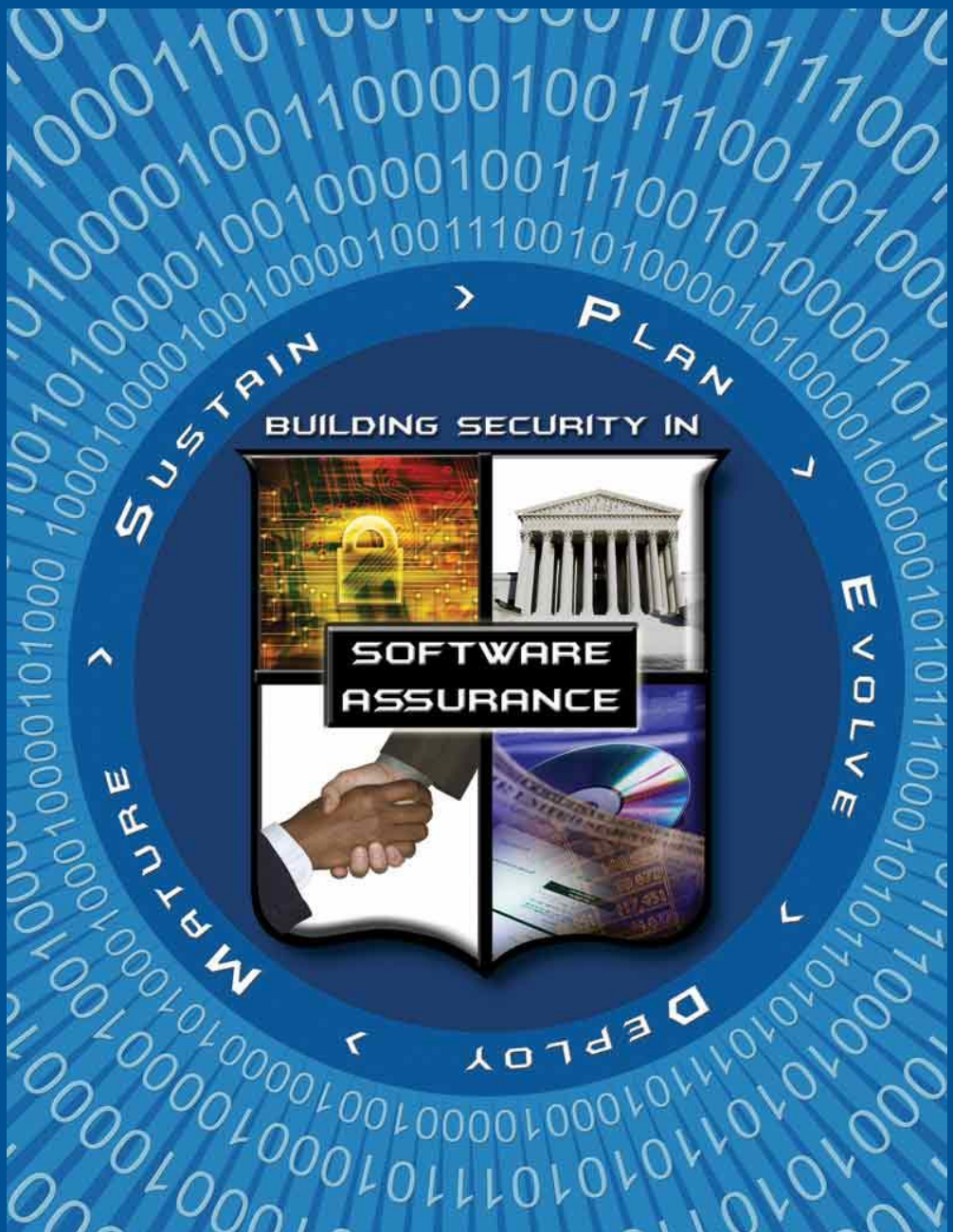
Software Assurance in Acquisition and Contract Language

Software Assurance Pocket Guide Series:
Acquisition & Outsourcing, Volume I
Version 1.1, July 31, 2009



Software Assurance (SwA) Pocket Guide Resources

This is a resource for 'getting started' in selecting and adopting relevant practices for delivering secure software. As part of the Software Assurance (SwA) Pocket Guide series, this resource is offered for informative use only; it is not intended as directive or presented as being comprehensive since it references and summarizes material in the source documents that provide detailed information. When referencing any part of this document, please provide proper attribution and reference the source documents, when applicable.

This volume of the Software Assurance Pocket Guide series focuses on contract language for integrating software security in the acquisition life cycle, including sample SwA Request for Proposal (RFP)/Contract language. Buyers and evaluators of software and suppliers can gain security risk-based insight. They can put suppliers on notice that consumers are concerned about software security and the risks to their organizations that are attributable to exploitable software.

At the back of this pocket guide are references, limitation statements, and a listing of topics addressed in the SwA Pocket Guide series. All SwA Pocket Guides and SwA-related documents are freely available for download via the SwA Community Resources and Information Clearinghouse at https://buildsecurityin.us-cert.gov/swa.

Acknowledgements

The SwA Forum and Working Groups function as a stakeholder mega-community that welcomes additional participation in advancing software security and refining SwA-related information resources that are offered free for public use. Input to all SwA resources is encouraged. Please contact Software.Assurance@dhs.gov for comments and inquiries.

The SwA Forum is composed of government, industry, and academic members. The SwA Forum focuses on incorporating SwA considerations in acquisition and development processes relative to potential risk exposures that could be introduced by software and the software supply chain.

Participants in the SwA Forum's Acquisition & Outsourcing Working Group collaborated in developing the material used in this pocket guide as a step in raising awareness on how to incorporate SwA considerations throughout the acquisition process.

Information contained in this pocket guide is primarily derived from ***"Software Assurance in Acquisition: Mitigating Risks to the Enterprise"*** available through the SwA Community Resources and Information Clearinghouse at https://buildsecurityin.us-cert.gov/swa/acqact.html. The full document was also co-developed with representatives from the Information Resources Management College (IRMC) http://www.ndu.edu/irmc/ and published through the National Defense University Press; so a copy can be accessed at http://www.ndu.edu/inss/press/NDUPress_Occasional_Papers.htm.

Special thanks to the Department of Homeland Security (DHS) National Cyber Security Division's Software Assurance team who provided much of the support to enable the successful completion of this guide and related SwA documents.

Overview

Software vulnerabilities, malicious code, and software that does not function as promised pose a substantial risk to the Nation's software-intensive critical infrastructure that provide essential information and services to citizens. Minimizing these risks is the function of Software Assurance (SwA). Software assurance is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that it functions in the intended manner [CNSSI No. 4009].

Often the common practice in acquisition is to accept software that satisfies functionality with little regard for specifying, determining or assuring security properties—increasing the risk exposure to users. Many purchasing organizations and acquirers continue to accept software riddled with exploitable flaws and other security vulnerabilities. This, in part, may be due to acquisition policies and procedures that do not ensure that security is a main concern of software.

Software Vulnerabilities Side Effects

- Unintentional errors leading to faulty operations,
- Destruction of information or major disruption of operations,
- Insertion of malicious code,
- Theft of sensitive, personal or classified information, and
- Changed product.

In addition, acquirers may not be aware of the increased life cycle costs and increased risk exposure to the organization attributable to software that is not secure. Purchasing secure software might entail moderate upfront costs to the acquisition project (especially in dealing with suppliers who have not incorporated security in their development processes); however, the price paid in lost time and resources to continually fix or patch a vulnerable software component can run as much as three times the initial purchase of secure software. Many organizations fall behind in properly patching vulnerable software due to those exponential costs, leaving them exposed to attack. Dangers may be attributable to software errors or other vulnerabilities to include the unknowing acceptance of software that contains malicious code.

A broad range of stakeholders now needs justifiable confidence that the software that enables their core business operations can be trusted to function as expected (even with attempted exploitation) and can contribute to more resilient operations. Therefore, the responsibility for SwA must be shared not only by software suppliers in the supply chain but also by the acquirer in the supply chain who purchase the software. There is a concern, however, that acquirers are not aware of this responsibility and are inadequately prepared to support SwA in the acquisition process.

In 2003, the U.S. Department of Defense (DOD), joined by the Department of Homeland Security (DHS), launched a SwA initiative to address SwA concerns of poor quality, unreliable, and non-secure software. The SwA Forum's Acquisition & Outsourcing Working Group, consisting of representatives from government, industry, and academia, was established to

address how to leverage the acquisition process to influence SwA in the supply chain. To that end, the SwA Forum's Acquisition & Outsourcing Working Group created this pocket guide to inform acquisition officials on how to influence SwA in software supply chain management by leveraging and including SwA considerations in the acquisition process.

This pocket guide provides information on contract language for incorporating SwA throughout the acquisition process from the acquisition planning phase to contracting, monitoring and acceptance, and follow-on phases. For each phase, the material covers SwA concepts, recommended strategies, and acquisition management tips.

Why You Need Software Assurance

Software assurance is a key element of national security and homeland security. It is critical because dramatic increases in business and mission risks are attributable to exploitable software. Software vulnerabilities jeopardize intellectual property, consumer trust, business operations and services, and a broad spectrum of critical infrastructures, including everything from process control systems to commercial software products.

To ensure the integrity of business operations and key assets within critical infrastructures, software must be reliable and secure. A Chief Information Officer Executive Council™ poll found 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 main objective of software assurance is to ensure that the processes, procedures, and products used to produce and sustain the software conform to all requirements and standards specified to govern those processes, procedures, and products.

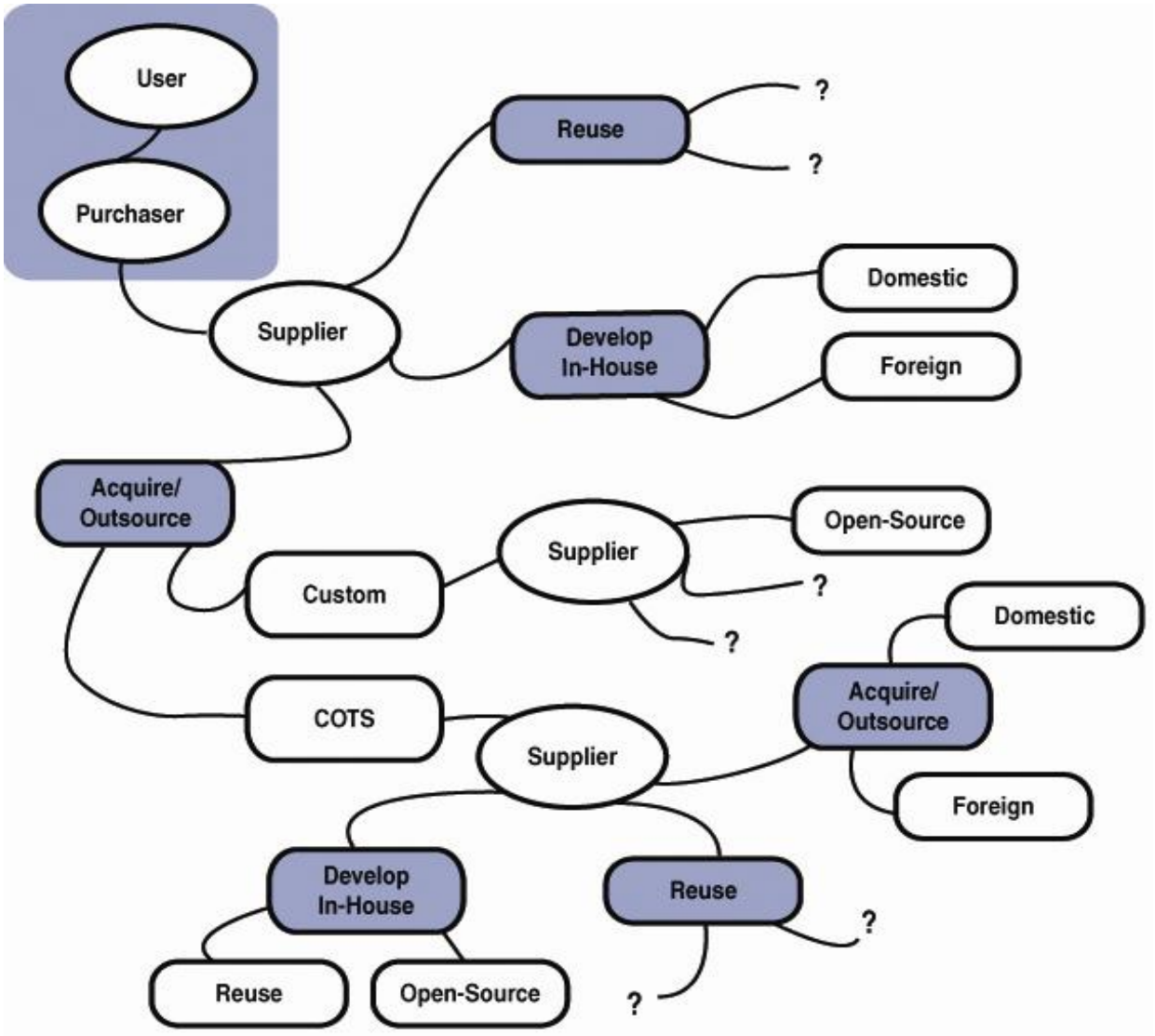
SwA Drivers:

- The Software Development Life Cycle (SDLC) provides opportunities for poor software design and malware insertion that can lead to exploitation;
- Commercial Off The Shelf (COTS) products reliance on foreign and non-vetted domestic suppliers;
- Lack of information on suppliers' processes' capabilities, and;
- Off shoring requires more comprehensive domestic strategies to mitigate risks.

Both research and "real world" experience indicate that correcting weaknesses and vulnerabilities as early as possible in the software's life cycle is far more cost-effective over the lifetime of the software than developing and releasing frequent patches for deployed software.

The software supply chain consists of (but is not exclusive to) the following: the acquirers in industry and government, information assurance personnel supporting acquisition managers, decision makers for software procurements (including program/project managers and requirements personnel), prime contractors and subcontractors in their supply chain, and software suppliers. Figure 1 illustrates a few potential paths that software can take.

Figure 1- Potential Software Supply Paths



Purpose and Scope

The ***purpose*** of this pocket guide is to provide information and increase awareness on how to incorporate SwA considerations in key decisions when acquiring software products and services by contract. The bottom line is to "build security in" and incorporate SwA considerations throughout the software acquisition process. This pocket guide may also be used as a foundation for training and educatic

Figure 2 - Scope

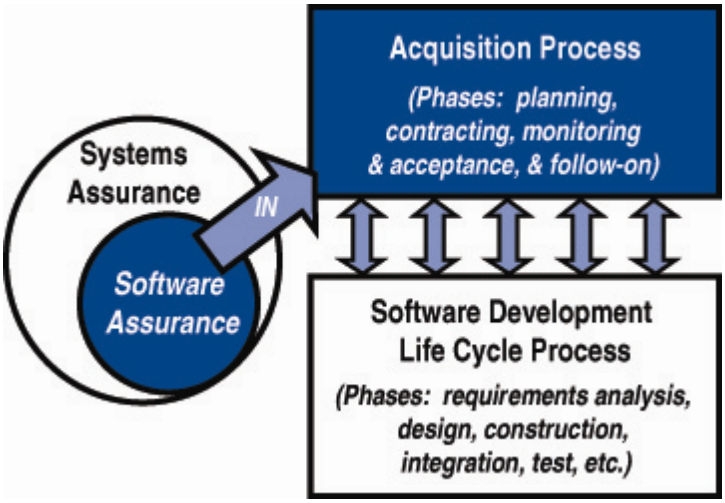


Figure 2 depicts the scope of this pocket guide which addresses SwA considerations when acquiring software products and services by contract (also called the acquisition process). This pocket guide is written from an acquisition process perspective (activities leading to the award and monitoring of contracts) versus the software development life cycle process perspective (technical activities involving requirements analysis, construction of the software solution, testing, etc.). These processes interact during the life of a contract because technical activities are normally addressed in a contract work statement.

In addition, as noted in Figure 2, this guide addresses the SwA perspective versus a system assurance perspective, although, at times, SwA considerations may overlap with system assurance considerations. For a system assurance perspective, refer to the National Defense Industrial Association [NDIA], System Assurance Committee efforts. This pocket guide is NOT an exhaustive coverage of SwA considerations when acquiring software products and services by contract.

Resources:

- "Software Development Security: A Risk Management Perspective," in *The DOD Software Tech News—Secure Software Engineering* 8, no. 2 (Rome, NY: Data and Analysis Center for Software, July 2005).
- The U.S. President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization*, February 2005, available at http://www.nitrd.gov/pitac/reports/index.html.
- Global Information Technology Working Group, Committee on National Security Systems report, CNSS–145–06, November 2006.

Audience: Acquirers

This is a high level guide for anyone, both government and private sector, involved in the management of acquisition and/or acquisition of software products or services by contract, including work that is outsourced or subcontracted. The generic term the "acquirers" is used throughout this guide to mean executives, managers, and members of the acquisition team. Members of the acquisition team perform a wide variety of functions.

Lastly, although this is a high-level guide for acquirers, it may also be used by the supplier team (e.g., prime contractors, integrators, and subcontractors in the supply chain) of software products or services to facilitate their understanding of SwA requirements that acquirers may request.

Acquisition Functions

- Developing requirements, plans, and strategies for contract(s),
- Developing and issuing Requests for Proposals (RFPs),
- Evaluating proposals,
- Negotiating and awarding contracts,
- Monitoring contract performance, and
- Accepting delivery of the software product or service.

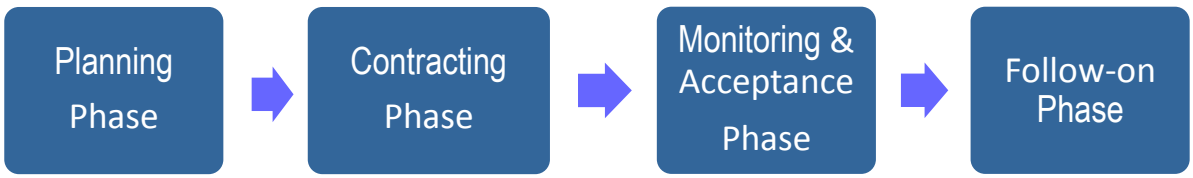
Members of the team may hold positions such as

- developers of requirements (may be systems/software engineers),
- contracting officer representatives (CORs) and contracting officer technical representatives (COTRs),
- contracting officers and specialists,
- procurement personnel,
- program/project managers, or
- supervisors of the above.

Acquisition Process

This pocket guide is organized around the major phases of a generic acquisition process. Figure 2 depicts the relationship of these phases to those of several other processes. Figure 3 depicts the sequence of the planning, contracting, monitoring and acceptance, and follow-on phases of the software acquisition process.

Figure 3 - Generic Software Acquisition Process



Planning Phase

This phase begins with (1) needs determination for acquiring software services or products, identifying potential alternative software approaches, and identifying risks associated with those alternatives. This set of activities is followed by (2) developing software requirements to be included in work statements; (3) creating an acquisition strategy and/or plan that includes identifying risks associated with various software acquisition strategies; and (4) developing evaluation criteria and an evaluation plan. SwA considerations are discussed for each of the major activities. See the ***"Software Supply Chain Risk Management and Due-Diligence"*** pocket guide where the development and use of SwA due-diligence questionnaires are discussed.

Needs Determination - During the needs determination process, an organization assesses its mission to determine if there are problems in mission performance that could be solved by a software solution. This is followed by an assessment of alternative software-based solutions. Determining the need to acquire software products or services (including software-intensive systems) is the first step in laying the groundwork for full development of software requirements, including SwA requirements.

Risk assessment (synonymous with risk analysis) is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.

Risk Assessment Questions

- What is the value of the software in dollars to protect?
- What software assets need to be protected and why, consequences?
- What is the impact of software unpredictability?
- How is residual risk determined and managed?
- What are the potential adverse conditions to be prevented and managed?

An initial risk assessment helps determine the security category, baseline security controls and assurance case required for the acquired software. The acquirer should ask and have answered all of the risk assessment questions.

Alternative Software Approaches - When considering alternative software approaches, acquisition officials and application owners should seek to reduce or manage the risks identified in the initial risk assessment. The steps are to:

- Evaluate alternatives for treatment of risks (accept, mitigate, avoid, transfer, share with a third party [such as a supplier]).
- Identify protection strategies (security control objectives and controls) that reduce risks to levels that are within acceptable tolerances. Controls can be deployed to reduce likelihood and impact.
- Identify potential tradeoffs between reducing risk, increased costs, and decreased operational effectiveness.
- Identify approaches for managing residual risks that remain after protection strategies are adopted.

Alternative software approaches may include one or more software types or services, i.e. COTS open-source, COTS proprietary, GOTS, Custom, Hosted Applications, etc. Each software type or service can introduce its own risks. The due-diligence questionnaires in the ***"Software Supply Chain Risk Management and Due-Diligence"*** pocket guide are broken up into software types/services since SwA concerns can vary by type or service.

SwA Requirements - The security category provides a basis for SwA requirements. In the Federal Government, the security category facilitates the selection of security controls (requirements) and other assurance requirements. The security controls mandated in Federal regulation are a minimum or baseline, and are not exhaustive list to address SwA. Other security and assurance requirements should be identified as required to reduce risk to an acceptable level. Sample SwA requirements language is provided in later sections of this pocket guide.

Resources:

- Federal Information Processing Standard (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
- National Institute of Standard and Technology (NIST) Special Publication 800–53, Recommended Security Controls for Federal Information Systems.
- Department of Defense Instruction (DODI) 8500.2, Information Assurance (IA) Implementation.
- Office of Management and Budget (OMB) Memorandum M–07–18, Ensuring New Acquisitions Include Common Security Configurations, 1 June 2007.

Acquisition Strategy - Acquirers may develop an acquisition strategy, acquisition plan, or both. They should refer to their organization's policy on developing strategies and plans. Acquisition strategies and plans precede the actual purchase. These strategies and plans provide a description of roles and responsibilities, a roadmap for completing actions and milestones, and a discussion for including special considerations in the purchase and implementation of products and/or services. Software assurance should be addressed in those strategies or plans. As a Federal Government example, Federal Acquisition Regulation (FAR) 7.105(b) (17) requires that plans discuss how agency information security requirements are to be met. In DOD, the Defense Acquisition Guidebook, Part 2, requires program managers to develop an acquisition information assurance (IA) strategy describing how IA/security requirements are to be incorporated. How SwA requirements are to be met should be included as part of how the IA/security requirements are met and acquirers should include SwA considerations in strategies and plans.

Acquisition Plan SwA Considerations:

- Vendor SwA Expertise,
- Initial Security Category,
- SwA Requirements,
- SwA Considerations in Contractor Selection,
- SwA Considerations in Contract Administration and Project Management, and
- Plans for Independent Testing.

Evaluation Plan - This activity involves creating a plan for evaluating proposals submitted in response to a solicitation and the criteria that will be used to evaluate the proposals. The evaluation plan describes the process by which proposals are secured and evaluated. SwA criteria should be included in the solicitation, and the evaluation plan must describe how to evaluate the products and services against the criteria. This includes discussing the timing of the evaluation and any measures that can be used to support the evaluation process.

Evaluation Criteria - SwA depends on people and organization, process maturity, and technology working together to be effective. Therefore, evaluation criteria should be developed to include those (people and organization, process maturity, and technology) broad categories. Criteria may be qualitative, quantitative, and/or "go/no-go." Qualitative and quantitative criteria are often evaluated using a scorecard method. The evaluation plan should describe how to determine the scores. The "go/no-go" criteria are evaluated based on whether the proposal satisfies the criteria. In the case where a proposal does not meet the criteria, the proposal is normally eliminated from future consideration for awarding a contract. SwA due-diligence questionnaires can be a means for gathering information to evaluate quantitative, qualitative, and/or "go/no-go" SwA criteria.

SwA Due-Diligence Questionnaires - The software assurance due-diligence questionnaires can assist acquirers in obtaining additional information about the software and its supplier. In this context, due-diligence involves taking all "reasonable steps" necessary to ensure that a software-intensive system not only meets business and technical requirements, but also addresses SwA concerns. The intent is to inform acquirers of potential risks associated with the software they are considering for purchase. The questionnaires are a means for gathering relevant information to support decision-making versus being a decision-making tool. Expertise in software, acquisition, and IA—as well as common sense—is critical in making smart decisions on acquiring trustworthy software. Questions should be posed by, and

responses assessed by, knowledgeable SwA experts or other appropriate functional experts. Sample due-diligence questionnaires are available for download from the Software Assurance Community Resources and Information Clearinghouse web site at https://buildsecurityin.us-cert.gov/swa.

Contracting Phase

The contracting phase includes three major activities: (1) creating/issuing the solicitation or RFPs with a work statement, instructions to offerors/suppliers, terms and conditions (including conditions for acceptance), prequalification considerations, and certifications; (2) evaluating proposals submitted in response to the solicitation or RFP; and (3) finalizing contract negotiation to include changes in terms and conditions and awarding the contract. Software risks are addressed and mitigated through terms and conditions, certifications, evaluation factors for award, and risk mitigation requirements in the work statement.

Recommended Work Statement SwA Requirements:

- Trustworthy software definitions,
- Security category description,
- Assurance plan,
- Security requirements assurance case,
- Software implementation safety and security risk management plan,
- Consideration for code auditing, and
- Software description and architecture.

Work Statement - Acquirers usually prepare the work statement. The FAR states that "agencies shall include the appropriate information technology security policies and requirements in all acquisitions for information technology" (FAR Subpart 39.101(d)). Acquirers should consider including software assurance requirements in a work statement.

Instructions to Offerors /Suppliers - In response to an RFP, suppliers must submit information that provides objective evidence of their ability to perform the SwA aspects of the work statement and terms and conditions. Clear instructions must be included in the RFP on what suppliers must submit for evaluation, including instructions pertaining to onsite evaluation, if required by the RFP. Instructions to suppliers explain how to answer the due-diligence questionnaire and what to submit in an initial assurance case and software description.

Terms and Conditions - Additional SwA requirements may be included in terms and conditions. Whether to include an item in the work statement or as a term or condition depends on the policies and structure of the acquisition organization. Selecting terms and conditions would depend on the type of software to be acquired. Because prime suppliers often subcontract software services, terms and conditions should be worded in such a way to ensure that they flow down to all levels of subcontracts.

Certifications - Certifications may also be a way to provide assertions of software trustworthiness when information may be too costly to compile or too voluminous for proposal evaluation. Certifications provide assertions by offerors of existing conditions or compliance in certain requirements. Using certifications shifts the burden of compliance to the suppliers.

Prequalification - Acquirers should consider prequalification. Prequalification can be done to evaluate organizational capabilities or other technical management capabilities. As a word of caution, there should always be additional evaluation for the unique SwA requirements of each acquisition.

Proposal Evaluation - Acquirers should ensure that SwA Subject Matter Experts (SMEs) are used to evaluate each proposal to determine the level of understanding of the SwA requirements. This includes an evaluation of the evidence provided to support answers to the due-diligence questionnaire.

Proposals have multiple components that should be weighed separately and then combined to provide an overall score. An example of three components may be management, technical (includes SwA), and price. All three should have weighted criteria to result in a numerical score.

Contract Negotiation and Contract Award - The evaluation results in the selection of the best proposals for contract negotiation. During negotiations, the acquirers and suppliers negotiate on requirements, terms, and conditions. It is important that the give-and-take on SwA requirements, terms, and conditions does not compromise the ultimate assurance goals or critical assurance goals. Suppliers may push back on the SwA requirements because they may not be fully competent to do the job or be willing to take the risk. Acquirers may find that suppliers may overbid because of perceived risk and doing something they have never done. Acquirers should consider "share in savings" arrangements (savings as a result of implementing SwA requirements as stated). The sharing includes not only costs and benefits but also the willingness to afford the supplier more time to engage in the education and training that is needed. An alternative would be to consider a contract type that shifts the burden of some of the risk to the acquirer and/or provide additional cost or performance incentives [see FAR Subpart 16.1 and FAR Subpart 16.3 for incentive contracts].

When awarding the contract, acquirers must ensure that all SwA agreements made during negotiation are incorporated into the contract when it is awarded. Negotiated agreements are sometimes overlooked when drafting the final contract award.

Monitoring and Acceptance Phase

The monitoring and acceptance phase (may also be called contract administration phase) involves monitoring of the supplier's work and accepting the final service or product. This phase includes three major activities: (1) establishing and consenting to the contract work schedule, (2) implementing change (or configuration) control procedures, and (3) reviewing and accepting software deliverables. During the monitoring and acceptance phase, software risk management and assurance case deliverables must be evaluated to determine compliance in accepted risk mitigation strategies as stated in the requirements of the contract.

Contract Work Schedule - The contract work schedule should include very specific timelines for delivering SwA requirements. If a work breakdown structure (WBS) is used, acquirers should ensure that SwA deliverables are identified in it.

Change Control - The change control procedures for a software-intensive system should ensure that SwA requirements are not compromised when changes are requested. Each change control request should include a specific section that addresses the impact of the requested change on SwA requirements. Change or configuration control of SwA requirements is managed as part of assurance case management.

Review and Acceptance of Software Deliverables - During this activity, examples of deliverables are the risk management plan for software, assurance case, and test documentation. Acceptance criteria should be explicit, measurable, and included in the assurance case or in the terms and conditions. See section "*Sample RFP/Contract Language: General Audience"* in this pocket guide for sample terms and conditions that include acceptance conditions. The SwA SMEs should review each software deliverable and analyze test results produced by the contractor or independent tester to ensure that SwA requirements are met. Acquirers should not accept the service or product until the SwA expert finds the requirements acceptable.

Risk Management - The FAR states: "Contracting and program office officials are jointly responsible for assessing, monitoring and controlling risk . . .during program implementation. . .Appropriate techniques should be applied to manage and mitigate risks during the acquisition of information technology." An initial risk assessment is performed during the acquisition planning process. This risk assessment results in the identification of a security category, which may be further refined during this phase of the acquisition process. Acquirers and suppliers who are responsible for implementation should create a plan for managing risks associated with the security category. The plan should include an identification of SwA risks, plans for mitigating those risks, associated measures, and plans for continually assessing those risks.

On-line Resources:

» *Federal Acquisition Regulation (*FAR). at http://www.arnet.gov/far/index.html.

Assurance Case Management - Acquirers must ensure that the assurance case is implemented in accordance with established requirements and approved project plans, in particular the assurance plan approved for use in the contract. (Note: If an assurance plan is not used, special attention should be paid to supplier processes and products on the project to give users and other stakeholders the confidence that software assurance has been considered in the product development.)

The assurance case must be managed as part of the risk management strategy for the acquisition. If the assurance case is used to demonstrate achievement of the security and dependability properties of the software system, then the acquirers must take appropriate steps to manage the assurance case's development and acceptance into operational service.

All elements of any project management methodology that acquirers use are affected by development and management of an assurance case. The text box labeled ***Assurance Case Management Components*** on the right lists common project elements (or principles) that contribute to the delivery of an assured software–intensive system and explain how they are crucial for a project manager to deliver a robust and complete assurance case for transition to operations.

Assurance Case Management Components

- Project Management Reviews,
- Risk Management Strategy and the Assurance Case,
- Scope Management,
- Schedule Management,
- Cost Management,
- Human Resource Management,
- Data and Configuration Management,
- Quality Management, and
- Assurance Case Measures.

Independent Software Testing - Acquirers should consider independent software testing. The completed software product is provided to an independent accredited software testing organization (International Organization of Standards (ISO)/ International Electrotechnical Commission (IEC) 17025) to verify that not only functional requirements but also SwA requirements are met. The testing organization can test in either a white or black box scenario depending on need.

Follow-on Phase

The follow-on phase involves maintaining (often called sustainment) the software. This phase includes two major activities: (1) sustainment (includes risk management, assurance case management, and change management) and (2) disposal or decommissioning. During the follow-on phase, software risks must be managed through continued analysis of the assurance case and should be adjusted to mitigate changing risks.

Sustainment (or Post-release Support) - Care should be taken to enforce terms and conditions contained in the initial contract that apply to the service or product. A provision for maintaining a specific security configuration of COTS software is a good example.

Additional contracts are often awarded to provide support during this phase. Analyses should be ongoing to ensure that security requirements remain adequate. To that end, acquirers should ensure that the assurance/security requirements implemented and accepted in previous contracts flow to the follow-on contract efforts. This includes continuous monitoring of the assurance case (including risks) and making appropriate adjustments in using and maintaining software to update the assurance case and mitigate risks.

Maintenance Activities

- Executing configuration control of executable product baselines;
- Performing software modification revalidation and integration;
- Conducting problem analyses reconstruction, review, and acceptance;
- Predicting software performance (defect density trending and so forth);
- Monitoring the engineering environment to ensure that it is fully documented and validated (or security accredited);
- Maintaining organization policies and processes for security and safety fixes; and
- Maintaining and executing software migration, data migration, and decommissioning policies and procedures.

A formal assurance case and risk management process should be maintained. This process should include continuous threat analyses and vulnerability assessments. In addition,

review and adjustment of mitigation strategies should occur regularly. A full-time assurance case/risk management team should be considered. If this team is contracted as a service, suppliers must be adequately trained and cleared. Because acquirers should not abrogate their security responsibility wholly to suppliers, trained and cleared SwA experts inside acquirers organizations must be a part of that team.

Risk Management - Risk management must continue after the implementation and acceptance phase. This includes updating the risk management plan. In this volatile information environment, new risks inevitably emerge. As a result, the security category may be further refined during this phase. In addition, SwA risks and strategies for mitigating those risks are likely to change as well. Measures should be used to provide insights into the changes in the risk environment and into impacts of risk mitigation strategies.

Assurance Case Management/Transition to Operations - The continual assurance (and certification) of software-intensive systems in the follow-on phase presents some unique challenges:

- Many software systems are not architecturally or detail designed for modifications, and enhancements are made many years after procurement.
- System and software engineering change control mechanisms can lack traceability, rigor, and documentation.
- Adequate assurance case maintenance processes may not be in place before the system transitions to operations.
- Support personnel turnover causes loss of corporate knowledge about maintaining and ensuring integrity of legacy software.
- Many software support agencies are not the original software manufacturer and do not employ the same methods, tools, and processes used in development.
- During previous acquisition phases, the software transition planning is typically poorly executed and "assurance concerns" are "thrown over the fence" for follow-on maintenance.

During implementation, acquirers and suppliers must identify the assurance requirements for the follow-on phase to maintain integrity and dependability in the system. These requirements are defined in greater detail as the product's transition to operations nears and the software risk exposure is clearer. Any claims, evidence, arguments, and assumptions in the assurance case that are neither consistent nor based on a known material state of the "in service" software weaken the credibility of the evidence and elevate the safety and security risk in using the system. The authority responsible for the assurance case maintenance must keep an auditable record of his or her decisions to include justification for changes made to the assurance case.

Change Management - Information systems are typically in a constant state of migration with upgrades to hardware, software, or firmware, and with possible modifications to the surrounding environment of the system. Weak change control procedures can corrupt software and introduce new security vulnerabilities.

Change management invokes revalidation efforts. When any hardware or software component is changed, the extent of revalidation must be evaluated. Generally, when hardware components are replaced like for like, no revalidation is necessary. When new hardware is used, the system must be revalidated to ensure no detrimental effects occur. When software is patched or upgraded, revalidation is always required.

Patches and upgrades make direct changes to software and potentially to the operating system configuration to which they are applied. Changes may degrade performance, introduce new vulnerabilities, or reintroduce old vulnerabilities. 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 and acceptance 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.

Disposal or Decommissioning - Disposal or decommissioning policies and procedures are often overlooked. Many organizations do not have such policies and procedures. Acquirers' organizations should ensure that policies and

procedures are developed and followed to ensure the safe and secure disposal or decommissioning of software, along with ensuring data are destroyed or migrated safely and securely. When a software-intensive system is retired or replaced, the data must be migrated by validated means to the new software-intensive system.

Sample RFP/Contract Language for Secure Software

The contract language contained in this pocket guide is offered only as an example. The authors and contributors make no warranties about using any of this language. The language should be used by acquirers as suggestions and should be tailored as appropriate in accordance with the acquirers' legal authorities and organizational policies and procedures. Language similar to the following can be used to communicate requirements and terms and conditions in Requests for Proposal and/or contracts. As used in this section, the terms contractor and offeror are synonymous with the term supplier.

Resources for Procurement, Acquisition and Outsourcing

OPEN WEB APPLICATION SECURITY PROJECT (OWASP) CONTRACT ANNEX - The OWASP provides a sample contract Annex that can be used as a framework for discussing expectations and negotiating responsibilities between acquirers (clients) and developers. The contract Annex is intended to help software developers and their clients negotiate and capture important contractual terms and conditions related to the security of the software to be developed or delivered. The language in the Annex may be used whole, in part, or as tailored to communication requirements in a work statement or stated as terms and conditions. The Annex can be obtained from: http://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex.

APPLICATION SECURITY PROCUREMENT LANGUAGE - *Application Security Procurement Language* is freely available at http://www.sans.org/appseccontract. These guidelines incorporate substantial language from the OWASP Secure Software Contract Annex. These help enable buyers of custom software to more explicitly make code writers responsible for checking the code and for fixing security flaws before software is delivered.

The sample procurement language offers General provisions that address Personnel, Security Training, Background Checks of Developers, Vulnerabilities, Risks and Threats, and Application Development. It provides procurement language to address the DEVELOPMENT ENVIRONMENT, including: Secure Coding, Configuration Management, Distribution, Disclosure, and Evaluation. It offers sample procurement language to cover TESTING, including: test planning, source code reviews, as well as vulnerability and penetration tests. The sample procurement language provides provisions for addressing Patches and Updates, along with notification and testing of those modifications to the software. It offers provisions for Tracking Security Issues. It has provisions for a vendor to self-certify and provide a "certification package" that establishes the security requirements, design, implementation, and test results were properly completed and all security issues were resolved appropriately. It offers provisions for specifying the developer is to warrant that the software shall not contain any code that does not support a software requirement and weakens the security of the application, including computer viruses, worms, time bombs, back doors, Trojan horses, Easter eggs, and all other forms of malicious code. It offers procurement language for how security issues will be investigated.

Sample RFP/Contract Language: General Audience

Anyone contracting for software or outsourcing software related services should take advantage of sample instructions to suppliers and work statements, along with language for acceptance criteria, security controls, secure configuration, and certifications for originality and security.

SAMPLE INSTRUCTIONS TO POTENTIAL SUPPLIERS - The following is generic language to include in solicitations. This language provides instructions to potential suppliers on what they must submit with their offer. The information submitted is used to evaluate offers or proposals.

1.0 Foreign ownership, control, or influence (FOCI) is a concern. For any software product that the supplier intends to acquire or develop, the supplier shall answer the following questions: [Note: Insert appropriate questions as shown in the sample questionnaires in the ***"Software Supply Chain Risk Management and Due-Diligence"*** pocket guide series or, if dealing with the US Government contracts, instruct the offerors to complete the Office of Management and Budget (OMB) Standard Form 328, "Certificate Pertaining to Foreign Interests."]

2.0 Due-Diligence Questionnaire. Offerors shall complete the SwA due-diligence questionnaire attached to this RFP.

3.0 Software Assurance Case

3.1 In order for the Acquirer to evaluate the proposed software assurance capabilities, the potential suppliers must submit an initial Software Assurance Case in accordance with ISO/IEC 15026, *Systems and software engineering — Systems and software assurance — Part 2: Assurance Case.* Paragraph 3.2 below identifies the minimum that should be included in the initial assurance case. The initial Software Assurance Case shall subsequently become a part of the contract and be used by the Acquirer as initial acceptance conditions.

3.2 It is understood that the initial Software Assurance Case will be broad in nature because potential suppliers will not know all the details of safety and security until contract performance. However, the assurance case should be comprehensive enough to convey a clear understanding of the safety and security requirement of this RFP. As a minimum, the initial Software Assurance Case shall include the following:

3.2.1 Top-level claims (and sub-claims as appropriate). These claims shall include all the characteristics of claims defined in ISO/IEC 15026.

3.2.2 Arguments for the top-level claims and sub-claims. These arguments shall include all the characteristics of arguments defined in ISO/IEC 15026.

3.2.3 Evidence and explicit assumptions supporting the arguments. The evidence shall include all the characteristics of evidence defined in ISO/IEC 15026.

3.2.4 Approving authority for the assurance case. The approving authority resume shall be included. The resume should include evidence of the authority's experience and education in software assurance and developing and managing software assurance cases.

4.0 Initial Software Description. The potential supplier shall submit an initial Software Architecture and such other descriptions as needed to provide a structure for the software. The Software Architecture shall include an initial description of the software components and connector, including software security related aspects. [NOTE: Include additional explanation.]

SAMPLE WORK STATEMENT

1.0 Trustworthy Software

1.1 Key definitions

"Security controls" mean the management, operational, and technical controls (that is, safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information [National Institute of Standards and Technology (NIST) Special Publication (SP) 800–53]. This definition includes software.

"Security category" means the characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals [Federal Information Processing Standards (FIPS) Publication (Pub) 199].

"Security objectives" mean confidentiality, integrity, and availability [44 United States Code (USC), Sec. 3542].

"Assurance" means grounds for justified confidence that a claim has been or will be achieved (ISO/IEC 15026).

"Assurance Case" means representation of a claim or claims, and support for these claims (ISO/IEC 15026). A Software Assurance Case includes (software assurance) claims and evidence that support those (software assurance) claims.

[Note: Include other appropriate definitions.]

1.2 Security Category. (NOTE: This is an example. Also see [FIPS 199] and [Department of Defense Instruction (DODI) 8500.2, Enclosure 4])

This software system is used for large procurements in a contracting organization and contains both sensitive and proprietary supplier information and routine administrative information. For the sensitive supplier information, the potential impact from a loss of confidentiality is moderate (for example, the loss may result in a significant financial loss), the potential impact from a loss of integrity is moderate (for example, the loss may result in the effectiveness of the contracting mission is significantly reduced and there is significant damage to the information asset), and the potential impact from a loss of availability is low (for example, the loss may result in downtime, but there is backup). For the routine administrative information, the potential impact from a loss of confidentiality is low, the impact from a loss of integrity is low, and the impact from a loss of availability is low.

Based on 1.2, the resulting security category of the software system is {(confidentiality, moderate), (integrity, moderate), (availability, low)}.

1.3 Software Security Requirements. Based on the security category for the software system, the minimum security requirements specified in [NOTE: Reference the external document(s)] are required.

[NOTE: Minimum security controls may be specified in this paragraph or in an external document similar to FIPS Pub 200; National Institute of Standards and Technology (NIST) SP 800–53; and DODI 8500.2, Enclosure 4].

1.4 Software Assurance Case. The Software Assurance Case shall be the primary instrument for refining and monitoring software assurance during the life of this contract. The Software Assurance Case shall be developed and conform to the requirements of ISO/IEC 15026, *Systems and software engineering—Systems and software assurance—Part 2: Assurance Case*. The supplier shall refine the Software Assurance Case throughout the development process and should be based on the software assurance requirements of this contract. The Contractor shall submit the case for review. [NOTE: Specify when the case should be reviewed, such as with the submission of the software design.] Lastly, the successful execution of the Software Assurance Case shall be a condition for final acceptance of the software product/service.

SAMPLE LANGUAGE FOR SECURITY CONTROLS - The following is sample language on implementing security controls and standards that may be considered for Federal agency use and may be appropriately modified for other uses. Federal Information Systems and National Security Systems are those defined by the Federal Information Security Management Act (FISMA), NIST standards and publications, and other publications applicable to a particular Federal agency's information systems. In using this language, Federal Information and National Security Systems need to be explicitly defined in accordance with the regulations and publications followed by the organization/agency. Contractor assets may be Contractor information technology or other assets that interface with Federal Information and National Security Systems. Paragraph (b) refers to certification and accreditation or other processes that an organization/agency may require. This should be explicitly stated in this paragraph as well.

Language for Security Controls and Standards

(a) When mitigating or remediating risks to confidentiality, integrity, and availability of Federal Information Systems, National Security Systems, Contractor assets that enable possession, control, or otherwise enable access to Federal Information or National Security Systems, the Contractor shall implement controls and standards as effective or more effective than those implemented by the Agency for the same or substantially similar risks with the same or substantially similar potential measure of harm.

(b) When selecting appropriate controls and standards for protecting confidentiality, integrity, and availability of Federal Information and National Security Systems, the Contractor shall use the analyses, processes, and standards established for Federal Government systems established by the [current organization/agency and other applicable standards] publications.

SAMPLE LANGUAGE FOR SECURE CONFIGURATION OF COMMERCIAL SOFTWARE - The following language is quoted from Office of Management and Budget Memorandum M–07–18, *Ensuring New Acquisitions Include Common Security Configurations,* dated 1 June 2007 (effective 1 February 2008). This is recommended language that may be supplemented as necessary. This language should also change when the software and associated regulations and suggestions for the configuration change. The use of common security configurations is included in part 39 of the Federal Acquisition Regulation. An example for Vista and Windows operating systems (OS) is included below. Other Operating System (OS) types such as Linux, Unix, etc. need to be configured securely as well:

Vista™ and Windows XP™ Standard Secure Configuration

(a) The provided information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html , and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html.

(b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to default "program files" directory and should be able to silently install and uninstall.

(c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

SAMPLE ACCEPTANCE CRITERIA - The following lists suggested generic software security acceptance and measurement criteria to be tailored as appropriate. These would apply at delivery and throughout the software life cycle. When using the language below or similar language, clarification should be provided on the specific meaning within the context of the software purchased:

(a) The Supplier shall provide all operating system, middleware, and application software to the Acquirer security configured by Supplier in accordance with the FAR requirement based on 44 USC 3544 (b) (2) (D) (iii).

(b) The Supplier shall demonstrate that all application software is fully functional when residing on the operating system and on middleware platforms used by the Acquirer in its production environment, configured as noted above.

(c) The Supplier shall NOT change any configuration settings when providing software updates unless specifically authorized in writing by the Acquirer.

(d) The Supplier shall provide the Acquirer with software tools that the Acquirer can use to continually monitor software updates and the configuration status.

(e) At specified intervals by the Buyer, the Supplier shall provide the Acquirer with a comprehensive vulnerability test report for the suite of applications and associated operating system and middleware platforms used by the Acquirer in its production environment, configured as noted above.

(f) The Acquirer and Supplier agree to work together to establish appropriate measures to quantify and monitor the supplier's performance according to the contract requirements. Specific guidance should include types of measures to be used, measures reporting frequency, measures refresh and retirement, and thresholds of acceptable performance.

(g) The Supplier shall provide all operating system, middleware, and application software to the Acquirer free of common vulnerabilities as specified by the Common Vulnerabilities and Exposures (CVE®)—The Standard for Information Security Vulnerability Names that can be retrieved from http://cve.mitre.org/.

(h) The Supplier shall provide all operating system, middleware, and application software to the Acquirer free of common weaknesses as specified in the Common Weakness Enumeration, A Community-Developed Dictionary of Software Weakness Types that can be retrieved from http://cwe.mitre.org/.

SAMPLE LANGUAGE FOR CERTIFICATION & ACCREDITATION AND COMMON CRITERIA - The following language relates to certification and accreditation processes and should be appropriately tailored for the organization's or agency's particular requirements for certification and accreditation:

Contractors must also warrant that proposed system and software product specifications and security and data access architectures have either been addressed in ongoing documentation required by the agency's certification and accreditation process [name the process, regulations governing the process, and specific documentation where this must be addressed] and are ready for evaluation in applicable phases of the process [list the specific phases of the process and specifically what is required in each phase]. Contractors must also address willingness to provide proposed equipment and engineering assistance as required, at no cost to the government, to the specified [name the testing facility] testing facility to obtain required certification of functionality.

The following language relates to Common Criteria:

Contractors must warrant that their products have been satisfactorily validated under Common Criteria or that products will be satisfactorily validated with the period of time specified in the contract and that such product validation will be maintained for updated versions or modifications by subsequent evaluation as required.

CERTIFICATE OF ORIGINALITY - The SwA Forum's **"Software Assurance in Acquisition: Mitigating Risk to the Enterprise"** Appendix F, provides a sample **"Certificate of Originality"** developed by **IBM** that requires the vendor to sign stating that the code in the product is their own creation and not copied from other sources. This certification covers more than SwA and should be used as an idea generator for ultimate requirements and terms and conditions that the acquisition official creates for the RFP and/or contract. The questionnaire must be completed by a vendor furnishing copyrightable material, such as software, audio/visual works, written materials, etc. Please visit https://buildsecurityin.us-cert.gov/swa/acqact.html for more details.

Resources:

- New York State "Application Security Procurement Language" at http://www.sans.org/appseccontract/.
- OWASP Secure Software Contract Annex at http://www.owasp.org/index.php/Category:OWASP_Legal_Project.
- Center for Strategic & International Studies "Security Cyberspace for the 44th President" at http://www.csis.org/component/option,com_csis_pubs/task,view/id,5157/.
- Idaho National Labs "Cyber Security Procurement Language for Control Systems" at http://www.msisac.org/scada/documents/4march08scadaprocure.pdf.
- Ounce Labs "Software Security Addendum" at http://www.ouncelabs.com/assurance/.
- Common Weakness Enumeration (CWE): A list of the known software security weaknesses at http://cwe.mitre.org/data/index.html.
- [IBM CO] No Author. (2006). *Certificate of Originality.* Poughkeepsie, NY: IBM Corporation.
- Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software (SwA CBK) developed by the DHS/DOD SwA Workforce, Education and Training Working Group at https://buildsecurityin.us-cert.gov.
- ISO/IEC 15408–3. *Information technology—Security techniques—Evaluation criteria for IT security—Part 3: Security assurance requirements at* http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm.
- *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components* at http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2.
- ISO/IEC 17799. *Information Technology—Security techniques—Code practice for information security management at* http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3.

Sample Language-US Government RFPs/Contracts

Although, the following sample language is tailored for government contracts (and task orders), other acquirers may tailor parts or all the language for their use, as well.

1.0 GENERAL

All work under this contract shall comply with the latest version of all applicable standards. Individual task orders will reference applicable versions of standards or exceptions as necessary. These may include, but are not limited to, {AGENCY} Manual(s), Acquisition Bulletins [AB], American National Standards Institute [ANSI] standards, and National Institute of Standards and Technology [NIST] standards, including Federal Information Processing Standards [FIPS] publications. Software Development Standards Life Cycle (SDLC) Guidelines contains a list of software development standards for {AGENCY} tasks. The {AGENCY} has developed its own Enterprise Life Cycle. While complying with the latest version of all applicable standards is not a new initiative, it does provide an emphasis of the {AGENCY}'s expectation that the Contractor will comply with, and provide verification that these standards are adhered to.

2.0 CORRECTION OF SOFTWARE AND DOCUMENTATION

The contractor shall, over the term of the contract, under any task order issued, correct errors in Contractor developed software and applicable documentation that are not commercial off the shelf which are discovered by the Government, and any other user of the software, or the Contractor. If the system is in production, such corrections shall be completed within one working day of the date the Contractor discovers or is notified of the error (or a date mutually agreed upon between the CO and the Contractor not to exceed 30 working days). If the system is not in production, such corrections shall be made within five working days of the date the Contractor discovers or is notified of the error (or a date mutually agreed upon between the CO and the Contractor, not to exceed 30 days). Latent defects will be handled in the same manner, as soon as they are discovered. Inability of the parties to determine the cause of software errors shall be resolved in accordance with the Disputes clause in Section I, FAR 52.233-1, incorporated by reference in the contract, but in no event constitutes grounds for delay of error correction beyond the periods specified.

3.0 SOFTWARE DEVELOPMENT PROCEDURES

3.1 CAPABILITY MATURITY MODEL INTEGRATION (CMMI)

3.1.1 All Contractors awarded task orders for any activity related to software development for the {AGENCY} shall comply with the {AGENCY} policy for CMMI® compliance. All tasks that fall within the software development life cycle shall at minimum comply with Level {2, 3, 4, or 5 as required} of the staged representation of the CMMI® for Software Engineering (CMMI-SW). There are no exceptions to this {AGENCY}'s policy. Contractors developing software for the {AGENCY} shall maintain Level {2, 3, 4, or 5 as required} or higher in the staged representation of the CMMI-SW in order to continue to receive software tasking.

3.1.2 The Capability Maturity Model (CMM) Review Team will monitor the Contractor's process maturity (1) using standard {AGENCY} Process Appraisal Review Methodology (PARM) processes, including execution of Standard CMMI Appraisal Method for Process Improvement (SCAMPISM), as needed, (2) performing annual cycles of review for CMMI-SW, and (3) considering all types of appraisal data and process improvement infrastructure data as standardized by the {AGENCY} PARM process to verify alignment and mapping of the Contractor's CMMI processes to the {AGENCY} Enterprise Life Cycle (ELC). The responsible organization is indicated as Contractor (to be delivered under this Task Order), Government (Government will prepare), or Joint

(a joint effort with the {AGENCY} in the lead). The Government may waive (indicated as Not Applicable) the requirements for certain deliverables or work products based on the approved Program Tailoring Plan.

3.2 SECURITY CONTROLS

3.2.1 The Contractor shall follow the NIST 800-53, Recommended Security Controls for Federal Information Systems and the {AGENCY} guidance to ensure that the Software will be or has been developed using secure coding practices in a manner that minimizes security flaws within the Software. Prior to the execution of a software development Work Request the Contractor shall provide the {AGENCY} a copy of the Contractor's secure coding best practices policy and upon delivery of the Software to the {AGENCY}, the Contractor shall certify to the {AGENCY} in writing that the Contractor complied with the Policy in the performance of its obligations under the task order.

3.2.2 The Contractor will be subject to an annual review that will allow the {AGENCY} to assess the effectiveness of security controls. In addition, the Contractor shall ensure that appropriate security management tools are in place to allow for the review of security configurations, user identities, etc.

3.3 REQUIREMENTS TRACEABILITY. The Contractor shall provide the requirements traceability matrix at the end of analysis phase, design phase, build phase, and deployment phase that designates the security requirements in a separate section so that they can be traced through the development life cycle. The Contractor shall also provide the application designs and test plan documentation, and source code to Government for review.

3.4 SOFTWARE CHANGES. Without exception, for changes that may produce an impact on security, the Contractor shall follow the Security Change Management procedures.

3.5 MALICIOUS CODE WARRANTY. The Contractor represents and warrants that the Software shall be free from all computer viruses, worms, time-outs, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the Software user's or another's software, hardware, networks, data or information.

3.6 ACCEPTANCE—SECURE SOFTWARE

3.6.1 Notwithstanding any other provision of the task order, the {AGENCY} will not accept the software until a Government source code and security analysis has been performed. The Software shall be deemed to be "Non-Secure" if the Software includes any one or more of the security flaws. A detailed listing of security flaws will be provided to the Contractor and will be updated based on newly discovered flaws.

3.6.2 If after a security audit the Software is determined to be Non-Secure, then upon written notice of such Non-Secure status, the Contractor, at its cost and expense, shall use its commercially reasonable best efforts to remedy the security flaws by modifying or replacing the Software within 30 days of receipt of such written notice (the "Remedy Period"). Upon receipt of revised Software and notice from the Contractor that the security flaws have been remedied prior to the end of the Remedy Period, the Government, shall again subject the Software to a security audit at the Contractor's expense.

3.6.3 Notwithstanding any other provision of the Agreement, if the Software is determined to be Non-Secure as set forth above and remains Non-Secure at the end of the Remedy Period, the {AGENCY} shall be deemed to have not accepted the Software under the terms of the Contract unless the {AGENCY} in its sole discretion otherwise expressly agrees in writing to accept the Software notwithstanding that it is deemed to be Non-Secure.

3.7 WORK PRODUCTS REQUIRED

(These will be defined within the Work Requests written for this sub-task.)

3.8 ACCEPTANCE CRITERIA--OTHER

(These will be defined within the Work Requests written for this sub-task.)

3.9 AGENCY SECURITY STANDARD. The security standard for the {AGENCY}, including both the security policies and the security requirements, are pre-defined. In general, the sources of these policies and requirements include:

- In accordance with the requirements of the Office of Federal Procurement Policy Act of 1974 (Pub. L. 93-400), as amended by Pub. L. 96-83,
- The Federal Information Security Management Act of 2002 (H.R. 2458, Title III, Section 301),
- OMB A-130, Management of Federal Information Resources, Appendix III,
- OMB A-127, Financial Management Systems,
- OMB A-123, Management's Responsibility for Internal Control,
- Publication 1075, Safeguarding Taxpayer Information for Federal, State, and Local Agencies & Entities,
- {Other appropriate Federal laws and/or directives},
- {Appropriate AGENCY or Senior AGENCY Directives and Manuals}.

4.0 PREPARATION AND MAINTENANCE OF CERTIFICATION AND ACCREDITATION DOCUMENTS

4.1 The Contractor shall participate in the {AGENCY} security Certification and Accreditation (C&A) process by providing all product specific input (electronic) to the Application System Security Plan (SSP) and the Application Information Technology Contingency Plan (ITCP). Refer to NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems (http://csrc.ncsl.nist.gov/publications/nistpubs), for additional guidelines in writing a security plan. An {AGENCY} Certification and Accreditation checklist, guidance and document templates is available to assist the Contractor. The purpose of the SSP and the ITCP is to provide the {AGENCY} with technical insight on how the Contractor meets the {AGENCY} security requirements.

4.2 The Contractor shall follow the {AGENCY} security standard and policies (see the document references) for security. The Contractor shall use the policies and other applicable guidance as a framework for specific security controls, documents, procedures and features when performing security requirements analysis and security design.

4.3 The Contractor shall provide draft updates (electronic) version of the Application System Security Plan within 30 calendar days of a major change to the system or at a minimum on an annual basis by June 30 to the Program Management Office (PMO).

4.4 Included with the submission of the draft SSP the Contractor shall maintain a current up-to-date version of the Application Information Technology Contingency Plan (ITCP) and related escalation procedures.

4.5 The PMO will review the security documents for 10 calendar days and provide written comments and changes for the Contractor to address. Contractors will have 10 calendar days to address the comments and complete the documents.

4.6 The security standard for the {AGENCY}, including both the security policies and the security requirements, are pre-defined. In general, the sources of these policies and requirements include:

{Appropriate AGENCY or Senior AGENCY Directives and Manuals}

- NIST Draft SP 800-37 “Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems,” November 5, 2002, http://csrc.nist.gov/sec-cert/,
- The Privacy Act (PA), and
- The Federal Information Systems Management Act (FISMA).

5.0 CONTINUOUS MONITORING, TESTING, AND REPORTING

5.1 SELF TESTING

5.1.1 SELF TESTING REQUIREMENTS. The Contractor shall perform self testing of their implemented security controls. The Contractor shall continuously monitor all testing activities and report on the performance and effectiveness of the {AGENCY} security controls (as required by FISMA, OMB Circular A-130, NIST guidance and FIPS publications) to the {AGENCY} project manager assigned to oversee this contract. The specific assessments procedures as outlined in draft NIST Special Publication 800-53A, shall be used by the Contractor in assessing whether appropriate corrective action was taken on previously closed Plan of Action and Milestones (POA&Ms) and volatile security controls.

5.1.2 SELF TESTING SCHEDULE. The Contractor shall work with {AGENCY} project manager to establish schedules, discuss roles and responsibilities, testing requirements, and other general activities to ensure continuous monitoring is well organized and completed in a timely manner and in accordance with the {AGENCY} procedures.

5.2 TESTING CONTROLS. The security controls specified in {AGENCY} policy {identify the policies or other documents} shall be tested by the Contractor using approved {AGENCY} methods. As part of testing controls, the Contractor shall examine existing data sources and metrics, such as self assessments, incident reporting statistics, risk assessments, third party evaluations, and other existing data and propose a set of metrics that leverages existing data and is consistent with the compliance evaluation criteria. The Contractor shall include verification and validation to ensure that appropriate corrective action was taken on POA&Ms closed in the last quarter.

5.3 REPORTING. The Contractor shall provide a determination, in a written form agreed to by the {AGENCY} project management, on whether the implemented corrective action was adequate to resolve the identified information security weaknesses and provide the reasons for any exceptions or risk-based decisions.

5.4 ASSESSMENT METHODOLOGY

5.4.1 ASSESSMENT PROCEDURES. The assessment procedures as outlined in draft NIST 800-53A shall be used by the Contractor as guide in the execution of the test procedures as deemed appropriate. These procedures shall be supplemented and augmented by tailored test procedures based on the control objective as it applies to {AGENCY}.

5.4.2 TEST METHODS. The Contractor shall use test methods that include interview, examine, and test. The interview method is the process of conducting focused discussions with individuals or groups of individuals within an organization to facilitate the reviewer's understanding, achieve clarification, or obtain evidence. The examine method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). Similar to the interview method, the primary purpose of the examine method is to facilitate the reviewer's understanding, achieve clarification, or obtain evidence. The test method is the process of exercising one or more objects (limited to activities or mechanisms) under specified conditions to compare actual with expected behavior. In all three cases (i.e., interview, examine, and test) where the methods are employed, the results are used to support the determination of overall security control effectiveness.

5.4.3 DETERMINATION STATEMENTS. The Contractor shall write a determination statement describing the results of each tested control.

5.4.4 SCORING. The Contractor shall mark each determination with an "S" for "Satisfied" or an "O" for "Other than satisfied." If all of the determination statements and test procedures for a control are marked as "S for Satisfied", then the Contractor shall score the control as "In Place". If one or more of the determination statements and test procedures for a control is marked as "O for Other than Satisfied", then the Contractor shall score the control as "Partially in Place." If most or all of the determination statements and test procedures for a control are marked as "O for Other than Satisfied," then the contractor shall score the control as "Planned".

5.5 REPORTING

The Contractor shall fully document tests in accordance with the reporting format prescribed by {AGENCY} procedures. When the results are partially satisfied or other than satisfied condition, the Contractor shall document any vulnerabilities indicating which portions of the security control have not been implemented or applied.

6.0 OTHER ACTIVITIES. ***The following are some ideas for additional activities—some of which may be repeated in previous paragraphs. These additional ideas provide additional language from which to choose. Also note that the language below and in some previous paragraphs apply to the "system" vice specifically to the "software" in the system.***

6.1 PO&M MAINTENANCE. The Contractor shall develop and support Web Services in implementing solutions that will provide a means of planning and monitoring corrective actions; define roles and responsibilities for risk mitigation; assist in identifying security funding requirements; track and prioritize resources; and inform decision-makers of progress of open POA&M items. The Contractor shall perform verification of IT security weaknesses to ensure that all weaknesses identified through third party (e.g., Office of Inspector General (OIG)) audits are included in the POA&Ms that the quarterly reporting to OMB is accurate, as well as actual activities are mirroring planned activities and the reasons for any exceptions or risk-based decisions are reasonable and clearly documented. This verification process will be done in conjunction with the continuous monitoring program and will leverage the knowledge and methodology established through that strategy.

6.2 FISMA COMPLIANCE. The Contractor shall plan and execute FISMA testing of controls.

6.3 C&A DOCUMENTATION. The Contractor shall update the Application Certification and Accreditation (C&A) documentation to ensure that the C&A artifacts are kept current and contain all information and supporting evidence is documented for the next certification and accreditation is available and complete. This shall include reviewing changes made to the system in order to identify any new data types that may have a Privacy Impact or change the Security Categorization of the system.

6.4 SECURITY RISK ASSESSMENT. The Contractor shall work with the {AGENCY} project manager in performing Security Risk Assessment (SRA). This includes identifying risks related to the design and functionality of a new system against compliance with the {AGENCY} risk management process, NIST SP 800-39, FIPS 200 and SP 800-53. Activities performed during this phase shall include analyzing how the security architecture implements the {AGENCY} documented security policy for the system, assessing how management, operational, and technical security control features are implemented by the software and hardware, how the system interconnects to other networks while maintaining security, and lastly analyzing other inherent design features. Procedures including a checklist shall be used to document compliance with baseline security requirements and existing agency guidance.

6.6 SECURITY TESTING AND EVALUATION (ST&E). The Contractor shall work with {AGENCY} project manager in performing pre-ST&E activities, including but not limited to, coordinating the ST&E and developing the ST&E Plan and ST&E test cases. The Contractor shall also assist project officer in performing dry run assessments to determine the adequacy of functional and non-functional controls in preparation for the ST&E, update the ST&E plan based on dry run assessments, observe and provide assistance to the ST&E testing team to ensure successful and timely completion of the test plans, and prepare the POA&Ms resulting from the ST&E results.

7.0 GOVERNMENT INDEPENDENT TESTING. The Government will perform periodic vulnerability testing to evaluate the security of {AGENCY}. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. The intent of testing is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. The frequency of the testing will be at a minimum quarterly and on demand based on the risk associated with newly discovered vulnerabilities.

Conclusion

This pocket guide compiles example RFP/Contract language for integrating SwA into the acquisition life cycle to support risk-based decision making by buyers and software evaluators. For the latest updates and details, visit the web sites listed in the preceding pages and resource box.

The Software Assurance Pocket Guide Series is developed in collaboration with the SwA Forum and Working Groups and provides summary material in a more consumable format. The series provides informative material for SwA initiatives that seek to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development, acquisition and deployment of trustworthy software products. Together, these activities will enable more secure and reliable software that supports mission requirements across enterprises and the critical infrastructure.

For additional information or contribution to future material and/or enhancements of this pocket guide, please consider joining any of the SwA Working Groups and/or send comments to Software.Assurance@dhs.gov. SwA Forums are open to all participants and free of charge. Please visit https://buildsecurityin.us-cert.gov for further information.

No Warranty

This material is furnished on an "as-is" basis for information only. The authors, contributors, and participants of the SwA Forum and Working Groups, their employers, the U.S. Government, other participating organizations, all other entities associated with this information resource, and entities and products mentioned within this pocket guide make no warranties of any kind, either expressed or implied, as to any matter including, but not limited to, warranty of fitness for purpose, completeness or merchantability, exclusivity, or results obtained from use of the material. No warranty of any kind is made with respect to freedom from patent, trademark, or copyright infringement. Reference or use of any trademarks is not intended in any way to infringe on the rights of the trademark holder. No warranty is made that use of the information in this pocket guide will result in software that is secure. Examples are for illustrative purposes and are not intended to be used as is or without undergoing analysis.

Reprints

Any Software Assurance Pocket Guide may be reproduced and/or redistributed in its original configuration, within normal distribution channels (including but not limited to on-demand Internet downloads or in various archived/compressed formats).

Anyone making further distribution of these pocket guides via reprints may indicate on the pocket guide that their organization made the reprints of the document, but the pocket guide should not be otherwise altered.

These resources have been developed for information purposes and should be available to all with interests in software security.

For more information, including recommendations for modification of SwA pocket guides, please contact Software.Assurance@dhs.gov or visit the Software Assurance Community Resources and Information Clearinghouse: https://buildsecurityin.us-cert.gov/swa to download this document either format (4"x8" or 8.5"x11").

Software Assurance (SwA) Pocket Guide Series

SwA is primarily focused on software security and mitigating risks attributable to software; better enabling resilience in operations. SwA Pocket Guides are provided; with some yet to be published. All are offered as informative resources; not comprehensive in coverage. All are intended as resources for 'getting started' with various aspects of software assurance. The planned coverage of topics in the SwA Pocket Guide Series is listed:

SwA in Acquisition & Outsourcing

I. Software Assurance in Acquisition and Contract Language
II. Software Supply Chain Risk Management & Due-Diligence

SwA in Development

I. Integrating Security into the Software Development Life Cycle
II. Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses
III. Risk-based Software Security Testing
IV. Requirements & Analysis for Secure Software
V. Architecture & Design Considerations for Secure Software
VI. Secure Coding & Software Construction
VII. Security Considerations for Technologies, Methodologies & Languages

SwA Life Cycle Support

I. SwA in Education, Training & Certification
II. Secure Software Distribution, Deployment, & Operations
III. Code Transparency & Software Labels
IV. Assurance Case Management
V. Assurance Process Improvement & Benchmarking
VI. Secure Software Environment & Assurance Ecosystem

SwA Measurement & Information Needs

I. Making Software Security Measurable
II. Practical Measurement Framework for SwA & InfoSec
III. SwA Business Case & Return on Investment

SwA Pocket Guides and related documents are freely available for download via the DHS NCSD Software Assurance Community Resources and Information Clearinghouse at https://buildsecurityin.us-cert.gov/swa.