Issue Date: 7/7/2008
Revision Date: <mm/dd/yyyy>

Document Purpose

This Practices Guides is a brief document that provides an overview describing the best practices, activities, attributes, and related templates, tools, information, and key terminology project managers need to be aware of as they implement the integrated security activities within the Enterprise Performance Lifecycle (EPLC) and address the specific approach to fulfilling the requirements of security within their projects. The document does not attempt to revisit the recommended approach to developing a system security plan or how to integrate security within a System Development program as these are documented in detail elsewhere. Instead, the document tries to outline where and how design decisions can simplify design and documentation requirements.

Background

The implementation of the EPLC Framework represents the recognition that security must be a continuous process addressing risks, vulnerabilities, and security controls, through regular reviews throughout all stages of a system's life cycle. Through this framework, information security is conducted in a manner that reduces risk to the information entrusted to HHS, and enables business activities through effective management of residual risks to information confidentiality, integrity, and availability.

For federal security practitioners, compliance with the Federal Information Security Management Act (FISMA) has been the driving force. The culmination of the FISMA process is a system security plan that

- Documents the people, processes, and IT resources implemented to protect a defined IT system;
- Allows business and security owners to certify that the system is adequately protected according to federal standards, and
- Formally accredits the system as authorized to process and store information, and
- Lays the groundwork for change management, self-assessment, vulnerability testing and other processes that ensure no new security risks are introduced into the system without approval of appropriate authority.

A number of federal laws and directives require integrating security into the development lifecycle of a system, including FISMA and Office of Management and Budget (OMB) Circular A-130, Appendix III.

The National Institute of Standards and Technology (NIST) has extensive information on integrating security within the development lifecycle. Project managers should review chapter three of NIST Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers* and for more detail review NIST SP 800-64, *Security Considerations in the System Development Life Cycle, Revision 2*. While the HHS EPLC establishes a more granular set of phases, these align closely with NIST documentation as shown in Table 1.

Table 1: Comparing the NIST Development Phases to HHS EPLC

NIST SDLC Phases	Initiation		Acquisition \ Development					Implementation \ Assessment	Operations \ Maintenance	Disposition
HHS EPLC Phases	Initiation	Concept	Planning	Requirements Analysis	Design	Development	Test	Implementation	Operations and Maintenance	Disposition

Practice Overview

One of the primary goals of the EPLC is to ensure that security considerations are planned for early and handled consistently in the project lifecycle. The primary goal of the Security Approach is to document a plan that coordinates the other project stakeholders toward this end while clearly defining how the intended services within a project will be secured with the best outcome for the requirements of the business. To do this the security approach must highlight the owners and activities that connect the business goals of the system to the implemented security controls to ensure those goals are delivered securely. While the security approach for a program is linked to the System Security Plan (SSP), and much of the planning and documentation can likely be re-used in the SSP, it is a distinct process.

The primary security document for a federal system is the SSP which is analyzed, updated, and accepted during the Certification and Accreditation (C&A) process. The SSP documents the system name, system categorization, system owner, Authorizing Official and contacts, information system type, system environment and interconnections, system description and purpose, applicable laws and regulations, selected security controls, completion and approval dates, and a plan for on-going maintenance. Details of the SSP and C&A development processes are well documented elsewhere within the EPLC and NIST.

However, establishing how and where to draw system boundaries can be the most critical and difficult part of securing a system. The FIPS 199 requirement to secure an information system to the high watermark or highest impact level must be applied when grouping minor applications/subsystems with varying FIPS 199 impact levels into a single general support system or major application unless there is adequate boundary protection.

Establish the Security Team

The security team is a critical resource for IT system security. The security team consists of the Business Owner, System Owner, System Security Manager, User Representatives, the Designated Approving Authority (DAA), Certify Authority and other key participants who are involved in the C&A process. The *EPLC C&A Practices Guide* provides details on the Department's process, including identifying others on the C&A team.

Document the Security Roles and Responsibilities – Clearly identifying the personnel on the security team with important security roles for the different phases of the EPLC will assure that the security requirements are properly addressed. Program Managers leverage the configuration or change management activities to ensure that all the security the security requirements are identified with a responsible security manager.

Developing the Security Approach

The process of developing the security approach is primarily concerned with the actions necessary to define, integrate, and coordinate all subsidiary planning documents into a single PMP. The security approach is usually drafted by the Project Manager in collaboration with the security team.

Like a good project management plan, the security approach does not need to be complicated or lengthy, so long as it covers the entire system and guides the later phases on how to collaborate with different team members and facilitate the business goals for the system. A fairly contained system or an update to an established system may not require an in-depth security approach as the difficult tasks of categorizing the system, characterizing the system, and defining the system boundary has already been done.

Categorizing the System – Before the security approach can be developed, the information system and the information resident within that system must be categorized based on a FIPS 199 impact analysis. Each system identified in the agency's system inventory must be categorized using FIPS 199. NIST Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, provides implementation guidance in completing this activity. See Table 2 for a summary of FIPS 199 categories.

Table 2: FIPS 199 Categorization

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Characterize the System – In compliance with OMB Circular A-130, the system in development should be characterized as part of a General Support System, Major Application, or Minor Application. All information systems labeled as a major application (MA) or general support system (GSS) must be covered by an SSP. Specific system security plans for minor applications are not required because the security controls for those applications should be provided by the GSS or MA in which they operate. Furthermore, changes to an existing system must be assessed for impact as major changes require the re-certification and accreditation of the system. Appropriately characterizing the system and/or the impact of any proposed changes will impact later phases not only by establishing the requirement for a new or updated SSP but also assists in defining the system boundaries and thus clarifying critical stakeholders.

Establishing the System Boundaries – The next step in establishing the security approach is defining where the system boundaries lie and how the system interfaces with other systems. This requires an analysis of both technical system boundaries and organizational responsibilities. Because the overall categorization of a system is established by its FIPS 199 'high water mark', the FIPS 199 impact levels must be considered when constructing the system boundaries. Constructing a preliminary notion of the physical and logical boundaries around a set of processes, communications, storage, and related resources identifies a system. The set of elements within these boundaries constitutes a single system. Each component of the system must:

- Be under the same direct management control (i.e., one system owner even though the MA may cross several business lines)
- Have the same general business function(s) or business objective(s)
- Have essentially the same operating characteristics and security needs

All components of a system do not need to be physically connected. Examples:

- A disparate set of identical systems used to provide redundant Internet services
- Geographically dispersed storage arrays used to provide operational and redundant mail stores
- A system with multiple identical configurations that are installed in locations with the same environmental and physical safeguards.

Most critically, it is certainly appropriate to reference an underlying GSS as providing a number of security requirements (e.g. authentication), or even define multiple systems within the same development program. In defining the various system boundaries, the Program Manager must work with the security team so that their approach ensures that meeting business requirements, system accreditation, as well as continuous monitoring and re-accreditation are cost effective and manageable.

Identify Programmatic Activities that Support Security
A number of activities support the security goals, but are not directly involved with the implementation of technical security controls. Document how these activities are being leverage in support of the security approach. Possible activities include IT security funding requests in capital planning and investment control activities, developer and staff training, risk, change and configuration management activities, and documentation development.

Best Practices

- **Prepare for later stages** – While the majority of security deliverables are completed in the Implementation phase, Program Managers can leverage increased return on investment in their security programs by using these deliverable targets to guide the earlier stages of a system, such as:
    - Early identification and mitigation of security vulnerabilities and misconfigurations, resulting in lower cost of security control implementation and vulnerability mitigation;
    - Awareness of potential engineering challenges caused by mandatory security controls;
    - Identification of shared security services and reuse of security strategies and tools to reduce development cost and schedule while improving security posture through proven methods and techniques;
    - Facilitating informed executive decision making through comprehensive risk management in a timely manner;
- **Coordinate with stakeholders** – Developers, business owners, and security partners all have insight into the goals and challenges likely to encounter when developing, integrating, and implementing system security. Including these individuals in the development of the security approach will facilitate the later phases.
- **Review and Modify** – A number of assumptions will be required in the earliest documentation of the security approach.
- **Integrate with related activities** – Outputs of the security approach activities will need to be integrated into other Program Management and EPLC activities, e.g.:
    - Security Requirements will need to be fed into the Requirements Analysis phase as well as the Configuration Management activities;
    - Conflicts and risk will need to be managed within the Risk Management or Issues Management activities;
    - System Boundaries estimates may affect Scope Management activities; and
    - Security Stakeholders need to be included within the Communications Management activities.
    - Individuals with key security responsibilities need to be identified, and ensuring they complete Mandatory Role-Based Training (RBT) must be considered when planning training requirements

Practice Activities

Activities within the security approach should help establishes the number and scope of system security plans and C&A documents required to effectively secure and document the output of the project.

- Coordinate system purpose, business needs and requirements, and security requirements
- Document the intended Security Approach
- Document the Security Critical Partners, Designated Approving Authority, and Certification Authority for each C&A package likely to be developed
- Establish preliminary System Security Categorization according to NIST SP 800-60 and FIPS-199
    - Identify information sensitivity
    - Select provisional impact level
    - Review provisional impact levels and adjust/finalize information impact
    - Assign system security category
- Establish system and sub-system boundaries
    - Identify data sharing and external system interconnections

  - Identify any interconnections with a GSS.
  - Define boundaries for any sub-system to be developed
- Document any required security controls from NIST SP 800-53 known to be provided by an underlying GSS or MA.
- Document critical stakeholders for supporting GSS or MA and include these individuals in the security approach development as appropriate.
- Document and map any required security controls from NIST SP 800-53 known to be provided by the system in development, a sub-system in development.
- Document any remaining security controls that cannot be mapped to the system or sub-systems in development, or an underlying GSS or MA.
- Document development teams responsible for design and implementation of new security controls.
- Document development teams responsible for integration with GSS, MA, minor applications, or other interconnected systems.

Practice Related Information

NIST FIPS Publications
All NIST Federal Information Processing Standards (FIPS) publications are available at the following site: http://csrc.nist.gov/publications/PubsFIPS.html.

- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

NIST Special Publications
All NIST Special Publications (SP) are available at http://csrc.nist.gov/publications/PubsSPs.html.

- NIST SP 800-64, Security Considerations in the System Development Life Cycle, Revision 2
- NIST SP 800-60, Draft Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes),
  Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories
  Volume 2: Appendices
- NIST SP 800-53 Rev. 2, Recommended Security Controls for Federal Information Systems
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems
- NIST SP 800-30, Risk Management Guide for Information Technology Systems
- NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems
- NIST SP 800-18 Rev. 1, Guide for Developing Security Plans for Federal Information Systems

Practice Key Terms

CA – Certification Agent
DAA – Designated Approving Authority
GSS – General Support System
ISSO – Information System Security Officer
MA – Major Application
SP – Special Publication
SSP – System Security Plan