights, and firewalls and encryption.

Simply implementing a variety of security mechanisms to protect information—the approach taken by most organizations—is not enough. Rather, security must be fully integrated into the organization's enterprise architecture (EA). In other words, rather than creating a unique instance of a security architecture, it is preferable to have security integrated into the current EA model. In effect, as opposed to addressing just information security or cyber security, it is more appropriate to take a holistic view of the requirement for providing enterprise security. This involves looking at all characteristics of business entities—people, processes, and facilities—that interact with, or have an impact on, information.

LMI has developed a methodology for integrating security into EA frameworks. That methodology—called the Secure Enterprise Architecture Methodology (SEAM)—establishes security as an inherent part of the EA process. This is critically important for effective enterprise security because security is cross-cutting, affecting every facet of the enterprise.

Government managers must decide where to apply scarce resources. SEAM helps them meet that challenge by integrating security measures into the EA. It reveals how existing resources are being applied to security concerns, supports setting priorities on security-related requirements, and clarifies shortcomings in security coverage, for existing *and* target architectures. Understanding the gaps between requirements and functionality is critical in efficiently allocating resources: SEAM assists in providing that understanding and allows for a complete accounting of security within the enterprise. Furthermore, because the methodology is based on business asset analyses, it integrates with all of the predominant EA frameworks in use today.

Security is only as strong as its weakest link; complete coverage of security requirements is essential. The artifacts provided by SEAM allow managers to measure the completeness of enterprise protection measures. These benefits make our methodology a practical tool to facilitate strategic security planning by federal managers.

Contents

Chapter 1
Introduction

Security is a critically important consideration in government today. Managers are driven by a variety of security requirements from various laws, statutes, regulations, and policies.[1] In addition, they must respond to increased threat of terrorism, increased reliance on information technology (IT), and issues of public trust. Security threats are cross-cutting, affecting IT planning, capital investment, systems design, operations, and IT governance. Failure to address security threats can interfere with a government organization's ability to carry out its mission.

Volumes have been written on the *what*, *how*, and *why* of security; but what do we really mean by "security"? Every enterprise has assets it uses to accomplish its goals, from people and information to computers and software. We describe those objects within the enterprise that require safeguarding. Therefore, when we talk about security, we are really talking about the *protection* of those *business assets.* At a high level, enterprise security is the process of appropriately protecting enterprise assets from various risks and threats. Ultimately, no enterprise can effectively meet its goals without protecting its assets.

Simply implementing a variety of security mechanisms—the approach taken by most organizations—is not enough. LMI believes that, to be effective, security must be fully integrated into the organization's enterprise architecture (EA).

Why incorporate security into the enterprise architecture? An EA is an invaluable tool for IT planning in the federal government; it is required by law and helps agency managers understand the inherent complexities of the enterprise.[2] Managers can gain that understanding because, as defined by the Federal Chief Information Officers (CIO) Council, an EA specifies the agency's mission, the information necessary to perform the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. An EA includes a baseline architecture, a target architecture, and a sequencing plan.[3] Thus, by integrating security into its EA,

[1] The Computer Security Act and the Privacy Act are two major governance documents describing basic security requirements for federal agencies.

[2] The Clinger-Cohen Act requires agency chief information officers (CIOs) to establish and maintain an EA. Additional mandates for EAs include the Government Paperwork Elimination Act, Freedom of Information Act, Government Performance Results Act of 1993, Office of Management and Budget (OMB) Circulars A-11 and A-130, and guidance from the General Accounting Office and the Federal CIO Council.

[3] Federal CIO Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0, February 2001, p. 5, and *Federal Enterprise Architecture Framework (FEAF)*, Version 1.1, September 1999, p. 2.

an organization can ensure proper alignment of security initiatives with enterprise drivers and can readily identify and address risks and threats.

Several frameworks exist for establishing and maintaining an enterprise architecture. Federal agencies may use any framework as long as it complies with the Federal Enterprise Architecture Framework (FEAF).[4] However, the predominant EA frameworks do not clearly address security considerations. To fill that gap, LMI developed an approach, called the Secure Enterprise Architecture Methodology (SEAM), that federal agencies can use to integrate security into their EAs, regardless of the framework. SEAM is framework independent because it is based on the identification and description of business assets, which are common to all frameworks.

This report presents SEAM and discusses the merits of our approach. The reader is expected to have a working knowledge of EA and related methodologies and frameworks.[5] The report is organized as follows:

- Chapter 2 defines several concepts necessary for understanding our methodology for integrating security into EA analyses.
- Chapter 3 describes SEAM.
- Chapter 4 describes the merits of applying SEAM.

The appendixes contain an annotated bibliography and a list of abbreviations used in the report.

This report does not provide a "magic bullet" for enterprise security, nor does it describe how to select or implement specific security measures in a particular environment. In addition, this report does not address operational security issues such as intrusion detection and incident response. Effective operational security practices must be founded in a solid understanding of the enterprise security posture provided by the framework articulated in this report.

[4] Several EA frameworks exist. See National Institute of Standards and Technology, *Information Management Directions: The Integration Challenge*, NIST Special Publication 500-167, September 1998; Federal CIO Council, *Federal Enterprise Architecture Framework (FEAF)*, Version 1.1, September 1999; Department of the Treasury, *Treasury Enterprise Architecture Framework (TEAF)*, Version 1, July 2000; Department of Defense, *C4ISR Framework*; and Logistics Management Institute, *LMI Enterprise Architecture Practice (LEAP)*, 2000.

[5] The expected audience of this report includes CIOs, critical infrastructure assurance officers, chief security officers, enterprise architects, and federal managers.

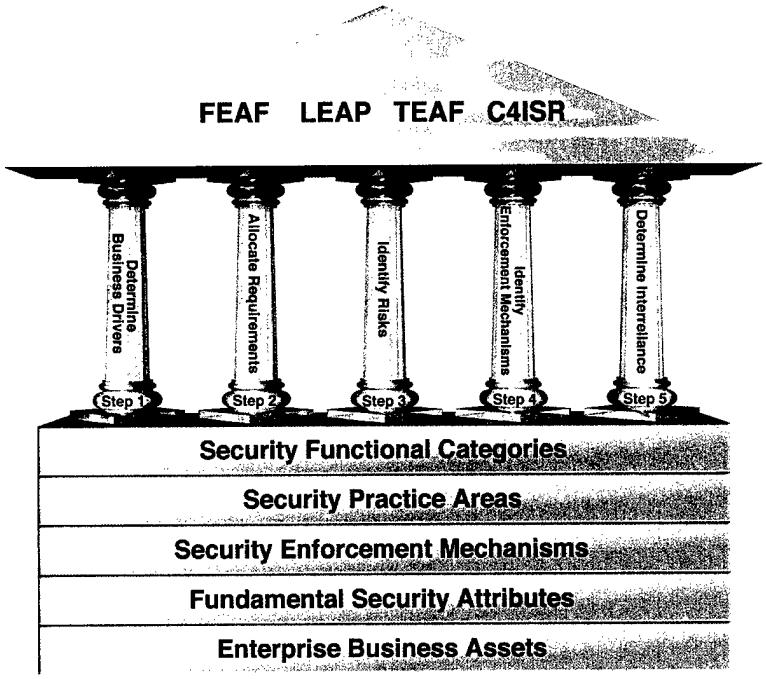
Chapter 2
Enterprise Security Concepts

This chapter describes five key concepts that form the foundation of our methodology for integrating security into enterprise planning:

- Enterprise business assets (EBAs)
- Fundamental security attributes (FSAs)
- Security enforcement mechanisms (SEMs)
- Security practice areas (SPAs)
- Security functional categories (SFCs).

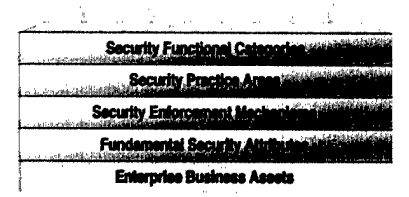
These concepts are critical to understanding SEAM and are detailed in the following sections. One can better understand the importance of these concepts by visualizing SEAM as a structure. As shown in Figure 2-1, the foundation represents the five concepts, or elements, and the five pillars represent the five steps required to incorporate security into any EA framework (represented by the roof of the structure).

Figure 2-1. Depiction of the Secure Enterprise Architecture Methodology



The remainder of this chapter describes SEAM's foundation.

ENTERPRISE BUSINESS ASSETS

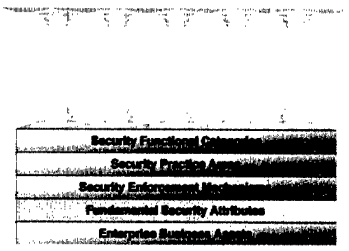


The primary goal of information security in the enterprise is to protect its core elements, or "things,"—such as people, data, information, buildings, money—critical to the enterprise. In the context of enterprise architecture, these components are referred to as enterprise business assets and are the starting point for building enterprise architecture data models and repositories.

Every EA framework we reviewed has some notion of business assets.[1] Personnel data and accounting records are two examples. We use this concept to tie our security analysis into the frameworks.

Once the analysis uncovers the business assets, some agencies will augment their framework by classifying or categorizing their business assets by sensitivity or criticality. This exercise provides value to the agency, but is not a requirement for SEAM.

FUNDAMENTAL SECURITY ATTRIBUTES



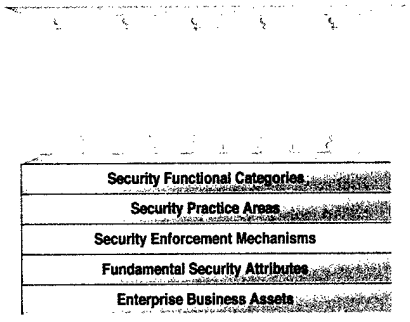
We identified seven fundamental security attributes to provide consistent language for describing security requirements, functionality, or principles. Any security function or requirement can be expressed using these attributes, which are defined in Table 2-1.

[1] None of the EA publications we reviewed uses the term "enterprise business assets," but all employ some concept of these entities. Some frameworks refer to business objects or components, but our terminology encompasses those.

Table 2-1. Fundamental Security Attributes

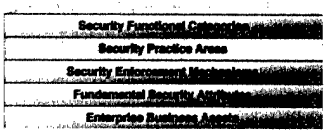
Attribute	Definition
Accountability	Binding of an activity to an actor, person, or object. Audit logs or sign-in sheets provide accountability by recording an action and the individual performing it. *Nonrepudiation* is a related concept; it is a very strong form of accountability, one in which a subject cannot reasonably deny having a role in a transaction.
Authentication	Act of deciding on a subject identity; in other words, the binding of an identity to a subject. When a software package accepts a user ID and password, it is authenticating the user. When a guard views an ID badge, he or she is authenticating the employee.
Authorization	Determination of an authenticated subject's ability to act. When a software package permits an authenticated user to perform a transaction, it is authorizing that user to perform that action. Likewise, when the guard allows an employee to enter a secure area he or she is authorizing admittance. *Access control* is a related concept; it is the effect of authorization decisions. Unauthorized access occurs when authorization mechanisms are bypassed.
Availability	Degree to which an information resource is functional when needed—in other words, a measure of reliability. Hot sites, backup tapes, and fail-over procedures all improve availability. *Survivability* is an analogous concept; it involves the effect of various events on availability. *Continuity of operations* (COOP) is a related concept; it contemplates the ability of an organization to continue its operations during and after disasters, which is heavily influenced by the availability of various systems.
Confidentiality	Prevention of the disclosure of certain information to certain subjects. Sealed envelopes, locked file cabinets, and encrypted e-mail all provide some measure of confidentiality. *Privacy* is a related concept; it results from keeping personal information confidential.
Integrity	Prevention of the unintended modification of data. Mechanisms that prevent or detect accidental or unauthorized changes to data provide integrity. *Authenticity* is a related concept; it refers to the ability of third parties to verify integrity.
Safety	Prevention of injury to people, whether customers, employees, or others. Metal detectors, seatbelts, hardhats, and smoke detectors all contribute to safety.

SECURITY ENFORCEMENT MECHANISMS



We refer to any aspect of the enterprise that has security-related functionality as an enforcement mechanism, termed "SEM." Firewalls, safes, guards, and encryption software are all examples of SEMs. Each provides some kind of protection for elements of the enterprise. Enforcement mechanisms are specific, identifiable elements—not concepts or goals. Any aspect of the enterprise that provides accountability, authentication, authorization, availability, confidentiality, integrity, or safety for some part of the enterprise is an enforcement mechanism. Identification and description of an enterprise's SEMs are necessary to fully understand the enterprise's security posture.

SECURITY PRACTICE AREAS



We identified nine practice areas, or SPAs, to serve as categories for every security discipline and skill set. The SPAs, defined in Table 2-2, also provide a comprehensive list of perspectives for risk analyses and threat identification. Every risk, threat, and mitigation strategy will fall under one of these practice areas.

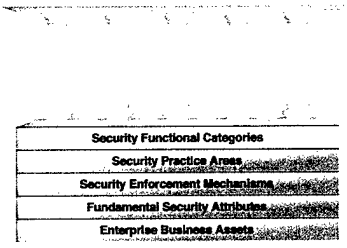
Table 2-2. Security Practice Areas

Practice area	Disciplines
Policy management	Identification of security requirements from relevant sources, including statutes, regulations, department guidelines, and expectations of public trust Establishment of necessary security policies Incorporation of enterprise security requirements into corporate policies
Process and procedure management	Establishment of procedures to support security policies Incorporation of necessary security procedures into business processes and corporate administrative procedures
Personnel security	Security-related activities with new employees such as background checks, nondisclosure agreements, and new employee orientation Training activities, including awareness, disaster recovery training, and incident response training Employee monitoring activities, including responding to policy violations Discharge activities, including debriefs, account suspensions, and notifications to staff of employee or contractor departure
Software security	System boundary definition as required by OMB Circular A-130 and defined in NIST SP 800-18 Software configuration management, which is needed to track software development activities Security features of various software applications, including internal applications, e-mail, groupware, and other commercial off-the-shelf applications Maintenance and updates, including the policies and procedures for handling new versions of software Virus management Authentication credential management for software access
Data security	Data encryption, including key management Database security, including authentication credential management and role definitions File sharing and file server configuration

Table 2-3. Security Practice Areas (Continued)

Practice area	Disciplines
Host security	Hardware configuration management, which is needed to track infrastructure Operating system hardening, or optimizing the security of the operating system for general-purpose computers Authentication credential management for host access
Physical security	Practices related to the security of physical items and corporate assets, including employees, inventory, and physical files Practices related to the employment of physical devices for security, such as locks, guards, and safes
Network security	Wide area network security, including Internet, virtual private networks, value-added networks, leased lines, and any remote access such as dial-up capability Local area network security, including network connectivity to all corporate systems Network border security measures, including firewalls, network address translation devices, proxies, and router access control lists
Mission assurance	Critical asset identification and protection measures Contingency planning practices, including COOP preparedness Disaster recovery planning, including backup practices and hot, warm, and cold sites Graceful degradation during disasters, heavy loads, or attacks, including practices for partial operating capabilities Risk identification, assessment, mitigation, and management

SECURITY FUNCTIONAL CATEGORIES



Security enforcement mechanisms fall into broader categories of functionality that we call security functional categories (SFCs). These categories provide for a grouping of like enforcement mechanisms and provide perspectives that aid in identifying existing or needed functionality. These categories are not mutually exclusive; it is possible for a particular enforcement mechanism to provide functionality from multiple categories. We identified five SFCs; Table 2-3 describes them.

Table 2-4. Security Functional Categories

Functional category	Description
Planning	Mechanisms that provide proactive coverage of enterprise-wide standard operating procedures, normally found as documentation. Continuity of operations, concept of operations, disaster recovery procedures, incident response handling, configuration management, and security plans are examples of planning mechanisms. *Preparedness* is a related concept; it results directly from planning.
Prevention	Mechanisms that protect the security attributes of enterprise business assets by actively impeding or preventing activities that would compromise those objects. Guards, firewalls and other perimeter defenses, safes, and locked doors are all examples of prevention mechanisms.
Detection	Mechanisms that identify or detect activities that may compromise enterprise business assets. Intrusion detection systems, smoke detectors, security cameras, and motion detectors are all examples of detection mechanisms. The detection enforcement mechanisms are monitors of activity, whether environmental controls or system logging.
Diligence	Mechanisms that involve proactive measures to continue planning mechanisms and to improve the overall security posture of the enterprise. Ongoing vulnerability assessments, continual employee training, operating system patching procedures, monitoring of hacker activities, threat classification, and reviews of vender security notices are examples of diligence mechanisms.
Response	Mechanisms employed after an enterprise business asset has been compromised in some way. Sprinkler systems, Federal Computer Incident Response Center engagement, disaster recovery procedures, and forensics procedures are examples of response mechanisms.

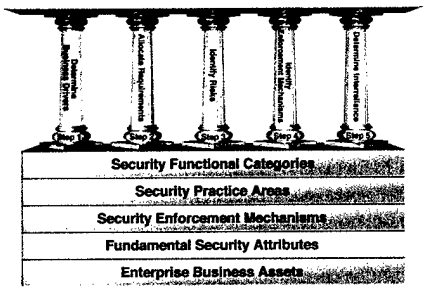
Chapter 3
Integrating Security into Enterprise Architectures

In this chapter, we describe how we use SEAM's security concepts to integrate security into enterprise architectures. We start by describing SEAM's specific steps and then discuss the application of SEAM to IT planning and risk management within the context of the EA framework.

DESCRIPTION OF THE METHODOLOGY

SEAM comprises five steps, which we describe in the following subsections. These steps, once integrated into the agency EA framework, provide for a complete accounting of security within the enterprise. The level of detail should be consistent with the level of detail in the EA, and information generated should be included in the EA repository.

Step 1: Determine Business Drivers

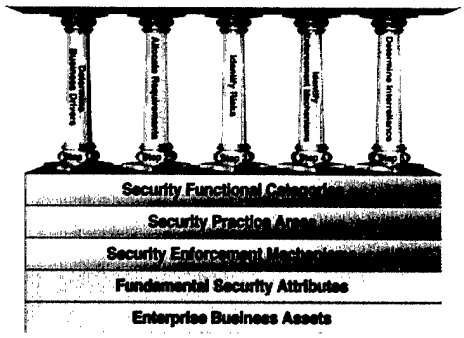


All EA frameworks call for the identification of business drivers. These drivers represent the high-level goals and requirements of the organization, and every facet of the enterprise should be aligned with them. Security is no exception to this rule. Security drivers for government organizations are derived from law, statute, or policies. Other business drivers may also have implied security requirements, such as ensuring the integrity or confidentiality of data the organization is required to disseminate.

The business area of financial management provides a good example. Each agency must comply with various laws, regulations, and policies about safeguarding business assets. In terms of SEAM, we describe this business driver as mandating that federal business owners be responsible for providing confidentiality and integrity of critical assets such as payroll and other sensitive personnel-related information. This protection requirement extends beyond internal agency IT processing of the assets; it includes dissemination to authorized outsiders such as the Internal Revenue Service (IRS), Social Security Administration (SSA), authorized financial institutions, and so on. In addition, these business drivers, while emanating from the top layers of the EA, will affect all lower layers through the business assets that support the financial management function within the agency.

The business drivers that are security related must be identified and clearly articulated. To ensure consistency, the drivers need to be succinctly described using the fundamental security attributes.

Step 2: Allocate Requirements to Enterprise Business Assets

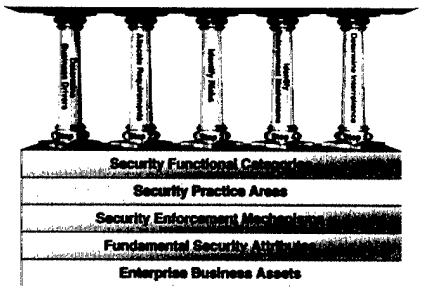


Business assets are the individually identifiable elements of the enterprise. These assets inherit the security requirements determined in the first step. For example, if one of the business security drivers is to maintain the confidentiality of accounting data, then each EBA involved in accounting must be reviewed to determine its particular security requirements. Essentially, the requirements identified in the first step are allocated out to the constituent elements of the enterprise. This step results in a list of enterprise assets that need to be protected and the specific type of protection that is required, stated succinctly using the security attributes.

The descriptions of the EBAs can be general or quite specific—either is "correct." For instance, financial management could be viewed as an overall concept or described as a combination of various accounting, payroll, and budget applications. It also could be described in even more detail. For example, the payroll asset could be described as series, grade step, and other specific information about employees or, in general, as the "applications" that generate the payroll.

The type of protection required for the asset is based on the requirements derived from the business drivers. For instance, the business assets involved in payroll inherit the confidentiality and integrity requirements derived from the financial management business drivers. To put it another way, because confidentiality and integrity are requirements for financial management, they are also requirements for all facets of financial management. So, to continue our example, all payroll assets, including the policy, procedures, and business processes involving payroll information, have confidentiality and integrity security requirements that must be addressed.

Step 3: Identify Risks



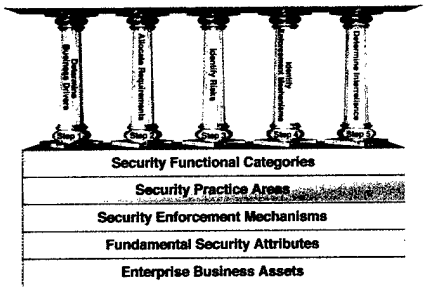
The third step is to identify and categorize the risks to the enterprise business assets needing protection. To continue with our financial management example, an agency may allow employees to use the agency network to access their earnings and leave data, including data about accruals and expenditures in benefit plans such as child care and medical. In addition, the agency may allow employees to access their earnings and

leave data from off-site. To ensure that its payroll and other financial management assets are protected, the agency should step through each of the SPAs (policy management; process and procedure management; personnel, software, data, host, physical, network security; and mission assurance) to identify any security issues.

Security practice areas aid in risk analysis by providing a comprehensive list of perspectives for determining each EBA's risk profile. The risks identified will vary with the different SPAs and perspectives. For example, a review from the perspective of personnel security might reveal a risk of funds embezzlement, while a review from the physical security perspective might reveal a threat to confidentiality resulting from a burglar stealing employee files.

This step is not intended to replace existing risk analysis techniques or efforts. Rather, this step integrates the identified risk, for each EBA, into the EA and provides consistent perspectives (via the SPAs) to categorize the security requirement.

Step 4: Identify Security Enforcement Mechanisms

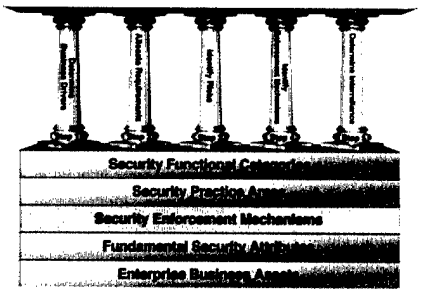


The purpose of this step is to identify and catalog the SEMs used to mitigate the risks determined in step 3. The security functional categories aid in this analysis by providing perspectives for identifying enforcement mechanisms in the enterprise. The specific security functionality should be succinctly stated using the fundamental security attributes, including the enterprise business assets that are being protected.

Ultimately, the SEMs are the components that enforce the overall security posture for the enterprise. Cataloging their functionality provides a comprehensive list of security features for the enterprise and allows for comparison of functionality with requirements (determined in steps 2 and 3).

For example, the payroll business asset in financial management is usually protected by multiple mechanisms in the *prevention* category. Locks on file cabinets containing hard-copy personnel records, specific policies and procedures for access to hard-copy records, backup tapes, firewall rules that do not allow access to payroll data, internal controls over access to operations and maintenance of the payroll application, and automated and manual audits of each payroll run are examples of prevention mechanisms. Mechanisms in the *diligence* category, such as reconciliation procedures and audits, are also often used. Just as there may be multiple risks to payroll business assets, there will be multiple enforcement mechanisms to secure those payroll assets.

Step 5: Determine Interreliance of Security Enforcement Mechanisms



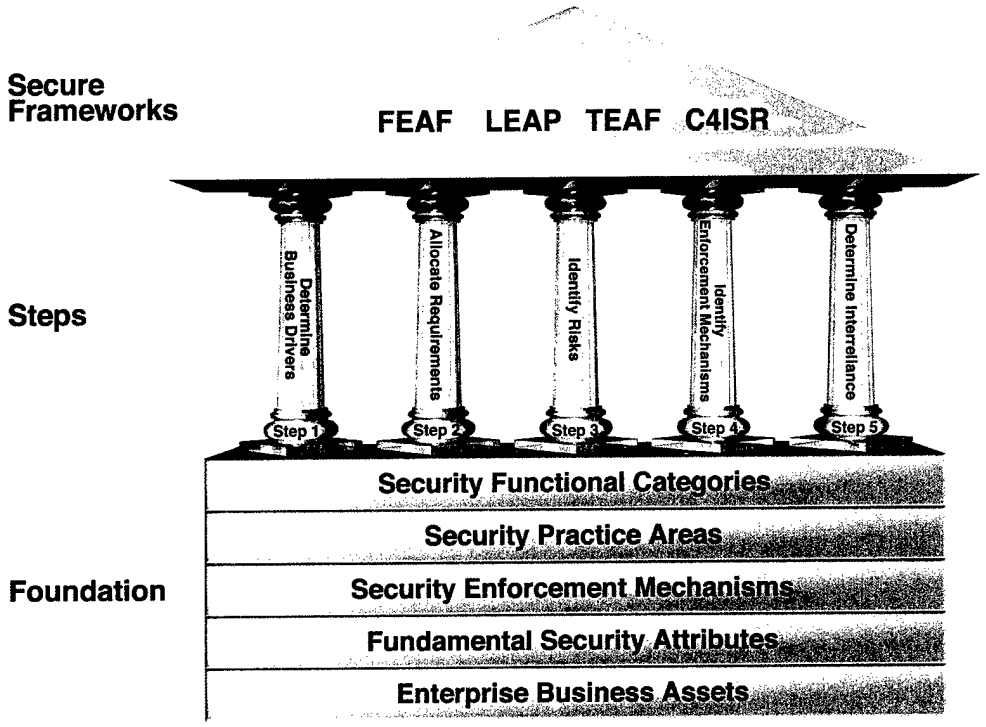
A particular business asset is rarely protected by a single enforcement mechanism. Similarly, SEMs rarely act independently. Understanding how various enforcement mechanisms rely on each other is critically important to understanding how security is enforced in the overall enterprise. It is commonplace for the compromise of a single mechanism to render all other SEMs useless. Therefore, the final step in our methodology is to identify and catalog the interrelationships of enforcement mechanisms.

Security professionals always strive for security measures that act like layers of an onion, where breaking through a single measure only reveals another. Unfortunately, in practice, security measures are more like links in a chain; the weakest link determines the overall strength of enterprise security. This step provides discipline to highlighting an agency's weakest link. For instance, the accounting software is protected by a firewall and a complex array of policies and procedures that prevent unauthorized access to agency funds. A user gains access to this software application via an ID and password. If the password is compromised by the end user (by someone writing the password on the side of a computer monitor, for example), all other protection mechanisms, no matter how comprehensive or complex, are defeated.

APPLICATION OF SEAM TO ENTERPRISE PLANNING

By applying SEAM, an organization augments its EA to account for security (Figure 3-1). The existing enterprise is documented as the current architecture, the baseline for information technology planning. As the needs of the organization change, the enterprise develops new target architectures to meet them. Through the use of SEAM, the organization is guaranteed that all of the security gaps are covered in the target architectures. It also reveals security shortfalls in the EA, highlights critical enforcement mechanisms, and ensures security alignment with agency business drivers. Simply stated, SEAM is a systemic, complete integration of security into EA frameworks.

Figure 3-1. SEAM Analogy Supporting Secure Frameworks



In practice, the EA is used as an integral part of IT planning. Generally, the existing enterprise is documented as the current architecture, which is used as the baseline for IT planning. As the needs of the organization change, new target architectures must be developed to meet those needs. Comparison of the current and the target architectures is called the gap analysis, which identifies work that has to be done to migrate to the target architecture.

Our methodology ensures that security is considered in the IT planning process. By using SEAM, an organization can ensure that the current architecture properly reflects the security posture of the baseline. Specifically, our methodology results in the identification and cataloging of security drivers, requirements, and functionality. Furthermore, it ensures that their relationships to the specific elements of the enterprise are determined and documented.

The findings in the documentation of the current architecture will drive some of the design of the target architecture. Our methodology elevates the visibility of several aspects of the architecture that will influence the process:

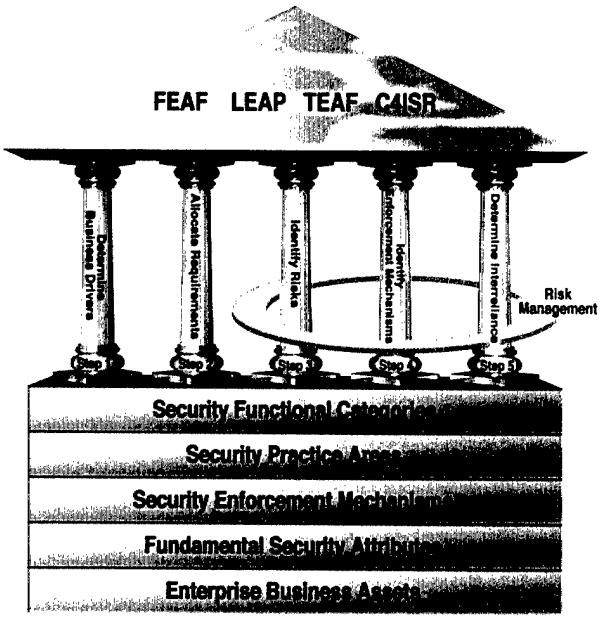
- *Reveals security shortfalls.* Comparison of enforcement mechanism functionality to business asset requirements will quickly reveal any gaps in security and the specific nature of the gap as described by the security principles. For example, there may be no mechanism to enforce the integrity of financial transaction data. This should drive the selection of SEMs in the target architecture to ensure proper coverage of the requirements.

- *Highlights critical enforcement mechanisms.* Analyses of the interreliance of SEMs may show excessive reliance on a small number of mechanisms. For example, it is possible that compromising an employee's password renders every other protection mechanism useless for many of the enterprise assets. If that is the case, potential improvements in the mechanisms protecting employee passwords should be carefully considered when designing the target architecture.

- *Ensures security aligns with business drivers.* Comparison of enforcement mechanism functionality to the security aspects of the business drivers may reveal improper alignment. One may find that resources are misallocated to security initiatives that properly align with the enterprise goals, while other core requirements are not met. Proper alignment of resources to business drivers should be considered in the design of the target architecture.

Once the target architecture is identified, the five SEAM steps should be applied to that architecture. The drivers, requirements, and functionality, as well as their relationship to the elements of the architecture, should be identified and cataloged. The same analysis prescribed above for the current architecture can then be used to determine whether the target architecture adequately meets the enterprise requirements.

RISK MANAGEMENT IN THE EA

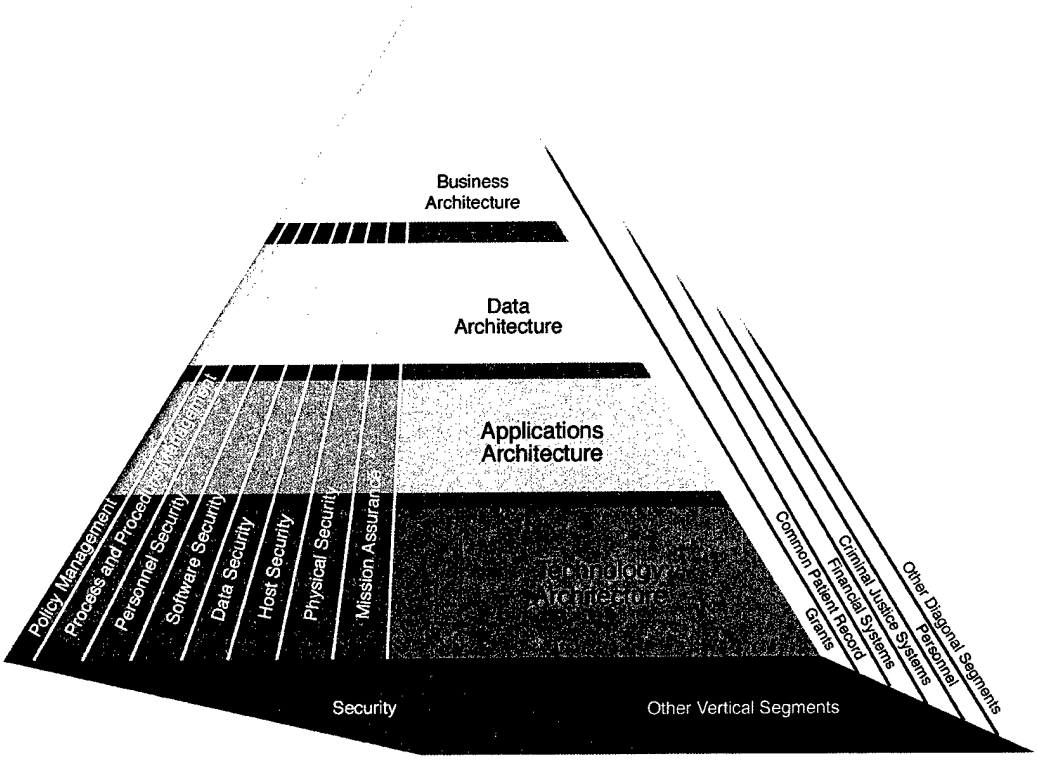


Risk management is an important aspect of security, as noted in the Computer Security Act of 1987 for IT systems handling sensitive information. The last three steps of SEAM ensure that agency risk management is integrated with the EA. Step 3 explicitly integrates risk identification into the EA. Further, through use of the different practice area perspectives, this step also ensures a comprehensive view of risks. Steps 4 and 5 integrate mitigation strategies into the EA and allow comparison between risks and requirements. Therefore, SEAM is consistent with federal statutes regarding risk management and appropriate for meeting the security needs of particular agencies.

SECURITY AS A FEAF VERTICAL SEGMENT

To depict how SEAM relates to every facet of an enterprise, Figure 3-2 shows the practice areas as a "vertical segment" of a framework (as defined by the CIO Council) using the Federal Enterprise Architecture Framework (FEAF). As shown in the figure, the security segment permeates all architectural layers and diagonal segments of the enterprise. The integration of security into architectures as a FEAF vertical segment is an ongoing effort. As elements within the architecture or diagonal segments change, the security analysis, as described in SEAM, must reflect those changes.

Figure 3-2. Security As a FEAF Vertical Segment



In summary, SEAM is intended to augment the normal EA process and integrates with existing frameworks. Documentation and understanding of the current and target architectures will include the security-related aspects of the enterprises. The gap analysis will also be enhanced to include security considerations. The IT planning process will therefore account for security issues. This approach ensures that security is an integral part of existing critical management practices, rather than an afterthought or sideline effort.

Chapter 4
Merits of the Secure Enterprise Architecture Methodology

Our methodology for integrating security into enterprise architectures has several benefits. Key among SEAM's benefits is that it enables an organization to answer the following questions:

- How complete is the organization's security coverage?
- Are security resources allocated properly?

SEAM also has two other important benefits:

- It fits into any enterprise architecture framework.
- It supports reuse.

This chapter discusses those benefits.

Completeness of Security Coverage

Within federal agencies, views of completeness differ depending on roles. For instance, Critical Infrastructure Assurance Officers and CIOs are interested in knowing and describing the posture of their agency with respect to security and the likelihood and source of gaps in security coverage. On the other hand, business owners are interested in knowing that their critical business assets are appropriately protected by the agency's security posture. Information gathered using SEAM allows for easy comparison of security requirements to existing security functionality, thereby giving a description of completeness to the security posture of any agency as it pertains to a particular role.

In practice, the completeness of a security posture must be determined through enforcement mechanism design and testing, accompanied by reviews and analyses of gaps in practice areas and functional categories:

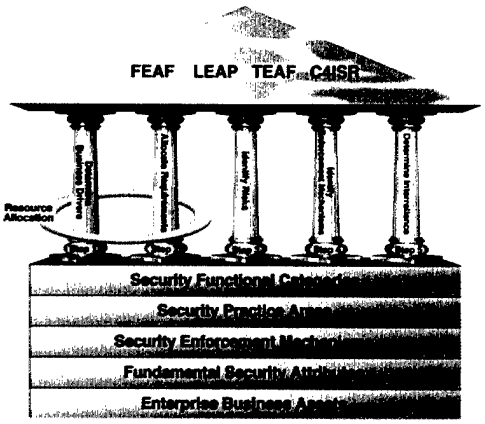
- *SEM design and testing.* Individual enforcement mechanisms must help to ensure the required level of security for each security attribute of every business asset subjected to that mechanism.
- *SPA reviews and gap analyses.* Practice area reviews and corresponding security gap analyses must address security linkages required in the enterprise architecture to support the interreliance of the SEMs. Insurance of

inheritance of security attributes of assets throughout all levels of the architecture should be part of the review of security linkages. Any security gaps should be addressed as part of the IT planning process in moving from the current architecture to the target architecture.

- *SFC reviews and gap analyses.* Functional category reviews of agency enforcement mechanisms helps to ensure that the approach to security is well-rounded and complete. The combination of SPA and SFC reviews brings a comprehensive perspective to describing and analyzing security in the EA.

All three sets of activities are required for achieving desired enterprise security results. Some security practitioners might be tempted to focus on SEM design and testing, which might accidentally result in incomplete (and therefore ineffective) security at the enterprise level. But that is not sufficient; SPA and SFC reviews and gap analyses are also required in order to describe the completeness of an agency's security posture.

ALLOCATION OF SECURITY RESOURCES



SEAM provides a linkage between security requirements and business drivers, helping to ensure alignment between business needs and security initiatives. Those business assets with higher priorities have corresponding security initiatives for risk mitigation that receive higher priorities. Therefore, the organization's managers must determine the relative priority of security initiatives and ensure that security resource allocation is consistent with enterprise priorities. As with other responsibilities of the enterprise, this is how it should be: executive direction, driven by business needs, specifies what is necessary, and the lower layers of the enterprise respond with how the requirements will be met. This is in contrast to a bottom-up methodology that places primary security responsibility at the technology or data layers of the enterprise.

The use of SEAM, especially the steps to identify risks and determine the interreliance of mechanisms to mitigate risks, enables an enterprise to highlight the relative importance of security mechanisms and groups of mechanisms. Measures with a greater breadth (mitigate more risks for more assets) could be characterized as higher in relative importance than measures of greater depth (attain a greater degree of security throughout the architectural levels), or vice versa. This type of characterization would typically be included in an assessment of the agency's current EA.

FIT WITH ENTERPRISE ARCHITECTURE FRAMEWORKS

SEAM is framework independent. The methodology's security attributes, practice areas, functional categories, and enforcement mechanisms are linked through business assets that must be protected, and everything related to enterprise security can be described in the context of SEAM's security attributes. Since all frameworks for enterprise architectures employ the concept of business assets as a key component, our methodology applies to, and integrates with, all EA frameworks, including FEAF.

The methodology is also flexible in terms of level of detail. All of the analyses relate back to the enterprise business assets, which can be generalized to whatever level of detail is appropriate. If the enterprise architecture defines business assets down to the individual application or server level, then the security aspects brought out by this methodology will also be at that level of detail. Enterprise business assets can also be defined in a general way, which allows for a less detailed analysis of the security posture.

REUSE OF ARTIFACTS, CONCEPTS, AND ANALYSIS

SEAM supports considerable reuse of artifacts, concepts, and analysis for EA efforts across the federal government. We can demonstrate SEAM's reusability using the financial management business area as an example:

- A federal agency can address the security of its financial management business area by
  - ➤ determining the financial management business drivers,
  - ➤ identifying the financial management enterprise business assets to be protected and their required security attributes,
  - ➤ identifying the risks to those assets,
  - ➤ identifying the appropriate or typical enforcement mechanisms and security functional categories for financial management, and
  - ➤ determining the interreliance of financial management security enforcement mechanisms across the enterprise.
- The agency can then make the information available to any federal agency with financial management in its enterprise architecture.

As this example shows, the results of applying SEAM to one organization often can be applied to other organizations.

CONCLUSION

Government managers must decide where to apply scarce resources. SEAM helps them meet that challenge by integrating security measures into the EA. It reveals how existing resources are being applied to security concerns, supports setting priorities on security-related requirements, and clarifies shortcomings in security coverage, for existing *and* target architectures. Understanding the gaps between requirements and functionality is critical in efficiently allocating resources: SEAM assists in providing that understanding and allows for a complete accounting of security within the enterprise. Furthermore, because the methodology is based on business asset analyses, it integrates with all of the predominant EA frameworks in use today.

Security is only as strong as its weakest link; complete coverage of security requirements is essential. The artifacts provided by SEAM allow managers to measure the completeness of enterprise protection measures. These benefits make our methodology a practical tool to facilitate strategic security planning by federal managers.

Appendix A
Annotated Bibliography

In preparation for developing our approach to integrating security into enterprise architectures, LMI researched numerous articles, websites, publications and reports. To allow for better understanding of background material on relevant government guidance, enterprise architectures and frameworks, and security, we provide an annotated bibliography in this appendix. The annotations provided are descriptive and informational without being evaluative or judgmental.

GOVERNMENT GUIDANCE

Clinger-Cohen Act of 1996 (formerly known as the Information Management Reform Act), February 10, 1996. Mandated that all federal agencies develop and maintain an enterprise architecture.

Computer Security Act of 1987, 40 Code of Federal Regulations (CFR) 759 (Public Law 100-235), January 8, 1988. Established a computer standards program at NIST. Requires each agency to have a risk-based security plan for each federal computer system identified as having "sensitive information."

Defense Authorization Act (P.L. 106-398) including Title X, Subtitle G, Government Information Security Reform, October 28, 2000. Requires agency chief information officers and inspectors general to evaluate their agency's computer security programs and report the results of those evaluations to OMB each September.

OMB Circular A-130, *Security of Federal Automated Information Resources* (February 1996 to present, with continuing updates), Appendix III. Requires federal agencies to consider risk when determining the adequacy of an agency's security and the security controls to be implemented. See http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html.

Paperwork Reduction Act of 1995, 35 CFR 44, January 4, 1995. Requires that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the federal government is consistent with applicable laws, including laws relating to privacy and confidentiality, security of information, access to information, and integrity, quality, and utility of the federal statistical system.

Presidential Decision Directive 63, *Protecting America's Critical Infrastructures*, May 22, 1998. Committed the federal government to "eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastruc-

tures, including especially our cyber systems" within 5 years. Resulted in the creation of the Critical Infrastructure Assurance Office to coordinate the federal government's initiatives in this area. Also established federal liaison responsibilities to work in partnership with the private sector in this area.

Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government*, October 21, 1998. Intended "to ensure survival of a constitutional form of government and the continuity of essential federal functions." Requires federal agencies to develop continuity of operations plans for essential operations.

ENTERPRISE ARCHITECTURES AND FRAMEWORKS

C4ISR Framework. Developed for use by DoD agencies to implement the DoD Architectural Framework (DoDAF). Provides for three views: operational, system, and technology. The elements of each view are intended to answer the questions of who, what, when, why, and how.

Federal Enterprise Architecture Framework (FEAF), Federal CIO Council, 1999. Provides a standard framework for documenting an agency's enterprise architecture. Purpose is to facilitate shared development of common processes across agencies. Consists of four architectural layers: business, data, applications, and technology.

LMI Enterprise Architecture Practice (LEAP), Logistics Management Institute, McLean, VA, 2000. Extends FEAF to include a method for describing and assessing current architectures and planning target architectures. Analytical approach provides a process for identifying and understanding the complex interrelationships of an organization's guidance, organizational units, business functions, business processes, and data, and the information technology that supports them. See www.lmi.org.

The Open Group Architecture Framework (TOGAF). Developed in 1994, provides a freely available architectural framework for IT that claims to be technology and tool neutral. Maintains a worldwide forum for all stakeholders. Contains TOGAF comparison with other frameworks such as FEAF, TEAF, Spewak, and Zachman. Currently in Version 7. Current plans for TOGAF migration from infrastructure to enterprise framework. See http://www.opengroup.org/public/arch/p4/others/others.htm.

Treasury Enterprise Architecture Framework (TEAF), Chief Information Officer Council, Department of the Treasury, Version 1, July 2000. A framework developed by Treasury for its agencies. Is aligned with FEAF and also with the Zachman Framework. TEAF provides a matrix for viewing the functional, information, organizational, and infrastructure architecture from various perspectives: planner, owner, designer, and builder. See http://www.treas.gov/teaf/arch_framework.doc.

Zachman Framework. Approach for documenting and developing an enterprise architecture. Provides multiple "perspectives" of the architecture and a categorization of the "artifacts" (objects or characterizations) of the architecture. Zachman provides a matrix of 36 cells intended to cover the who, what, where, when, why, and how of an enterprise. The enterprise is then divided into six levels of abstraction that are top-down, from the business level to the implementation level. See www.zifa.com.

SECURITY

Alberts, C., and A. Dorofee, *An Introduction to the OCTAVE Method*, Carnegie Mellon University, Software Engineering Institute, CERT Coordination Center, January 2001. Defines the essential components of a comprehensive, systematic, context-driven information security risk evaluation. OCTAVE uses a three-phased approach: build asset-based threat profiles, identify infrastructure vulnerabilities, and develop security strategy and plans. See http://www.cert.org/octave/methodintro.html.

CIO Council, *Federal IT Security Assessment Framework*, November 2000. Tool for evaluating the status of an agency's IT security program. Identifies five levels of security effectiveness and associated measurements for determining the degree to which the five levels are met.

Communications and Information Industries Directorate, Department of Trade and Industry, United Kingdom, *ISSO 17799, A Code of Practice for Information Security Management* (British Standard 7799), 1998 with continuing updates. Provides a framework to initiate, implement, maintain, and document information security within an organization. The standard is a business-led approach to best practice on information security management. Approach has three steps: creation of a management framework for information, risk assessment, and selection and implementation of controls. See http://www.dti.gov.uk/cii/datasecurity/1998dataprotectionact/what_is_bs_7799.shtml.

General Accounting Office, *Executive Guide on Information Security Management: Learning From Leading Organizations*, May 1998. Designed to promote senior executives' awareness of information security issues. Describes 16 practices, organized under five management principles, that GAO identified during a study of nonfederal organizations with reputations for having good information security programs. Each practice contains specific examples of the techniques used.

General Accounting Office, *Federal Information System Control Audit Manual (FISCAM)*, GAO/AIMD-12.19.6, January 1999. Document generally used by GAO auditors and agency inspectors when conducting an audit involving IT systems.

General Accounting Office, *Information Security Risk Assessment Practices of Leading Organizations*, GAO/AIMD-99-139, August 1999. Supplements the 1998 GAO Executive Guide on Information Security Management. Provides the elements of a "risk assessment process" along with critical success factors for that process. Discusses case studies, from both the private and public sectors, of risk assessment practices of four organizations "known for their efforts to implement good risk assessment practices."

National Communications System, *Public Switched Network Security Assessment Guidelines*, September 2000. Provides guidelines and methodologies for conducting a security assessment of PSN service providers. Designed to provide an overall review of their security stature. Includes security policy, physical security, network element and operations security, network access security, security training and awareness programs, and intrusion response procedures. Summary checklists are also provided. See www.ncs.gov/ncs/Reports/NCS_Security_Assessment_Guidelines_Version1_sep00.pdf)

National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP): Guidance on Securing Information Technology Systems*, NIST Special Publication 800-14, September 1995. Puts forth the premise that for the security of any system to be strong, the system's owners must consider three fundamental security areas: management controls, operational controls, and technical controls. Also recommends that strong management controls be used to tie all aspects of security together into a "sensible protection strategy." The eight NIST GSSPs are based on principles developed by OECD for its "Guidelines for the Security of Information Systems" in 1992. One of the eight principles, "Computer Security Requires a Comprehensive and Integrated Approach," suggests that a variety of areas—both within and outside of the computer security field—be part of such an integrated approach.

National Institute of Standards and Technology, *Guide for Developing Security Plans for Information Technology Systems*, Special Publication 800-18, December 1998. Provides guidance for federal IT managers regarding the preparation of IT security plans required by OMB Circular A-130, Appendix III, Management, Operational, and Technical Controls. Provides the framework for the development of security plans. See http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.doc.

National Institute of Standards and Technology, *Guidelines for Computer Security Certification and Accreditation*, Federal Information Processing Standard 102, September 1983. Contains guidelines relative to an agency's staff, applications, and other systems appropriate for certification and accreditation, including scheduling or reviews and recertifications. See http://csrc.nist.gov/publications/fips/index.html.

National Institute of Standards and Technology, Information Technology Laboratory, *Management of Risks in Information Systems: Practices of Successful Organizations*, March 1998. Describes some security practices identified by GAO in its review of best practices of leading organizations that had adopted superior security programs. "All of the organizations studied had reoriented their security programs to make them visible, integral components of their business operations." See http://www.itl.nist.gov/lab/bulletns/archives/mar98.htm.

National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems*, NIST Special Publication 800-30, October 2001. Intended to provide "a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems." Focus is on the ability to protect the organization and its ability to accomplish its mission, not just protecting its IT assets.

National Institute of Standards and Technology, *Self-Assessment Guide for Information Technology Systems* (Draft), November 2001. Provides a standard approach for assessing the security of an IT system. Contains an extensive questionnaire for assessing a system and guidelines for utilizing the completed questionnaire for analysis and follow-up, including examples for systems of a hypothetical agency. See http://csrc.nist.gov/publications/drafts/SelfAssessmentGuideITSystems-Review.doc.

National Institute of Standards and Technology, *Underlying Technical Models for Information Technology Security*, NIST Special Publication 800-33, December 2001. Describes the "models that should be considered in the design and development of technical security capabilities." The models described are taken from lessons learned, good practices, and specific technical considerations. Lists five objectives to meet the goals of security: availability, integrity, confidentiality, accountability, and assurance.

National Security Agency, Information Assurance Directorate, *Information Security (INFOSEC) Assessment Methodology*, August 2001. High-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks. NSA provides a training program on INFOSEC based on its experience in applying the methodology for its government customers. See http://www.nsa.gov/isso/iam/index.htm.

National Security Agency, *Information Assurance Technical Framework (IATF)*, September 2000. An unclassified reference document developed to help security managers and system security engineers address security concerns of their organizations. Is intended to help audience understand its technical needs and to select approaches to meet those needs regarding information assurance. Intended for use by both military and civilian agencies. The IATF document focuses on the technology aspects of Defense-in-Depth, which has four

objectives: defend the network and infrastructure, defend the enclave boundary, defend the computing environment, and supporting infrastructures. IATF provides a means for describing the security posture of an agency's systems, examples of threats to be defended against, as well as technical prescriptions for meeting specific security needs. See http://www.iatf.net/framework_docs/version-3_0/index.cfm.

National Security Telecommunication and Information Systems Security Committee No. 1000, *National Information Assurance Certification and Accreditation Process*, 2000. Provides a minimum standard set of activities, general tasks, and a management structure to certify and accredit systems, from an enterprise-wide view. See http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf.

System Administration, Networking and Security (SANS) Institute, online reading room. SANS Institute was established in 1989 as a cooperative research and education organization. SANS publications include papers written by university and other funded researchers, vendors (after review and approval by SANS), and people attempting to receive certifications offered through SANS training and certification programs. See http://rr.sans.org/index.php.

Appendix B
Abbreviations

C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CIAO	critical infrastructure assurance officer
CIO	chief information officer
COOP	continuity of operations
EA	enterprise architecture
EBA*	enterprise business asset
FEAF	Federal Enterprise Architecture Framework
FedCIRC	Federal Computer Incident Response Center
FSA*	fundamental security attribute
IRS	Internal Revenue Service
IT	information technology
LEAP	LMI Enterprise Architecture Practice
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SEAM*	Secure Enterprise Architecture Methodology
SEM*	security enforcement mechanisms
SFC*	security functional category
SPA*	security practice areas
SSA	Social Security Administration
TEAF	Treasury Enterprise Architecture Framework

* Abbreviation defined by the Secure Enterprise Architecture Methodology (SEAM)

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
10-2002	Final	

4. TITLE AND SUBTITLE
A Practical Approach to Integrating Information Security into Federal Enterprise Architectures

5a. CONTRACT NUMBER
IR229.00

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
DiDuro, John Crosslin, Robert,
Dennie, Debra; Jung, Paul;
Louden, Christopher;
Shepherd, David

5d. PROJECT NUMBER

5e. TASK NUMBER
IR229

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Logistics Management Institute
2000 Corporate Ridge
McLean, VA 22102-7805

8. PERFORMING ORGANIZATION REPORT NUMBER
LMI-IR229T1

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Logistics Management Institute
2000 Corporate Ridge
McLean, VA 22102-7805

10. SPONSOR/MONITOR'S ACRONYM(S)
LMI

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
A Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Security is a critically important consideration in government today. Managers are faced with a variety of security concerns driven by various laws, statutes, and regulations; agency policy; increased threat of terrorism; increased reliance on information technology; and issues of public trust. Security threats are cross-cutting, affecting IT planning, capital investment, systems design, operations, and IT governance. Failure to address security threats can interfere with a government organization's ability to carry out its mission. Simply implementing a variety of security mechanisms—the approach taken by most organizations—is not enough. Rather, security must be fully integrated into the organization's enterprise architecture. This report presents a methodology for doing that. The methodology is framework independent because it is based on the identification and description of business objects, which are common to all frameworks. The report also defines several concepts necessary for understanding the methodology and describes the benefits a federal agency will derive. By integrating security into its EA, an organization can ensure proper alignment of security initiatives with enterprise drivers and can readily identify and address security threats.

15. SUBJECT TERMS
security, enterprise architecture

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Nancy E. Handy
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	Unclassified Unlimited	45	19b. TELEPHONE NUMBER *(include area code)* 703-917-7249