Software Assurance: Five Essential Considerations for Acquisition Officials[1]

Mary Linda Polydys
National Defense University

Stan Wisseman
Booz Allen Hamilton

Software Assurance (SwA) is a key element of national security; it is critical because dramatic increases in business and mission risks are attributable to exploitable software [1]. *A recent Chief Information Office (CIO) Executive Council poll indicated that the top two most important attributes of software are reliable software that functions as promised and software free from security vulnerabilities and malicious code. The acquisition process can be leveraged to achieve these important attributes. As part of the Department of Homeland Security (DHS) and Department of Defense (DoD) SwA initiative, a working group developed a guide,* Software Assurance in Acquisition: Mitigating Risks to the Enterprise *<https://buildsecurityin.us-cert.gov>, for acquisition officials on how to incorporate SwA considerations in key decisions throughout the acquisition process.*

Dependency on information technology (IT) makes SwA[2] [2] a key element of national security. IT in critical information infrastructures is composed of systems, system of systems, and family of systems (SoS/FoS). Most of these systems involve integrating a complex value chain of commercial off-the-shelf (COTS), government off-the-shelf (GOTS), open-source, embedded, and legacy software. Attackers exploit unintentional vulnerabilities or insert intentional vulnerabilities into these software components.

In a 2006 poll taken by the CIO Executive Council on the impact of software flaws, vulnerabilities, and malicious code, respondents indicated that the top two most important attributes of software are *reliable software that functions as promised* (95 percent of respondents) and *software free from security vulnerabilities and malicious code* (70 percent of respondents) [3].

SwA in the Acquisition Process

A broad range of stakeholders now need justifiable confidence that the software which enables their core business operations can be trusted to perform (even with attempted exploitation) and contribute to more resilient operations. In SoS/FoS, multiple software suppliers are usually involved. Therefore, the responsibility for SwA must now be shared by acquisition officials and supply chain constituents – building the assurance case starts with the acquisition process. To that end, acquisition officials[3] involved in the purchase of software services or products have a responsibility to factor in SwA to reduce the risk of exploitable software being passed to users.

However, there is a growing concern that acquisition officials are not aware of this responsibility and are not prepared to exercise SwA due diligence in the buying process. To assist acquisition officials in understanding and exercising SwA due diligence, a guide [4] was developed by a working group (as part of a larger SwA[4] initiative) on how to incorporate SwA considerations in key decisions throughout the acquisition process.

This article provides a summary of five essential SwA considerations that acquisition officials should include in their decision-making. These considerations are extracted or synthesized from the acquisition guide developed by the working group. The acquisition guide provides more detailed discussion and explanation along with additional considerations.

Five Essential SwA Considerations in Acquisition Decision-Making

SwA considerations should be included in each phase of the acquisition process from the initial acquisition strategy and plan, requirements development, contract or purchase, and contract administration through follow-on software support efforts. The objectives of these SwA considerations are to ensure the delivery of *reliable software that functions as promised* and *software free from security vulnerabilities and malicious code*.

Essential Consideration #1 – Build Security In: Create Acquisition Strategies and Plans That Include Essential SwA Considerations

To *build security in*, SwA considerations should be planned from the inception of a software or software-intensive system acquisition through delivery and post-release support. The Federal Acquisition Regulation (FAR) requires that an acquisition plan be developed for all acquisitions and that all plans discuss how agency information security requirements are being met [5]. The Defense Acquisition Guidebook requires program managers to develop an Acquisition Information Assurance (IA) Strategy as part of their Acquisition Strategy [6]. Whether developing a strategy or plan in accordance with the FAR, Defense Acquisition Guidebook, or another directive, SwA should be part of the discussion on how information security requirements are to be met. To that end, the strategies or plans might include a discussion on the participation of SwA subject matter experts in the acquisition process, initial SwA risk considerations, plans for including SwA requirements, SwA considerations in contractor selection, and SwA considerations in contract administration and project management.

Acquisition officials should require the participation of SwA subject matter experts in the acquisition process from planning, requirements development, source selection, contract award through contract administration, and project management. This is essential not only for establishing appropriate SwA requirements, but also in evaluating potential contractors and ensuring that secure software is delivered. Acquisition strategies and plans should state the level of SwA expertise required as well as specific statements of involvement. An example: This acquisition requires support from an SwA subject matter expert. This individual will develop the SwA requirements, evaluate the SwA aspect of proposals, and monitor the assurance case proving the delivery of SwA requirements during contract performance.

Strategies and plans should include an initial discussion on risk management. For information assurance/security, the security category (SC) (based on a range of risk levels) should be included in strategies

and plans. The Federal Information Processing Standard Publication (FIPS Pub) 199 [7] as mandated by the Federal Information Security Management Act (FISMA) of 2002 requires that a security category be designated for each software-intensive system. The DoD Instruction (DoDI) 8500.2 [8] provides security categorization[5] rules for DoD software-intensive systems using Mission Assurance Categories (MAC) and confidentiality levels. The FIPS Pub 199 states that security categories should be based on the mission that the software is to support, the environment in which the mission is performed, and, generally, the kind of information that is generated and maintained to support the mission (e.g., medical, privacy, classified, time sensitive, warfighter combat information, financial, security management, etc.). Security categorization includes an assessment of three security objectives defined in FISMA: confidentiality[6], integrity[7], and availability[8] [9]. Two examples follow:

- **EXAMPLE 1 – From FIPS Pub 199:** A law enforcement organization managing extremely sensitive *investigative information* determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting SC of this information type is expressed as: SC investigative information = (*confidentiality*, HIGH), (*integrity*, MODERATE), (*availability*, MODERATE).
- **EXAMPLE 2 – [NOTIONAL], MAC, and Confidentiality Level:** A system must provide access to sensitive and classified combat support data. There must be uninterrupted service and data availability. The loss of confidentiality and integrity are unacceptable and could include the immediate and sustained loss of mission effectiveness. The resulting MAC and confidentiality level is expressed as: *Confidentiality*: TOP SECRET; *MAC I*: Requires the most stringent of protection measures.

Acquisition strategies and plans should include statements of critical, high-level SwA considerations. These high-level statements guide the ultimate detailed statement of requirements. Acquisition officials developing acquisition strategies and plans should rely heavily on the SwA personnel assigned to the acquisition. Three examples follow:

- **EXAMPLE 1 – COTS Software:** In order to ensure that COTS is consistent with the overall security requirements of the software-intensive system, SwA personnel assigned to this acquisition will provide requirements to ensure delivery of COTS that has specified pre-set security settings. In addition, requirements will mandate that testing of the specified pre-set software be accomplished on the operating system and platform proposed for production.
- **EXAMPLE 2 – Software Development or Systems Integration:** To manage the development and delivery of SwA requirements, an SwA case shall be developed that presents a convincing argument the software will operate in an acceptably secure manner. To support the SwA case, definitive evidence (e.g., processes, procedures, test results, etc.) shall be produced to present a convincing argument that the software will be acceptably secure throughout its life cycle, including termination. The security stakeholders (e.g., accreditors) will evaluate the SwA case in determining that the software will function as expected and be as free of vulnerabilities as possible.
- **EXAMPLE 3 – Generally:** The software shall address the required security properties and functionality, relevant laws, regulations, standards, and other legal and societal requirements. In addition, independent verification and validation (IV&V) shall be performed on the code to determine the software's security posture. This IV&V shall be performed by a qualified SwA IV&V entity.

High-level statements on how SwA is to be considered in the selection of contracts should also be included in acquisition strategies and plans. As an example: Due diligence questionnaires will be used to solicit answers from offerors on their SwA practices. The answers will be part of the evaluation plan.

Lastly, high-level statements should be included in acquisition strategies and plans on how SwA requirements are to be monitored during contract performance, for example: SwA personnel will monitor the delivery of SwA requirements.

Essential Consideration #2 – Require Secure Software: Include SwA Requirements in Software Requirements Document

The security category is the basis for SwA requirements. The FAR requires that federal agencies use FIPS pubs for IT standards and guidance [10]. The FIPS Pub 200 includes guidance on minimum security requirements for federal information and information systems [11]. The National Institute for Standards and Technology Special Publication (NIST SP 800-53) provides specific security control requirements based on security category [12], and the DoDI 8500.2 contains security control requirements based on mission assurance category for the DoD. The guide for acquisition officials includes additional sources for SwA requirements, as well as some examples. Table 1 shows examples of general requirements of SwA that acquisition officials should consider, including statements of work or terms and conditions. Table 2 shows specific requirements of SwA.

Essential Consideration #3 – Be an Educated Consumer: Ask the Right Questions During the Contracting Process

Knowing what to ask and asking the right questions regarding offerors' SwA environments is essential in determining how well offerors' meet business and technical goals for SwA. The guide for acquisition

Table 1: *Examples of General SwA Requirements*

General Requirements
• Definitions relative to SwA for a common understanding.
• A full explanation of the SC.
• Assurance case that addresses the SwA requirements (see more in Essential Consideration #4).
• SwA acceptance criteria (associated with the SwA case).
• SwA risk management that includes a formal program for risk management.
• Consideration for auditing code for security by an independent body.
• Software Architecture that includes SwA components.
• A security test plan that defines the approach for testing SwA requirements.
• Configuration guidelines for all security configuration options.
• Legal responsibilities relative to SwA.
• Qualifications and required SwA training of software personnel.
• Identification of key security personnel.
• Required information relative to foreign ownership, control, or influence.

officials includes sample software due-diligence questionnaires for various types (e.g., COTS only, software integration services, software development, etc.) of software acquisitions. These questionnaires provide the acquisition official a means to gather, in advance, some of the information needed to make a decision about whether it offers the process capabilities to deliver *reliable software that functions as promised* and *software free from security vulnerabilities and malicious code*.

Questionnaires may be used informally or incorporated into a formal process. For example: Informally, the buyer of COTS software may apply the questions to conduct market research into COTS products available to satisfy an organization's software requirements. Formally, the acquisition official may incorporate questions into a Request for Information or Request for Proposal (RFP) as part of a major software-intensive system acquisition. Answers to the questions form a basis for evaluating offers.

Questions in a software due diligence questionnaire may be organized into categories that represent a logical grouping of SwA concerns such as organization background, software production policies, software pedigree, assurance, preventive measures, quality control, operations and support, and service governance. Table 3 lists a partial set of example questions that may be used in the acquisition of custom software development services (the guide includes the comprehensive set of questions).

Essential Consideration #4 – Demand Delivery of Secure Software: Ensure SwA Requirements Are Met During Contract Administration and Project Management

Acquisition officials should ensure that all the SwA requirements are adequately monitored and implemented. This includes work plan management, assurance case management, software risk management, and final acceptance of the software product or service.

Acquisition officials must ensure that SwA requirements are specifically included in a contract work plan and/or work breakdown structure, if required. SwA subject matter experts should be used to ensure that SwA requirements are included in the work plan.

Table 2: *Examples of Specific SwA Requirements*

Specific Requirements
• A server-side software application shall never rely on the client to perform input validation. The server application should always validate any input it receives, regardless of whether that input was previously validated by the client.
• The software application shall verify that the actual results match the expected results criteria.
• The software application shall prevent any entity from performing application functions that entity's authorizations do not explicitly permit it to perform.
• Server/Web service that authenticates based on role or group authentication shall perform individual authentication first.
• Authentication technology shall be implemented based on published open standards.
• Code shall meet organizational and industry standards, conform to a consistent style guideline (code format), and shall be well documented.
• Appropriate security metrics shall be used during security review/audit in the software life cycle to measure the degree to which security criteria/requirements have or have not been satisfied.
• Security testing shall be performed both on individual units/components and on the whole integrated software application.
• Error messages shall not reveal more details than necessary about the software application.
• No software developer *backdoors*, debug interfaces, or unauthorized access paths shall be present in the production version of the software.
• After it goes into production, the software application's security posture shall be periodically reviewed to ensure that new vulnerabilities have not emerged.
• The software application shall continue functioning, possibly in a degraded mode, when subjected to input patterns that indicate a denial of service attack.
• Any COTS software shall be configured in accordance with security configurations specified in the statement of work. The contractor shall provide written assurance that the software operates as intended and as initially configured with each subsequent software release.

Acquisition officials must ensure that the SwA case is managed in accordance with the contract and should be managed as part of the acquisition risk management strategy. The development of an SwA case is an iterative process throughout a system's life cycle and contains a plethora of claims and evidence types not collated or contained together. Therefore, the SwA case must be developed and managed in such a fashion that all evidence is able to be preserved, traced, and accessed. Throughout the acquisition life cycle, SwA case reports – as stipulated in the contract – should be delivered at key project milestones. These reports should be reviewed by appropriate SwA subject matter experts for issues and recommendations. Acquisition officials must ensure that periodic reviews of the SwA case are transparent and any corrective actions are followed to a conclusion prior to acceptance of the case argument. Example issues related to SwA case management during contract performance include the following:

- **Performance.** Is the SwA case development progressing in accordance with contract requirements? Are project technical milestones incorporating SwA case review? Does the SwA case comply with contract requirements, including regulations and certification requirements?
- **Resources.** Has the contractor allocated appropriate, qualified personnel to the task? Is the SwA case being developed with appropriate tools? Is the SwA case budget realistic?
- **Quality.** Is the supplier engaging the right acquisition officials to review the acceptability of the SwA case? Are corrective actions being followed up adequately? Are the contractor's claims, arguments, and evidence sufficiently robust and commensurate with risk?
- **Time.** Is the SwA case development on schedule and fully integrated with software system development?

Final acceptance should be based on the acceptance of the final SwA case. Criteria for acceptance should be explicit and included in the SwA case.

Essential Consideration #5 – Continue SwA for the Life of the Software: Maintain SwA in Follow-On Support

Follow-on support is the logistics tail in the acquisition of software. Additional contracts are often awarded to provide support during this phase. There should be ongoing analyses to ensure that security requirements remain adequate. To that

end, acquisition officials should ensure that the assurance/security requirements implemented and accepted in previous contracts flow to the follow-on contract efforts. Additionally, acquisition officials should ensure that contract language is in place to guide the transition process from an incumbent contractor to a new contractor responsible for follow-on support.

Information systems are typically in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment of the system. Weak change/configuration control procedures can corrupt software and introduce new security vulnerabilities. Therefore, acquisition officials should ensure that strong change/configuration control flows to follow-on contract efforts.

Patches and upgrades make direct changes to software and potentially the configuration of the operating system to which they are applied. Changes may degrade performance, introduce new vulnerabilities, or reintroduce old vulnerabilities. In order to understand patch risks, the patch process must be examined in some detail during the initial acquisition and again when follow-on support contracts are awarded. One of the most common patch failures stems from a lack of encryption and authentication in the implementation phase. Suppliers should provide updates in a secure fashion. There should be no doubt that the source is legitimate and the update's integrity is maintained in transit.

Partial Set of Example Questions
• How does your company use security best practices that are designed to address security concerns in the software development life cycle (SDLC)?
• Are there formal software quality policies in place? How are they enforced?
• What measurement practices and data does your company use to enable realistic project planning, timely monitoring of project progress and status, identification of project risks, and effective process improvement?
• What training does your company offer related to defining security requirements, secure architecture and design, secure coding practices, and security testing?
• Describe the company's policy and process for professional certification of developers and ensuring certifications are valid and up-to-date.
• Are security requirements developed independently of the rest of the requirements engineering activities, or are they integrated into the mainstream requirements activities? Explain.
• What threat modeling process, if any, is used when designing the software? What analysis, design, and construction tools are used by your software design teams? What security design and security architecture artifacts are produced? How are they maintained?
• Does the software development plan include peer reviews for quality and security?
• Are tools provided to help developers verify that the software they have produced is free of defects that could lead to vulnerabilities? What are they?
• Explain how your company ensures that software is able to detect, recognize, and respond to attack patterns in input it receives from human users and external processes?
• Are static or dynamic software security analysis tools used to identify vulnerabilities in the software? If yes, what tools are used? What classes of vulnerabilities are covered?
• Are security-specific regression tests performed during the development process? How broad is the test coverage? How frequently are security-specific regression tests performed?
• What policies and processes does your organization use to verify that software components do not contain unintended, *dead*, or malicious code? What tools are used?
• Does your company perform background checks on members of the software development team? If so, are there any additional *vetting* checks done on people who work on critical application components, such as security? Explain.
• Does your company have formally defined security policies associated with clearly defined roles and responsibilities for personnel working within the SDLC, including work that is subcontracted or outsourced, along with management oversight and enforcement? Explain.

Table 3: *Partial Set of Questions for Custom Software Development Services*

Conclusion

Large numbers of vulnerable software-based systems exist today, in many cases due to the acquisition of vulnerable software. The rampant, worldwide increase in exploitation of software vulnerabilities demands that acquisition officials not only check for acceptable functionality, but also achieve acceptable SwA. Security cannot be *bolted on* after software services and products are delivered. To that end, acquisition officials must become educated consumers in the purchase of secure software, and each phase of the acquisition process must be leveraged to *build security in* to ensure the delivery of *reliable software that functions as promised* and *software free from security vulnerabilities and malicious code.*◆

References

1. President's Information Technology Advisory Committee. Cyber Security: A Crisis of Prioritization. Arlington, VA: National Coordination Office for Information Technology Research and Development, Feb. 2005 <www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf>.
2. U.S. Committee on National Security Systems (CNSS). CNSS Instruction No. 4009, National Information Assurance Glossary. Fort Meade, MD: CNSS, 2006 <www.cnss.gov/Assets/pdf/cn ssi_4009.pdf>.
3. CIO Executive Council. New CIO Executive Council Poll Reveals CIOs Lack Confidence in Software. CIO Executive Council News Bureau, 2006 <www.cioexecutivecouncil.com/nb/>.
4. DoD and D HS. SwA Working Group. Software Assurance in Acqui-sition: Mitigating Risks to the Enter-prise (V1.0). Washington: DoD/ DHS, Mar. 2007 <https://buildsecurityin us-cert.gov>.
5. FAR. Part 7, Acquisition Planning, Subpart 7.105(b)(17). Washington: General Services Administration, DoD, and National Aeronautics and Space Administration, 2005 <www.arnet.gov/far/>.
6. DoD. Defense Acquisition Guidebook. Part 2.3, Systems Acquisition: Acquisition Strategy <http://akss.dau.mil/dag/DoD5000.asp?view=document>.
7. U.S. Department of Commerce. NIST. FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg, MD: NIST, 2004 <http://csrc.nist.gov/publications/fips/index.html>.
8. DoD. DoD Instruction 8500.2, Information Assurance Implementation. E4, Baseline Information Assurance Levels. Washington: DoD,

2003 <www.dtic.mil/whs/directives/corres/ins1.html>.
9. FISMA of 2002. 44 U.S.C., Sec 3532 <www.access.gpo.gov/uscode/title44/chapter35_subchapterii_.html>.
10. FAR. Subpart 11: Selecting and Developing Requirements Documents, Subpart 11.102: Standardization Program. Washington: GSA, DoD, and NASA, 2005 <http://www.arnet.gov/far/>.
11. Department of Commerce. NIST. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems. Gaithersburg, MD: NIST, 2006 <http://csrc.nist.gov/publications/fips/index.html>.
12. Department of Commerce. NIST. NIST SP 800-53, Rev 1, Recommended Security Controls for Federal Information Systems. Gaithersburg, MD: NIST, 2006 (Final Public Draft) <http://csrc.nist.gov/publications/nistpubs/index.html>.

Notes

1. The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, the DoD, or the U.S. government.
2. SwA is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its life cycle, and the software functions in the intended manner (CNSS Instruction No. 4009).
3. The generic term *acquisition official* is used throughout this article to mean the contracting officers or purchasing officials and other members of the purchasing team. Members of the purchasing team may include personnel who develop requirements and statements of work for contracts, contracting officer representatives to include contracting officer technical representatives, or program/project managers.
4. In 2003, the DoD launched an SwA initiative led by Joe Jarzombek. This was joined in 2004 by the DHS to address concerns of poor-quality, unreliable, and non-secure software. In March 2005, Jarzombek moved to DHS as the Director for SwA, National Cyber Security Division (NCSD). He provides the leadership in the collaborative SwA efforts. Several working groups (with members across government agencies, industry, and academia) were established. The initial working groups for DHS including the following:
   - Software technology, tools, and product evaluation.
   - Software acquisition.
   - Software processes and practices.
   - Software workforce educational and training.

   The goal of the SwA Acquisition working group is to look at how to enhance software supply chain management through improved risk mitigation and contracting for secure software. The overwhelming recommendation of the group is the development of a guide that provides due-diligence questionnaires, sample templates, and sample language that could be used in statements of work, RFPs, and contracts.
5. The FISMA of 2002 requires the development of security categorization standards. The security categories are the basis for establishing information security requirements based on a range of risk levels. See FIPS Pub 199 for security categorization of information and information systems that form a basis for confidentiality, availability, and integrity requirements. Also see DoD 8500 policies regarding security categorization-mission assurance categories. The DoD has three defined mission assurance categories that form the basis for availability and integrity requirements. Confidentiality requirements are based on the security classification of information.
6. ... *preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information* [44 U.S.C., Sec. 3532]. A loss of *confidentiality* is the unauthorized disclosure of information.
7. … *guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity* [44 U.S.C., Sec. 3532]. A loss of *integrity* is the unauthorized modification or destruction of information.
8. … *ensuring timely and reliable access to and use of information* [44 U.S.C., Sec. 3532]. A loss of *availability* is the disruption of access to or use of the software-intensive system.

About the Authors

Mary Linda Polydys is currently the Department Chair of the Information Operations and Assurance Department, Information Resources Management, National Defense University and co-chairs the DHS NCSD SwA working group. For more than 33 years, she has provided the U.S. government expert services in information security and assurance education, information technology acquisition and project management, enterprise architecture, and data management. Polydys has a bachelor's degree in decision sciences and a master's degree in information systems from George Mason University.

Information Resources Management College
National Defense University
FT Lesley J. McNair,
Marshall Hall
Washington, D.C. 20319
Phone: (202) 685-3889
Fax: (202) 685-3974
E-mail: polydysm@ndu.edu

Stan Wisseman is a senior associate at Booz Allen Hamilton and has 22 years of experience in the IA field. He currently co-chairs the DHS NCSD SwA Acquisition working group, leads the IA team for the U.S. Department of Transportation's Vehicle Infrastructure Integration project, and oversees a SwA practice. Wisseman holds Certified Information Systems Security Professional, Certified Information Security Manager, and Project Management Professional (PMP) certifications. He has a bachelor's degree in computer science from Texas A&M University and a master's degree in engineering management from Santa Clara University.

Booz Allen Hamilton
8251 Greensboro DR
McLean, VA 22102
Phone: (703) 902-4673
Fax: (703) 902-3281
E-mail: wisseman_stan@bah.com