Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals

JANUARY 2014

Deputy Assistant Secretary of Defense for Systems Engineering
and Department of Defense Chief Information Officer

Washington, D.C.

Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)) and Department of Defense Chief Information Officer (DoD CIO). 2014. *Suggested Language to Incorporate System Security Engineering for Trusted Systems and Networks into Department of Defense Requests for Proposals.* Washington, D.C.: DASD(SE) and DoD CIO.

Office of Primary Responsibility:

Deputy Assistant Secretary of Defense
Systems Engineering
3030 Defense Pentagon
3C167
Washington, DC 20301-3030
www.acq.osd.mil/se

Contents

Introduction 4

Section C: Statement of Work 5

Section C: System Requirements Document 9

Section L: Instructions, Conditions, and Notices to Offerors 10

Section M: Proposal Evaluation Criteria 11

Introduction

This document is intended for use by Department of Defense (DoD) program managers preparing requests for proposals (RFP) for major defense acquisitions. Notes in *italics* are directions to the program office and are not to be included in the RFP.

This RFP language implements the policy outlined in Department of Defense Instruction (DoDI) 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," only. This language does not address critical program information (CPI), anti-tamper, or defense exportability.

The program office should tailor this RFP language based on the cost-benefit analysis for each acquisition.

References

Defense Acquisition Guidebook. Washington, D.C.: Under Secretary of Defense for Acquisition, Technology, and Logistics. https://dag.dau.mil/.

Department of Defense Instruction (DoDI) Interim 5000.2. 2013. "Operation of Defense Acquisition System." Under Secretary of Defense for Acquisition, Technology, and Logistics (November 25). http://www.dtic.mil/whs/directives/corres/pdf/500002_interim.pdf

Department of Defense Instruction (DoDI) 5200.44. 2012. "Protection of Mission-Critical Functions to Achieve Trusted Systems and Networks." Washington, D.C.: DoD Chief Information Officer/Under Secretary of Defense for Acquisition, Technology, and Logistics (November 5). http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf

Department of Defense Instruction (DoDI) 8582.01. 2012. "Security of Unclassified Information on Non-DoD Information Systems." Washington, D.C.: DoD Chief Information Officer (June 6). http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf

Dougherty, Chad, et al. 2009. *Secure Design Patterns.* SEI-2009-TR-010. Hanscom Air Force Base, Mass.: Software Engineering Institute, Carnegie Mellon University/Department of Defense. http://www.cert.org/

MIL-STD-882. 2012. Department of Defense Standard Practice: System Safety. https://assist.dla.mil

National Defense Industrial Association (NDIA) System Assurance Committee. 2008. *Engineering for System Assurance.* Arlington, Va.: NDIA. http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf

National Institute of Standards and Technology (NIST) Interagency Report 7622. 2012. *Notional Supply Chain Risk Management for Federal Information Systems.* Washington, D.C.: NIST, U.S. Department of Commerce. http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf

Section C: Statement of Work

The following proposed clauses should be tailored and added to the Statement of Work (SOW) Systems Engineering section:

[SOWxxx1] The contractor shall develop and update mission criticality analysis(-es), vulnerability assessment(s), risk assessments(s), and identification and counter measurement implementation(s) for Mission-Critical Functions, the failure of which would result in either Level I (Catastrophic) or Level II (Critical) compromise of mission capability.

[SOWxxx2] Adapting the MIL-STD-882 (System Safety) (https://assist.dla.mil) definitions of criticality to mission criticality, the contractor shall define the following criticality levels:

- Level I (Catastrophic) protection failure that results in total compromise of mission capability
- Level II (Critical) protection failure that results in unacceptable compromise of mission capability or significant mission degradation
- Level III (Marginal) protection failure that results in partial compromise of mission capability or partial mission degradation
- Level IV (Negligible) protection failure that results in little or no compromise of mission capability.

[SOWxxx3] For each Level I and Level II Mission-Critical Function identified by the contractor in the criticality analysis, the contractor shall identify the associated logic-bearing system components (e.g., hardware, firmware, and software) that implement, protect, or introduce vulnerability, to that function (hereafter referred to collectively as the "critical components").

[SOWxxx4] The contractor shall demonstrate that the contractor has mechanisms in place to effectively monitor the supply chain for critical components, understands how supply chain risk[1] can be introduced through those components, and has implemented or plans to implement countermeasures to mitigate such risks.

[SOWxxx5] The contractor shall plan for and implement countermeasures that mitigate the risk of foreign intelligence or foreign influence, technology exploitation, supply chain and battlefield threats, and vulnerabilities that result in Level I and Level II protection failures of the system; countermeasures include the following:

1. The application of supply chain risk management best practices, applied as appropriate to the development of the system. Supply chain risk management key practices may be found in the National Institute of Standards and Technology (NIST) Interagency Report 7622, *Notional Supply Chain Risk Management for Federal Information Systems* (http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf), and the National Defense

[1] As defined in DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," the term "supply chain risk" means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

Industrial Association (2008) guidebook, *Engineering for System Assurance,* both publicly available (http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf).

[Note to program office: Other publicly available references or internal documents made available may be added to the documents noted.]

2. The enumeration of potential suppliers of critical components, as they are identified, including cost, schedule, and performance information and proposed selection decisions for the purposes of obtaining approval from the Government and engaging in the development of mutually agreeable risk management plans for the selected suppliers of critical components.
3. The processes to control access by foreign nationals to program information, including, but not limited to, system design information, DoD-unique technology, and software or hardware used to integrate commercial technology.
4. The processes and practices employed to ensure that genuine (i.e., not counterfeit) information and communications technology (ICT) are employed in the solution and that processes and requirements for genuine ICT are levied upon subcontractors. ICT includes all categories of ubiquitous technology used for gathering, storing, transmitting, retrieving, or processing information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). ICT is not limited to information technology (IT), as defined in section 11101 of title 40, U.S. Code. Rather, this term reflects the convergence of IT and communications.
5. The processes used to protect both unclassified and classified DoD information, technical data (e.g., source code), and computer software in the development and support environments (e.g., Government- or contractor-owned facilities and the integrated development environment) from entities without a need to know.

[SOWxxx6] The provisions of [SOWxxx1], [SOWxxx2], [SOWxxx3], and [SOWxxx4] at a minimum shall be included in all solicitations, contracts, and subcontracts for all suppliers of critical functions and associated components at all tiers.

[SOWxxx7] The contractor shall ensure that updated assumptions, rationale, and results related to the criticality analyses, vulnerability assessments, risk assessments, supply chain risk information, and risk mitigations are made available for Government review at each Systems Engineering Technical Review (SETR).

[SOWxxx8] The contractor shall use Government-provided foreign intelligence and technology-exploitation threat information, along with the traditional acquisition and battlefield threat information, to inform system security engineering (SSE), systems engineering, and procurement decision processes.

[SOWxxx9] The contractor shall develop a set of secure coding standards and secure design features drawing upon the "top 10 secure coding practices" (https://www.securecoding.cert.org/confluence/display/seccode/Top+10+Secure+Coding+Practices), the CWE/SANS top 25 most dangerous software errors (http://cwe.mitre.org/top25/index.html), and the secure design patterns (www.cert.org/archive/pdf/09tr010.pdf - 2009-10-23) to use with all Level I Mission-Critical Function components.

[SOWxx10] The contractor shall develop, document, and update Table X software assurance plans and actuals in accordance with the table description provided in the Defense Acquisition Guidebook section 13.7.3 (https://acc.dau.mil/CommunityBrowser.aspx?id=492079#13.7.3).

Table X: Application of Software Assurance Countermeasures (sample)

Development Process								
Software (Critical Function components, other software)	**Static Analysis p/a (%)**	**Design Inspect**	**Code Inspect p/a (%)**	**CVE p/a (%)**	**CAPEC p/a (%)**	**CWE p/a (%)**	**Pen Test**	**Test Coverage p/a (%)**
Developmental Level I and II Critical Function SW								
Other Developmental SW								
COTS level I and II Critical Function SW								
COTS (other than Critical Function) and NDI SW								
Operational System								
	Failover Multiple Supplier Redundancy (%)	**Fault Isolation**	**Least Privilege**	**System Element Isolation**		**Input Checking / Validation**		**SW Load Key**
Developmental Level I and II Critical Function SW								
Other Developmental SW								
COTS Level I and II (CF) and NDI SW								
Development Environment								
SW Products	**Source**	**Release Testing**	**Generated Code Inspection p/a (%)**		**OEM or Authorized Dealer**			
[List the COTS products used in the software development environment]								

CAPEC: Common Attack Pattern Enumeration and Classification
COTS: commercial off-the-shelf
CVE: Common Vulnerabilities and Exposures
CWE: Common Weakness Enumeration
NDI: non-developmental item
OEM: Original Equipment Manufacturer
p/a: plan vs. actual
Pen: penetration testing
SW: software

[SOWxx11] For Level I Mission-Critical Functions and their Critical Components, the contractor shall establish basic protection requirements unless not establishing such requirements is justified by a cost-benefit analysis approved by the Government. Critical function Supply Chain and Development basic protections shall include the following:

- A Supplier Management Plan that:
  - Includes supplier selection criteria to reduce supply chain risks
  - Evaluates and maintains a list of suppliers and alternate suppliers with respect to the criteria established
- An Anonymity Plan that:
  - Limits the disclosure of the baseline design, test, and supply chain data
  - Uses blind buys for component procurement
- Additional access controls that:
  - Further limit access to critical components and information about critical components beyond normal program control
  - Log access
  - Establish data collection for post-attack forensic analysis
  - Require inspection and approval of changes
- Third-party software assurance and supply chain attack testing of development processes, system, and development environment.
- Material and non-material attack and compromise response process.

[Note to program office: Also consider applying some or all of these to Level II critical functions and associated components.]

[SOWxx12] The contractor shall protect unclassified DoD data from unauthorized access or disclosure in accordance with DoDI 8582.01, "Security of Unclassified Information on Non-DoD Information Systems," (http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf) and the program's Security Classification Guide.

Section C: System Requirements Document

The following proposed clauses should be tailored and added to the System Requirements Document (SRD):

[SRD001] For critical components of Level I Mission-Critical Functions, the system shall establish basic protection requirements unless justified by a cost-benefit analysis approved by the government. Those basic protections shall include:

- Establish least privilege using distrustful decomposition (privilege reduction) or a similar approach to move Level I critical functions into separate mutually untrusting programs.*
- Physical and logical diversification of critical components for Mission-Critical Functions which require redundancy to meet reliability or safety requirements.
- Physical and logical diversification with voting to establish trustworthiness of selected Level I Mission-Critical Function components.
- Wrappers for COTS, legacy, and developmental software to enforce strong typing, context checking, and other interface validation methods for interfaces with Mission-Critical Functions; see SEI-2009-TR-010 (Dougherty et al. 2009).
- Wrappers for COTS, legacy, and developmental software to identify and log invalid interface data using secure logging approaches; see SEI-2009-TR-010, *Secure Design Patterns,* Software Engineering Institute, Carnegie Mellon University/Department of Defense (http://www.cert.org/).

Section L: Instructions, Conditions, and Notices to Offerors

The following proposed clauses should be tailored and considered individually for addition to section L :

[SecL001] The offeror, as part of its technical proposal, shall describe the use of its system security engineering (SSE) process in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities. As a part of describing this SSE process, the offeror shall describe the criticality analysis process used to determine Mission-Critical Functions and the protection techniques (countermeasures and sub-countermeasures) used to achieve system protection and mission effectiveness.

[SecL002] The offeror, when describing its systems engineering, integration, and test (SEI&T) processes, shall describe what steps are planned or taken to include system security engineering (SSE) as an integral part of its overall SEI&T approach that will be used to deliver the required system capability.

[SecL003] The offeror, as part of the technical proposal, shall describe the approach used to prevent, detect, and respond to supply chain risk including malicious insertion of malware the program's supply chain for critical function components.

Section M: Proposal Evaluation Criteria

The following proposed criteria should be tailored and considered individually for addition to section M:

The offeror's proposal will be evaluated based upon:

1. The extent to which the offeror employs a disciplined, structured system security engineering (SSE) process, including criticality analysis, in arriving at its system specification and design.
2. The extent to which the SSE process identifies and mitigates threat and vulnerability risks to the system mission effectiveness.
3. The extent to which the SSE process is integrated within the overall Systems Engineering, Integration and Test (SEI&T) process.
4. The extent to which supply chain risk protection, detection, and response procedures and activities are incorporated into the system acquisition.