Software Engineering Institute | Carnegie Mellon University

Assuring Software Systems Security: Life Cycle Considerations for Government Acquisitions

Rita Creel

June 2007

ABSTRACT: When systems are built under government contract, the acquirer and contractor share responsibility for the outcome, not only in terms of cost, schedule, and performance, but also with respect to quality attributes such as security. Using an acquisition life cycle framework, this article identifies acquirer activities, products, and resources that are necessary to establish and support contractor efforts to build secure software-intensive systems.

ACKNOWLEDGMENTS: Contributions and reviews by Kristi Keeler, Gary McGraw, Nancy Mead, Tim Morrow, and Stan Wisseman are gratefully acknowledged. Errors and omissions are the author’s.

INTRODUCTION

Software-intensive systems are critical to the administration and operation of every government organization. These systems come in vastly different configurations and are used in activities ranging from financial records management to aircraft navigation and flight control. Since they are built under government contract, it is not only the developer who is responsible for the outcome. The activities, products, and behaviors of the government acquisition office have a substantial influence.

Historically, large government acquisitions—especially those with a major hardware development component—have treated software as less deserving of early attention than the hardware elements of the system. Software was an afterthought, something to be considered after completing the hardware architecture and design.

Current trends are changing these attitudes [Boehm 06, Ellison 07]. The composition of systems has changed from primarily hardware to highly software intensive. Software problems in government systems regularly make national headlines and have been featured in government reports [DSB 00, GAO 04]. And increased hardware and software capability are driving highly touted plans to maximize system integration and interoperability. Finally, we all experience the

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

consequences of software that is not quite robust enough to identify and reject intrusions such as spam, viruses, and worms. All these trends contribute to a growing need for government acquirers to pay more attention to software from the very start.

The U.S. Department of Homeland Security, Cyber Security Division, Software Acquisition Working Group has prepared a guidebook focused on enhancing software supply chain management throughout the software acquisition and purchasing process [DHS 07]. Appendix A lists resources to assist acquirers with software acquisition improvement in general. These resources are useful in establishing a framework for software acquisition that will support the insertion and sustainment of robust software security practices.

While acquisition activities for all government systems must comply with the Federal Acquisition Regulation (FAR) [GSA 05], many additional policies and guidelines exist specific to the type of system and the acquisition authority. This article focuses on engineering activities of major acquisitions in general rather than on specific acquisition policies. In the next section, we define the scope of this article relative to three broad categories of government systems. We then present a generalized acquisition life cycle model and identify key acquirer actions to incorporate software security from initial concept analysis through system retirement and disposal.

CATEGORIES OF GOVERNMENT SYSTEMS

This article targets three categories of software-intensive government systems: major systems acquisitions, national security systems, and information technology systems.

Major systems acquisitions (MSA) include systems consisting of software, hardware, equipment, or a combination thereof that function together to fulfill a mission need and for which (a) the U.S. Department of Defense (DoD) is responsible and estimated total expenditures for research, development, test, and evaluation exceed $173.5 million or the eventual total expenditure for the acquisition exceeds $814.5 million; (b) a civilian agency is responsible and total expenditures are estimated to exceed $1.8 million or the dollar threshold for a major system established by the agency pursuant to Office of Management and Budget (OMB) Circular A-109, “Major System Acquisitions,” whichever is greater; or (c) the head of the responsible agency has applied the designation “major system” [GSA 05, Subpart 2.1]. Systems not considered “major” are “non-major” per OMB Circular A-11, Section 300 [OMB 06].

National security systems (NSS) include systems used or operated by an agency, a contractor of an agency, or on behalf of an agency, with functions or operations that involve intelligence activities; cryptologic activities related to national security; command and control of military forces; equipment that is an integral part of a weapon or weapons system; direct fulfillment of military or intelligence missions, with the exception of systems used for routine administrative and business applications; and systems protected by procedures authorized by Executive order or deemed by an Act of Congress to be classified in the interest of national defense or foreign policy [Barker 03]. These systems often include a significant hardware technology effort, but they have become increasingly software intensive.

Information technology systems (ITS) include computers, ancillary equipment and peripherals, software, firmware, procedures, services, and related resources, not including equipment acquired incidental to a contract or containing embedded information technology that is used as an integral part of the product but is not used to process or manage data or information [GSA 05, Subpart 2.1]. In this definition, ITS include records management systems but exclude special-purpose devices that control, for example, heating, ventilation, and air conditioning systems and medical equipment.

The categories MSA, NSS, and ITS are not mutually exclusive, as is shown in Figure 1. A system may belong to one, two, or all three categories. When a system belongs to the NSS category and one or more of the others, NSS acquisition, security, and other policies take precedence. In other cases in which more than one category applies, further analysis is needed to determine the governing policies.

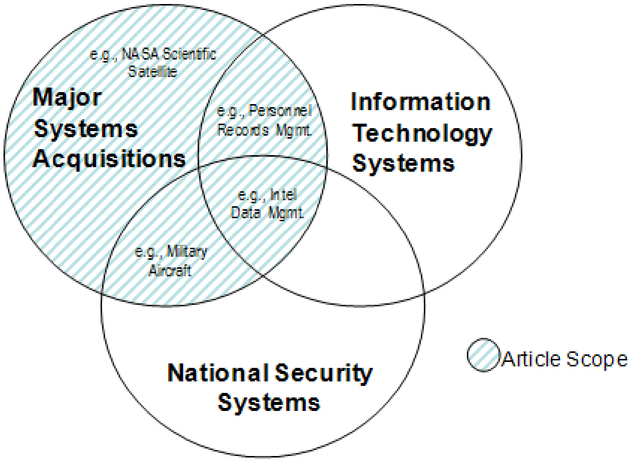
e.g., NASA Scientific Satellite
Major Systems Acquisitions
e.g., Personnel Records Mgmt
Information Technology Systems
e.g., Intel Data Mgmt
e.g., Military Aircraft
National Security Systems
Article Scope

Figure 1. Categories of government system acquisitions

As shown in Figure 1, the scope of this article is MSA, including systems that may also be NSS, ITS, or both. The article excludes the procurement of COTS-only systems that do not meet the MSA definition. The article Security Considerations in Managing COTS Software identifies risks and presents a systematic risk mitigation approach for COTS software. Also excluded from the article are non-major acquisitions and specialized systems designed for an urgent need and for which an ultra high level of risk is acknowledged and accepted (for some intelligence missions, for example).

THE GOVERNMENT ACQUISITION LIFE CYCLE

An acquisition life cycle model is a framework of activities, reviews, decision points, and interrelationships used to guide procurement of a materiel solution to a government agency capability need. Several variations on the government acquisition life cycle model exist, each geared toward the needs of a particular domain. While the models are similar, the names, duration, and exact content of life cycle activities, reviews, and decision points may differ. In addition, the models may be implemented to support either a single-step or evolutionary approach to capability delivery. With a single-step approach, there is a single delivery of full capability. With evolutionary approaches, there is a phased delivery of capabilities until full capability is reached. This phased delivery may be incremental (the final capability is defined up front) or evolutionary (the capability definition evolves over the life cycle).

The acquisition life cycle for a major system governs the overall procurement. Within that life cycle, subordinate development life cycle models are defined for major system components. For example, a small embedded subsystem may be developed using a waterfall model for both hardware and software. A large command and control element may be developed using a waterfall model for hardware and an incremental or spiral model for software. These and other components are later integrated to form the end-to-end system governed by the over-arching acquisition life cycle model.

To discuss acquirer activities throughout the government life cycle for MSA, we will use a generic model based on ISO/IEC 15288, Systems engineering – system life cycle processes [ISO/IEC 02, INCOSE 06]. Other relevant life cycle models are described in DoD Instruction 5000.2, Operation of the Defense Acquisition System [DoD 03]; National Security Space Acquisition Policy NSS 03-01, Guidance for DoD Space System Acquisition Process [USAF 03-01]; and agency-specific policies.

The acquisition life cycle model shown in Figure 2 includes three time frames: Pre-Systems Acquisition, Systems Acquisition, and Sustainment. Each consists of one or more life cycle stages characterized by activities, reviews, and decision points—gates at which readiness to progress from one major acquisition activity to the next is evaluated. In parallel with the acquisition life cycle are the ongoing mission and business cycles for the organization. Needs for new capabilities emerge in the context of these cycles.

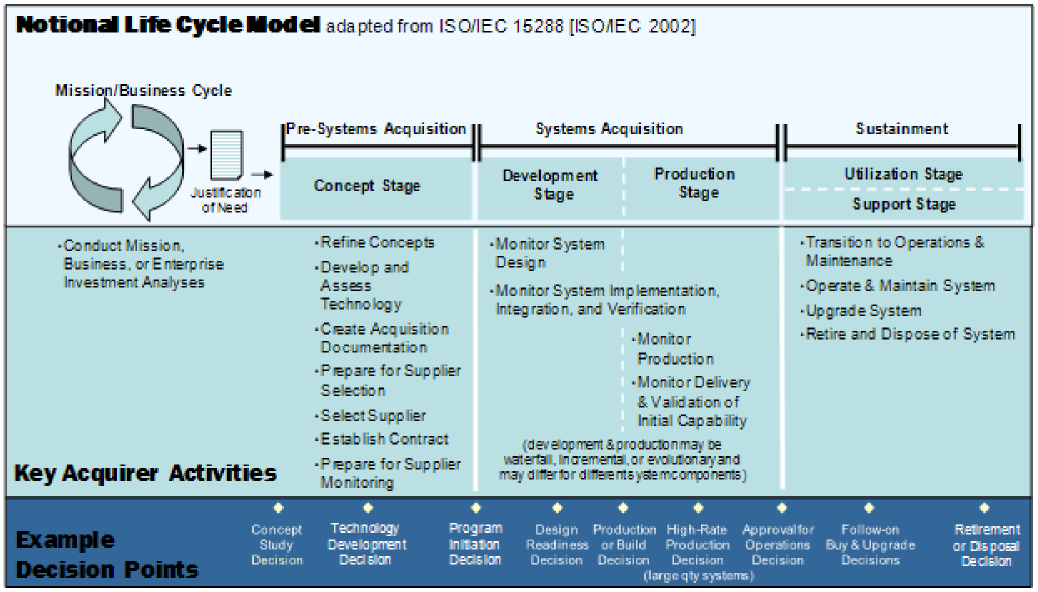
Notional Life Cycle Model adapted from ISO/IEC 15288 [ISO/IEC 2002]
Mission/Business Cycle
Justification of Need
Pre-Systems Acquisition
Systems Acquisition
Sustainment
Concept Stage
Development Stage
Production Stage
Utilization Stage
Support Stage
•Conduct Mission, Business, or Enterprise Investment Analyses
•Refine Concepts
•Develop and Assess Technology
•Create Acquisition Documentation
•Prepare for Supplier Selection
•Select Supplier
•Establish Contract
•Prepare for Supplier Monitoring
•Monitor System Design
•Monitor System Implementation, Integration, and Verification
•Monitor Production
•Monitor Delivery & Validation of Initial Capability
(development & production may be waterfall, Incremental, or evolutionary and may differ for different system components)
•Transition to Operations & Maintenance
•Operate & Maintain System
•Upgrade System
•Retire and Dispose of System
Key Acquirer Activities
Example Decision Points
Concept Study Decision
Technology Development Decision
Program Initiation Decision
Design Readiness Decision
Production or Build Decision
High-Rate Production Decision (large qty systems)
Approval for Operations Decision
Follow-on Buy & Upgrade Decisions
Retirement or Disposal Decision

Figure 2. Generalized government acquisition life cycle

The next sections describe each time frame in the acquisition life cycle stage and candidate acquirer activities related to software security.

The Ongoing Mission and Business Cycles

The needs that eventually lead to a new acquisition arise from an organization's day-to-day mission and business operations. Investment and work process analyses articulate these needs and may recommend process changes, procurement of a new system, or both. If procurement of a new system is an option, the organization enters Pre-Systems Acquisition.

Table 1. Analysis of system needs

Activity Name	Activity Description
Mission, Business, or Enterprise Investment Analysis	**Objective:** Review key mission or business processes (collectively, work processes), changes in the operational environment, and gaps in capability to determine the need for a new system. **Typical Artifacts:** Investment/work process analysis report documenting business environment, work flows, data and participants, and work environment (for business systems) or threat environment, concepts of operations (CONOPS), and description of missing capabilities (for military or other types of systems); plan for an Analysis of Alternatives (AoA) and other activities to identify and refine potential solutions; initial security risk assessment related to investment analysis report **Software Security Actions:** Identify and document threats, given the information in the investment/work process analysis report. Consider how threats may evolve over the life of the system, including potential vulnerabilities in the work processes that could be exploited. Identify high-priority risks and establish security evaluation criteria to support a high-level assessment of mission and work process alternatives and risk mitigation options as these processes are refined. Identify organizations that may influence security requirements and processes, and establish points of contact.

Pre-Systems Acquisition

The goal of Pre-Systems Acquisition is to mature a system solution concept to the degree that

- a suitable acquisition strategy can be developed
- capability need and solution constraints can be adequately expressed in a Request for Proposal (RFP), such that the offerors can scope and estimate the cost and schedule for the necessary work tasks
- the acquirer understands enough about the solution to plan and prepare for supplier monitoring

The degree of maturation expected in Pre-Systems Acquisition will depend on the complexity of the system to be acquired and the level of technology, cost, and schedule risk deemed acceptable.

Activities performed during Pre-Systems Acquisition include Refine Concepts, Develop and Assess Technology, Create Acquisition Documentation, Prepare for Supplier Selection, Select Supplier, Establish Contract, and Prepare for Supplier Monitoring. These activities are listed in Table 2, along with software security actions the acquirer should perform to lay the foundation for secure software development.

Table 2. Pre-Systems Acquisition activities

Activity Name	Activity Description
Refine Concepts	Objective: Analyze and document (*a*) user demographics and needs, (*b*) required capabilities, quality, and performance, (*c*) concepts of operation, maintenance, and evolution, (*d*) interfaces with other systems and organizations, including interface stability, and (*e*) concept-related risks. Typical Artifacts: CONOPS, capabilities descriptions, AoA, market research and technology assessment, initial integrated architecture description, initial system threat assessment, technology development strategy, systems engineering plan (SEP), test and evaluation (T&E) strategy Software Security Actions: Establish a software security function, led by an experienced software security professional, within the program office. Prepare charter, effort, schedule, and resource requirements. Continue to identify threats and vulnerabilities in the emerging operational environment and solution space. Apply security evaluation criteria to concept refinement activities and artifacts. If COTS or other non-developmental items are identified as part of candidate solutions, research the items' current and potential security risks. Document the approach to continuously identify, specify, and manage software security risks throughout the life cycle. Hold technical interchange meetings with stakeholders to begin developing an understanding of potential software security issues.
Develop and Assess Technology	Objective: Develop new or unproven hardware and software technologies to an acceptable maturity level for the acquisition. Typical Artifacts: Technology readiness assessment, cost analysis, interoperability and supportability assessment, revised AoA, integrated architecture description, system threat assessment, SEP, TDS, and T&E master plan (TEMP) Software Security Actions: Continue security activities identified for Refine Concepts. Identify software quality attributes, including security, in candidate system architecture descriptions. Begin to select and define security properties to monitor throughout the life cycle. Hold technical interchange meetings with stakeholders to specify software-related system-level security requirements. Ensure these requirements are traceable to verification activities in the TEMP. Ensure cost analyses consider costs associated with building in and verifying security. If software technology development has produced prototype or demonstration systems, ensure appropriate plans exist to "productize" the prototype (i.e., to develop robust software for the operational system) and that these plans include security.

Create Acquisition Documentation	Objective: Develop strategy and plan for acquisition, considering key cost, schedule, and performance constraints, and risk. Also, develop and secure approval of documents required by law for the type of system to be acquired. Typical Artifacts: Acquisition strategy and acquisition plan; documents required for compliance with statutory and regulatory requirements; threshold and objective values for performance, quality, cost, and schedule parameters (for DoD, these compose the Acquisition Program Baseline); acquisition risk management plan Software Security Actions: Ensure that the acquisition strategy and plan accommodate security activities and resource requirements. Review compliance with security-related statutory and regulatory requirements. Define and incorporate security parameters into the Acquisition Program Baseline.
Prepare for Supplier Selection	Objective: Develop Request for Proposal (RFP) and Supplier Selection Plan (SSP) [GSA 05, Subpart 15.2]. Typical Artifacts: RFP, with technical requirements, instructions to offerors, statement of work, requirements for contractual deliverables (management and technical), evaluation criteria, and other conditions related to the proposal; and SSP, identifying organization and responsibilities of the source selection team, evaluation criteria, and detailed procedures for proposal evaluation Software Security Actions: Ensure that the RFP (for additional detail, see Appendix B) • requires offerors to apply robust software engineering practices (e.g., [DoD 94]) for all software regardless of origin and to demonstrate in the proposal their intent and ability to do so • specifies technical and management requirements and standards for software security, expected contractor support for government-led security reviews and audits, and expected government participation in contractor-led security reviews • requires delivery and update of a preliminary software/ system security plan covering all offeror team members with software responsibility. Example content for a software/system security plan may be found in [NIST 06] (agency-specific guidelines also exist). • specifies content and delivery schedule and media for software artifacts to be produced during System Acquisition • identifies government access required to contractor artifacts and facilities for security reviews • requires that the offerors identify and estimate the work tasks and costs associated with interacting with government security organizations throughout the life cycle Ensure that the source selection team includes a software security expert who will participate in proposal evaluation to identify strengths, weaknesses, and risks associated with security-related technical and management practices and deliverables and corresponding cost and schedule estimates. Develop a strategy and plan for evaluating, during supplier selection, the offerors' ability and intent to meet critical security requirements.

Select Supplier	Objective: Select the proposal that represents the best value [GSA 05, subpart 15.3]. Typical Artifacts: Strengths, deficiencies, significant weaknesses, and risks of each proposal as documented against the evaluation criteria defined in the RFP and per the SSP; clarification requests; cost realism analysis; ability of offerors to meet technical requirements; initial and final proposals; and source selection decision and rationale Software Security Actions: Ensure software security expert reviews proposal sections with software security implications. Before competitive range is established and as needed, prepare security-related clarification requests to be submitted to offerors. After competitive range is established and if discussions are permitted, prepare for discussions on security deficiencies, weaknesses, or risks related to offerors' approaches.
Establish Contract	Objective: Finalize the contract and complete preparation for supplier monitoring. Typical Artifacts: Final contract Software Security Actions: Review and approve contractor plans for mitigating security-related weaknesses and risks identified in the winning proposal. Identify and plan for security-related review activities.
Prepare for Supplier Monitoring	Objective: Document plan for supplier monitoring activities along with resource needs (quantity and area of expertise). Identify resources to be used for each activity, artifacts to be produced (e.g., review comments), and plan for approving, using, and archiving these artifacts. Identify and document known risks. Typical Artifacts: Supplier monitoring plan and updated acquisition risk management plan. Software Security Actions: Include in supplier monitoring plan activities for a software security expert to review evolving artifacts and participate in relevant system and software reviews. Ensure acquisition risk management plan incorporates software security risk. Define approach to monitor the evolving system and operational context and manage emerging software security risks. Conduct software kick-off workshop for security (may be included as part of an overall workshop to address quality attributes in a software context). In defining a framework for government involvement in software security, ensure change control boards have a standing member who is a security specialist and include evaluation of software security implications and risks.

Systems Acquisition

The goal of Systems Acquisition is to design, develop, and deliver an initial system capability. As the contractor team conducts its engineering activities, the acquirer evaluates the progress and outcomes of these activities, including interim artifacts. This is especially critical for large, complex systems in which there are many variables and risks. For a non-functional attribute such as software security, it is particularly important to remain vigilant throughout Systems Acquisition, because changes in requirements, the environment, and cost and schedule constraints can overwhelm efforts related to such "invisible" attributes.

Note that for some types of systems, especially those with complex hardware development, system-level activities may not correspond directly with software activities. For example, with iterative software development methods, some software items may complete design during early system design, while other software items may not start design until system design is complete.

Activities performed during Systems Acquisition include Monitor System Design; Monitor System Implementation, Integration, and Verification; and Monitor Delivery and Validation of Initial Capability. These activities are listed in Table 3, along with software security actions the acquirer should perform to prevent, or identify and mitigate, security issues.

Table 3. Systems Acquisition activities

Activity Name	Activity Description
Monitor System Design	Objective: Ensure the design for the system, including all hardware, software, interfaces, and operations and sustainment concepts, is adequate to support implementation. Typical Artifacts: Evolving software and system artifacts (e.g., architectures, requirements, designs, software, hardware, verification and review records, plans, measures, review presentations, change requests, assurance cases and evidence) Software Security Actions: Review/audit software artifacts against security criteria. Review security-related artifacts, e.g., use and abuse cases, assurance cases, SSP, certification and accreditation plans. Ensure these artifacts are updated and matured as the system evolves. Conduct biweekly technical interchange meetings during system design to ensure an adequate and sustained focus on security. Ensure adherence to security plans and modification of plans if necessary. Continue to identify, manage, and track security risks and issues identified through contractor and government reviews. Identify risks associated with • dependencies between systems • multiple administrative control points • operations for individual systems and systems of systems • impact of changing system states and operating environment • volatility (architecture, requirements, design, code, staff, plans, procedures) For software developed using iterative approaches, ensure each iteration (increment, build, spiral) includes a security risk evaluation. Evaluate proposed upgrades and changes to non-developmental items (e.g., COTS and reuse) for continuing suitability with respect to security criteria.

	Re-evaluate security artifacts and activities as the operational context, system definition, and threat environment change.
Monitor System Implementation, Integration, and Verification	Objective: Implement and integrate the system and verify that it is ready for production (for high-quantity systems) or build activities and integration into the operational environment. Typical Artifacts: Evolving software and system artifacts (e.g., architectures, requirements, designs, software, hardware, instructions and procedures, verification and review records, certification and accreditation records, assurance cases and evidence, plans, measures, review presentations, change requests) Software Security Actions: Continue security activities initiated previously. Monitor changes to system and software artifacts driven by requirements changes, iterative development, and deficiency reports for security impacts. Review delivery and installation processes for security risks. Review test plans and test equipment to ensure they will adequately address security requirements, given changes to system and software artifacts. Review operator, user, and maintenance manuals and associated processes for security risks. Ensure security-related configuration management and control practices are established and ready for use in the operational environment and maintenance facility, review regression testing procedures, and participate in C&A activities.
Monitor Delivery and Validation of Initial Capability	Objective: Ensure the system (or first increment of capability) is acceptable for use in the operational environment. Typical Artifacts: System hardware and software; installation and configuration management procedures and report; acceptance report; verification/validation records; operator, user, and maintenance manuals; system security plan; other deliverable documentation; deficiency reports; C&A report; and assurance cases and evidence Software Security Actions: Review artifacts. Monitor installation process to ensure appropriate configuration of deployed system. Document and resolve security risks and issues. Monitor initial operations and early defect reports and change requests. Monitor change procedures, if applicable, for security risks and issues. Ensure security-related configuration management and control practices are applied, and participate in C&A activities.

Sustainment

In Sustainment, the system is in use and evolves through periodic and event-driven maintenance and upgrades. For software-intensive systems, Sustainment presents critical challenges to maintaining the security posture. Maintenance in the operational environment is essential to provide for system restoral in the case of failure and for rapid resolution of mission-impacting deficiencies. In the nonoperational maintenance environment, approved changes are implemented to resolve less critical deficiencies and enhance the system. In either case, maintenance actions may put the operational mission and system security at risk.

For systems that include from a few to hundreds of COTS products, periodic upgrades are needed to maintain compatibility across the products and ensure continuing vendor support. Since the acquirer cannot control COTS evolution, a new release of such a system may bring with it changes not requested or expected by the user, operator, or maintainer. So COTS upgrades further complicate security reviews.

Activities performed during Sustainment include Transition to Operations and Maintenance, Operate and Maintain System, Upgrade System, and Retire and Dispose of System. These activities are listed in Table 4, along with software security actions the acquirer—and after transition, the operator and maintainer—should perform to prevent, identify, and mitigate the impacts of security risks and breaches.

Table 4. Sustainment activities

Activity Name	Activity Description
Transition to Operations and Maintenance	Objective: Transition system to operations and maintenance function. Typical Artifacts: Transition plan and report, verification and validation records Software Security Actions: Identify security risks in the environment and the system. Given the operations and maintenance environment, provide an assessment of the robustness of the system and its resilience against security risks. Provide mitigation recommendations. Participate in C&A activities.
Operate and Maintain System	Objective: Use the system in its intended environment, performing maintenance as directed to address deficiencies in performance and quality. Typical Artifacts: Transition plan and report, verification and validation records, updated operator, user, and maintenance manuals Software Security Actions: Identify security risks in the environment and the system. Ensure adequate regression testing is conducted when the system is modified and participate in C&A activities. Given the operational environment, provide an assessment of the robustness of the system and its resilience against security risks. Provide mitigation recommendations. Ensure the software maintenance activity can support and test the security requirements for the system.

Upgrade System	Objective: Incorporate new features into the delivered system. These features may be delivered under the same contract (e.g., for a planned incremental capability) or under a new or modified contract. Typical Artifacts: Depending on the extent and nature of the features, the process may return to the Design or Implementation, Integration, and Verification activity of System Acquisition. Some or all of the same artifacts will be produced or modified. Software Security Actions: Same as the security actions of all activities from the relevant System Acquisition activity through Operate and Maintain System.
Retire and Dispose of System	Objective: Dispose of system when it is no longer required. Typical Artifacts: System disposal records Software Security Actions: Ensure precautions are taken so that security countermeasures are not revealed and so that disposal does not compromise other systems (e.g., ensure data that could allow entry into another system or reveal its vulnerabilities is destroyed). If media are to be sanitized, ensure required information is retained and secured first.

SUMMARY

A solid foundation for acquisition includes not only the required technical and management activities but also the budget, schedule, and staff needed to carry them out. This is challenging, in part due to pressures to reduce costs and hasten delivery of new capabilities, but also because of historical attitudes toward software. At the policy level, this is beginning to change with software's growing role in implementing critical capabilities and interoperability requirements and with higher expectations for system dependability. But more work is needed for these changes to reach the core of the acquisition program office and impact the outcomes of major systems acquisitions.

We have presented a preliminary framework of activities focused on building security into the government's major systems, spanning the acquisition life cycle from identification of a mission or business need to system disposal. This framework will be refined as policy, technology, and practices evolve. Future papers will provide more detail for activities in each stage of the framework, including the concept, development, production, and utilization and support stages.

REFERENCES

[Adams 04]

Adams, R. J.; Eslinger, S.; Hantos, P.; Owens, K. L.; Stephenson, L. T.; Tagami, J. M.; Weiskopf, R.; Newberry, Lt Col G. A.; & Zambrana, M. A. Software Development Standard for Space Systems (Aerospace TOR-2004(3909)-3537). El Segundo, CA: The Aerospace Corporation, September 2004.

[Albert 02]

Albert, Ceci & Brownsword, Lisa. Evolutionary Process for Integrating COTS-Based Systems: An Overview (CMU/SEI-TR-2002-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, July 2002.

[Anderson 06]

Anderson, William; Brown, Mary Maureen; & Flowe, Rob. Joint Capabilities and System-of-Systems Solutions: A Case for Crossing Solution Domains (CMU/SEI-2006-TN-029). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 2006.

[Barker 03]

Barker, William C. Guideline for Identifying an Information System as a National Security System (NIST SP 800-59). Gaithersburg, MD: National Institute of Standards and Technology, August 2003.

[Boehm 06]

Boehm, Barry. “Some Future Trends and Implications for Systems and Software Engineering Processes.” System Engineering 9, 1 (January, 2006): 1-19.

[Carney 03]

Carney, David J.; Morris, Edwin J.; & Place, Patrick R. H. Identifying Commercial Off-the-Shelf (COTS) Product Risks: The COTS Reuse Risk Evaluation (CMU/SEI-2003-TR-023). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, September 2003.

[DHS 07]

Department of Homeland Security Cyber Security Division. Software Assurance in Acquisition: Mitigating Risks to the Enterprise, Draft Version 1.0. March 5, 2007.

[DoD 03]

U.S. Department of Defense. Operation of the Defense Acquisition System (DoD Instruction 5000.2). May 12, 2003.

[DoD 94]

U.S. Department of Defense. Software Development and Documentation (MIL-STD-498). December 1994.

[DSB 00]

Defense Science Board. Report of the Defense Science Board Task force on Defense Software. Washington, DC: Office of the Under Secretary of Defense for Acquisition and Technology, November 2000.

[Ellison 07]

Ellison, Bob & Creel, Rita. Acquisition Overview: The Challenges, 2007.

[GAO 04]

Government Accountability Office (GAO). DEFENSE ACQUISITIONS: Stronger Management Practices Are Needed to Improve DoD's Software-Intensive Weapon Acquisitions (GAO Report GAO-04-393). Washington, DC: Government Accountability Office, March 2004.

[GSA 05]

General Services Administration, Department of Defense, & National Aeronautics and Space Administration. Federal Acquisition Regulation. Washington DC: General Services Administration, March 2005.

[IEEE/EIA 98a]

IEEE/EIA. IEEE/EIA 12207.0-1996, Industry Implementation of International Standard ISO/IEC 12207: 1995, ISO/IEC 12207, Standard for Information Technology – Software life cycle processes. New York: IEEE, March 1998.

[IEEE/EIA 98b]

IEEE/EIA. IEEE/EIA 12207.0-1996, Industry Implementation of International Standard ISO/IEC 12207: 1995, ISO/IEC 12207, Standard for Information Technology – Software life cycle processes – Life cycle data. New York: IEEE, April 1998.

[IEEE/EIA 98c]

IEEE/EIA. IEEE/EIA 12207.2-1997, Industry Implementation of International Standard ISO/IEC 12207: 1995, ISO/IEC 12207, Standard for Information Technology – Software life cycle processes – Implementation considerations. New York: IEEE, April 1998.

[INCOSE 06]

International Council on Systems Engineering (INCOSE). Systems Engineering Handbook—A Guide for System Life cycle Processes and Activities, version 3 (INCOSE-TP-2003-002-03). Seattle, WA: INCOSE, June 2006.

[ISO/IEC 95]

ISO/IEC. ISO/IEC 12207: 1995, Information Technology – Software life cycle processes. Geneva, Switzerland: International Organization for Standardization, June 13, 1995.

[ISO/IEC 02]

ISO/IEC. ISO/IEC 15288: 2002(E), Systems Engineering – system life cycle processes. Geneva, Switzerland: International Organization for Standardization, November 1, 2002.

[NIST 06]

Swanson, Marianne; Hash, Joan; & Bowen, Pauline. Guide for Developing Security Plans for Federal Information Systems (NIST SP 800-18, Revision 1). Gaithersburg, MD: NIST Computer Security Division, February 2006.

[OMB 06]

Office of Management and Budget. OMB Circular A-11, Preparation, Submission, and Execution of the Budget. Washington DC: Office of Management and Budget, June 2006.

[USAF 03]

United States Air Force (USAF). National Security Space Acquisition Policy Number 03-01 (NSS 03-01): Guidance for DoD Space System Acquisition Process. Secretary of the Air Force, 2003.

APPENDIX A: SELECTED RESOURCES FOR ACQUISITION BEST PRACTICES

Studies by the Defense Sciences Board and the US Government Accountability Office [GAO 04] identified shortcomings in acquisition products and processes as major reasons for defense software problems. Public law 107-314, Section 804 of the Bob Stump National Defense Authorization Act for FY03, requires all military departments and defense agencies that manage major defense acquisition programs with a substantial software component to implement a software acquisition process improvement program.

These documents all recommend a renewed and persistent emphasis on program management and systems engineering basics. But emerging trends in the nature of what we are acquiring—the increasing prominence of software, the move toward net-centric operations, and changes in technology—mean that the "basics," which were designed with hardware in mind, need to be reinterpreted. The following resources can be used to help acquisition offices understand what they need to do to improve software acquisition in the face of today's trends.

Adams, R. J.; Eslinger, S.; Owens, K. L.; & Rich, Mary A. Software Acquisition Best Practices: Experiences from the Space Systems Domain, Aerospace TR-2004(8550)-1. El Segundo, CA: The Aerospace Corporation, September 2004.

Albert, Ceci & Brownsword, Lisa. Evolutionary Process for Integrating COTS-Based Systems: An Overview (CMU/SEI-TR-2002-009). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, July 2002.

http://www.sei.cmu.edu/publications/documents/02.reports/02tr009.html (document)

http://www.sei.cmu.edu/cbs/epic/ (overview)

Bernard, Tom; Gallagher, Brian; Bate, Roger; & Wilson, Hal. CMMI® Acquisition Module (AM), Version 1.1 (CMU/SEI-2005-TR-011). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, May 2005.

http://www.sei.cmu.edu/publications/documents/05.reports/05tr011.html (document)

http://www.sei.cmu.edu/news-at-sei/features/2005/1/feature-1-2005-1.htm
(overview)

Data & Analysis Center for Software (DACS) Gold Practices Web Site. ITT Corporation, 2006.

Dodson, Kathryn M.; Hofmann, Hubert F.; Ramani, Gowri S.; & Yedlin, Deborah K. Adapting CMMI® for Acquisition Organizations: A Preliminary Report (CMU/SEI-2006-SR-005). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2006.

Software Program Manager's Network (SPMN). 16 Critical Software Practices. Integrated Computer Engineering, Inc., 2005.

USAF. Guidelines for Software Acquisition Management (GSAM), Version 4.0. Hill AFB, Utah: Software Technology Support Center (STSC), February 2003.

APPENDIX B: THOUGHTS ON THE REQUEST FOR PROPOSAL

A key activity in preparing for supplier selection is developing the Request for Proposal (RFP). In negotiated Government acquisitions, the RFP is used to communicate requirements and solicit proposals. Considerable effort is required to prepare a sound RFP, with knowledge drawn from experts in a variety of areas.

In the RFP, the Government must clearly convey software security expectations to prospective contractors. These expectations may include security-related standards, policies, technical and management requirements, activities, plans, processes, reviews, and government access and rights to artifacts and information. The basic framework for an RFP is specified in the Federal Acquisition Regulation (FAR) [GSA 05, Subpart 15.2].

Regarding the technical effort, the RFP usually contains a statement of work or objectives, technical requirements, instructions to prospective contractors on technical topics to be covered in the proposal, proposal evaluation criteria, a list and schedule of deliverables, applicable specifications and standards with tailoring, special provisions related to data access and government reviews, and other information as required.

The remainder of Appendix B identifies basic material that should be included in an RFP for a secure software-intensive system. The material is not meant to be comprehensive and should be supplemented and tailored to fit program needs.

In the RFP, the material below should be reflected in Section L, Instructions to Offerors, Section M, Evaluation Factors for Award, and the Statement of Work. The proposal content submitted in response to Section L is evaluated against criteria specified in Section M. Deliverables should be identified in the Contract Data Requirements List (CDRL) with content and format requirements specified in Data Item Descriptions (DIDs).

General Software Engineering Practices

Ensure the RFP requires offerors to apply robust software engineering practices for all software regardless of origin and to demonstrate in the proposal their intent and ability to do so.

- Require the offeror to apply a robust software development standard (e.g., MIL-STD-498 [DoD 94] or IEEE/EIA 12207 [IEEE/EIA 98a, 98b, 98c], the US implementation of ISO/IEC 12207 [ISO/IEC 95]), tailored to the needs of the program and covering
    - all offeror team members with software responsibility

    - all software, regardless of origin (developed, COTS, reuse, etc.)
- Request delivery and update of a preliminary software development plan (SDP) based on the standard via the Contract Data Requirements List (CDRL).
- If COTS or other non-developmental software (NDS) such as reuse is under consideration, incorporate a thorough evaluation of the COTS/reuse plan.
    - A COTS Usage Risk Evaluation (CURE) can be used to evaluate contractor plans [Carney 03].
    - The Evolutionary Process for Integrating COTS-Based Systems (EPIC) can help the acquirer and developer manage aspects of COTS use [Albert 02].
    - The report Software Development Standard for Space Systems provides sample evaluation criteria for COTS and reuse software products [Adams 04, Appendix B].

Software Security

Specify technical and management requirements and standards for software security, expected contractor support for government-led security reviews and audits, security measures and indicators, and expected government participation in contractor-led security reviews.

- Request evidence that the security requirements can be met given the proposed technical solution.
- Request that the contractor identify and fully define security measures to be analyzed and delivered.

Ensure the RFP requests delivery and update of a preliminary software/system security plan (via the CDRL) covering all offeror team members with software responsibility. Example content for an SSP may be found in [NIST 06]. (Agency-specific guidelines for SSPs also exist.) In addition, the plan should discuss

- development and application of abuse/assurance cases based on security risks documented in previous activities and risks identified by the contractor or acquirer
- identification of security reviews for system and software artifacts (e.g., plans, measures, requirements, architecture and design descriptions, code, and procedures for development, integration, verification, delivery, installation, checkout, certification and accreditation (C&A), and sustainment)
- linkage of security reviews to other reviews in the development and acquisition life cycle models, such as
    - reviews of the software item, the component/element to which it belongs, and the system as a whole

    - reviews associated with spiral anchor points, waterfall-type reviews, peer reviews, or other reviews, depending on the development approach

- a process for handling security-related deficiencies
- processes for dealing with software security for evolving, non-developmental software items (e.g., COTS and reuse), including criteria for initial suitability evaluation and criteria for evaluating and incorporating updates
- a process for continuous management of security risks and elevation of risks to higher levels as appropriate
- development of a security plan for operations, maintenance, and evolution

Access to Deliverable and Interim Artifacts and to Contractor Facilities

Identify government access required to contractor artifacts and facilities for security reviews.

Specify content and delivery schedule and media for software artifacts to be produced during System Acquisition.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0001120