Raytheon

CYBER RESILIENT AND SECURE WEAPON SYSTEMS ACQUISITION / PROPOSAL DISCUSSION

Integrated Defense Systems

Holly Dunlap

October 2017

Perception, Expectations and Reality

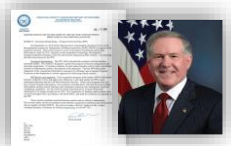
Cyber Resilient and Secure Weapon System Acquisition

- National Strategy, Priorities and Big Picture Messaging
- DoD Cybersecurity Budget Review
- Current State RFP Analysis
- Acquisition RFP Guidance
- Channel the Energy and Contribute
- Recommendations
- Final Thoughts

DoD Policy and Strategy

2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017

Oct '10: Establishment and standup of U.S. Cyber Command

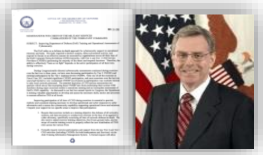

Frank Kendall
Deputy Under Secretary for AT&L

Jul '11: Memo outlining Program Protection Plan (PPP) for Cyber hardening of DoD Systems

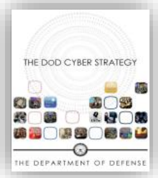
Feb '13: PPD-21, security and resilience of critical infrastructure against cyber threats

Gen. Alexander, Commander USCYBERCOM

Mar '13: Public acknowledgement of Cyber warfare "teams" ready by 2015

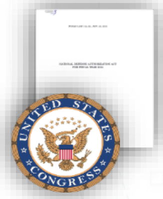

J. Michael Gilmore, Director, OT&E

August 14: Directed Cybersecurity in OT&E

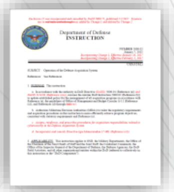


Apr '15: DoD strategy expands network defense beyond their own systems and addresses synchronization of Cyber operations with kinetic effects

2015: Multiple proposed bills to address information sharing between gov't and private sector



2016: NDAA 16 Section 1647 Evaluation of Cyber Vulnerabilities



2017: DoD 5000.02 Encl 14, Cyber security in the Defense Acq Sys

> " *Improve weapons systems cybersecurity.* DoD will assess and initiate improvements to the cybersecurity of current and future weapons systems, doing so on the basis of operational requirements. For all future weapons systems that DoD will acquire or procure, DoD will mandate specific cybersecurity standards for weapons systems to meet. "
>
> – *The DoD Cyber Strategy, April 2015*

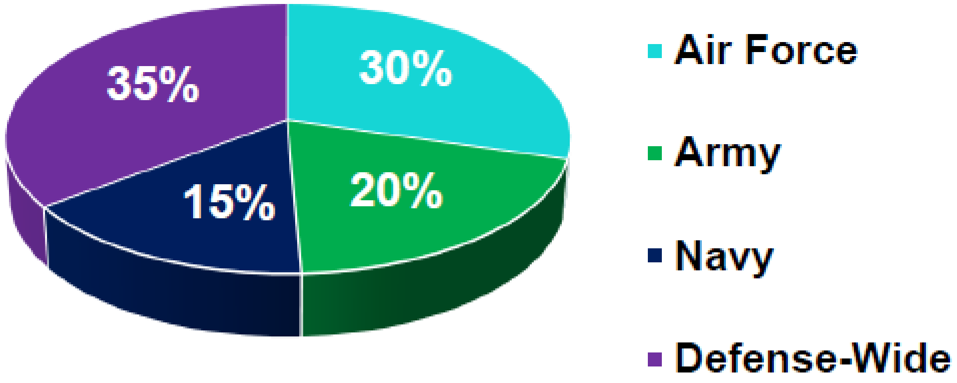
Policy is evolving, acquisition requirements need to incorporate policy requirements

DoD FY17 PB Request for Cybersecurity Overall

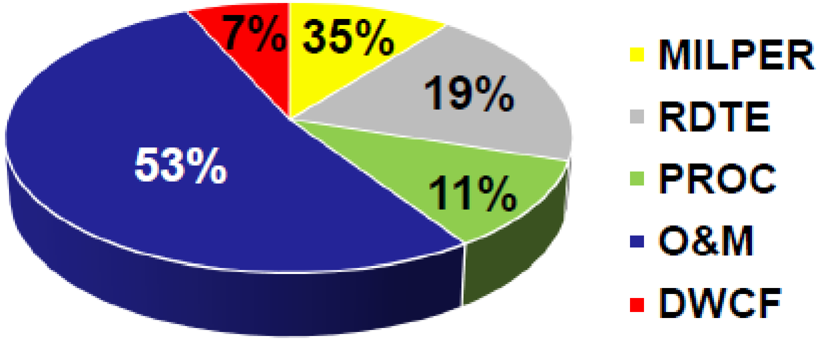
($M)	FY16En	FY17	
Air Force	1,545.6	1,990.5	+28%
Army	945.1	1,329.6	+41%
Navy	950.2	1,038.2	+9%
Defense-Wide	2,300.8	2,375.4	+3%
Total	5,741.7	6,733.7	+17%

($M)	FY16 En	FY17	
MILPER	637.3	713.3	+12%
RDTE	1,062.9	1,299.1	+22%
PROC	587.7	725.2	+23%
O&M	2,992.0	3,545.1	+18%
DWCF	462.2	451.0	-2%

FY17



FY17



MILPER:	Military Personnel
RDTE:	Research, Development, Test and Evaluation
PROC:	Procurement
O&M:	Operations and Maintenance
DWCF:	Defense Working Capital Fund

CYBERSECURITY BUDGET INCREASES AS THE PRIORITY INCREASES

2017

$2B

requested for cybersecurity procurement and RDT&E

Approved for Public Release

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.

Raytheon

A Look At Current State Proposal Requirements

Defense Platform/Embedded Program RFP Analysis

The analysis included 10 RFPs in 2016.

The following keywords were used to extract sections of the RFP Statement of Work and Sections L and M language.

Customers included:

- (3) Air Force (1) United States; (1) direct commercial sale, (1) Foreign Military Sale
- (4) Navy (2) United States; (2) direct commercial sale
- (3) Army (3) United States

KEYWORDS USED:
cyber
cyber security
cybersecurity
cyber hardening
cyber defense
cyber protection
information assurance
IA
program protection
system security
security assessment
risk management framework
RMF
vulnerability analysis
survivability
resiliency
DIACAP
INFOSEC

RFP SOW Analysis Results Summary

Request for Proposal, Statement of Work (SOW) Analysis Results Summary

CYBER RESILIENCY AND SECURE SYSTEMS RELEVANT REQUIREMENTS – HOLISTIC PROGRAM PROTECTION

							FMS	DCS	International	International
Program Protection	Navy #1	Navy #2	Army #1	Army #2	Army #3	AirForce #1	Air Force #2	Navy #3	International Customer #1	Navy #4
	x	x	x	x	x	x	x	x	x	x
• Program Protection Plan (PPP) development and implementation • Systems security Architecture • Software assurance • Secure coding • Information Assurance (IA) • Cyber hardening • Computer Network Defense (CND) • Embedded system security	Cybersecurity Plan	DFARS CDI	PPiP	Cybersecurity	Cybersecurity	Program Protection Plan	References System Security but really cybersecurity	**Cyber resiliency** (not specific words)	**Resiliency**	Cyber **resiliency**
			Critical Functional Analysis	PPiP	Anti-tamper	Cyber **Resilient Architecture**	**PPiP**	cybersecurity	System Security Architecture	Cyber security system
			Cybersecurity	**SwA**	Defense Exportability Features	Cybersecurity	**Validation Plans**		Security Management Plan (Emphasis on cybersecurity)	
			System Security Plan	**Key Management**		Software Assurance			Lifecycle considerations for security	
						Anti-tamper			Computer Network Defense	
						SCRM (Trusted Access Program Office, TAPO)			Cyber Hardening	
						Validation & Verification			Information Assurance	

How many cyber resiliency and system security relevant SOW requirements made the transition to Section L and Section M?

Section L and Section M

- Section L: Instructions, Conditions and Notices to Bidders
- Section M: Evaluation Factors and Rating Methodology

How many cyber resiliency and/or system security relevant SOW requirements made the transition to Section L and Section M?

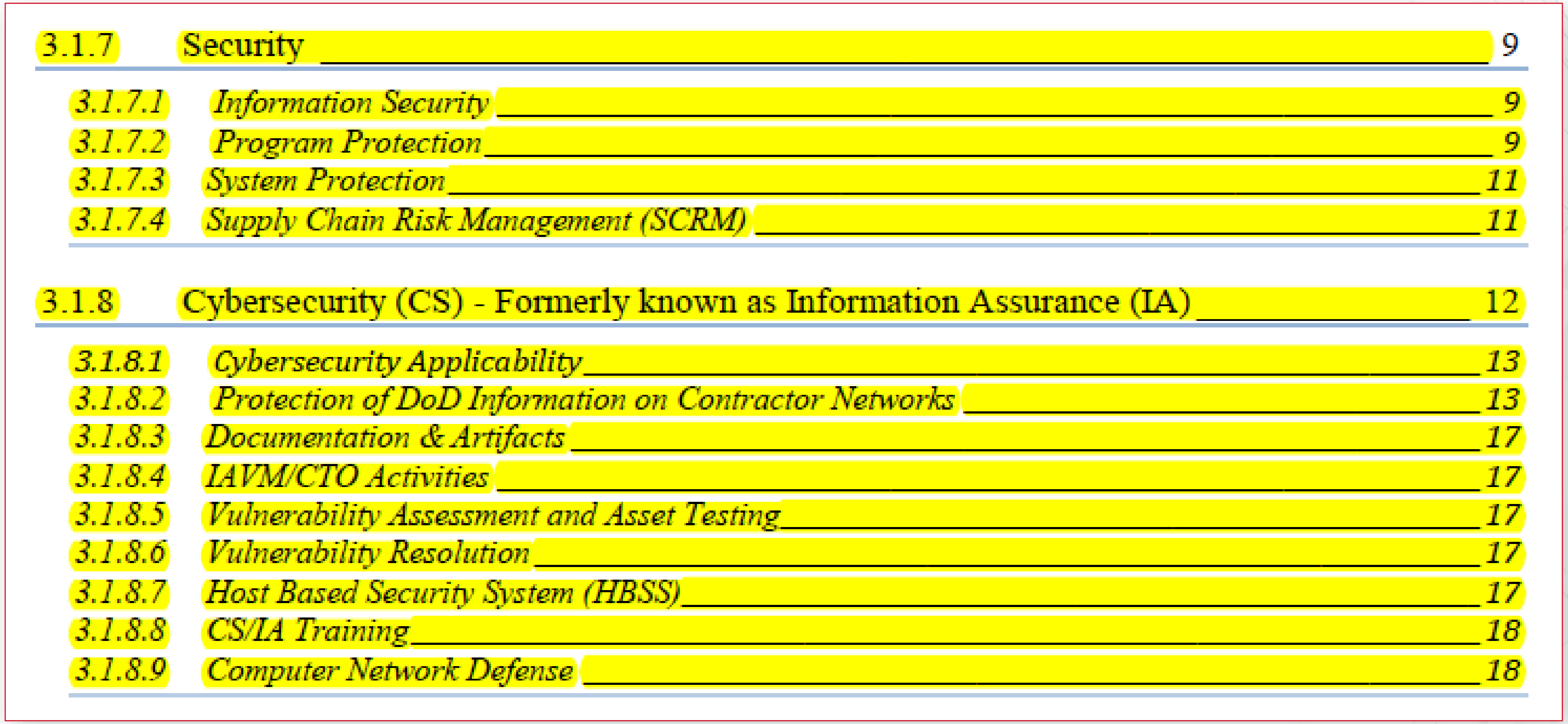
ZERO

Opportunity for Improvement

- Flow and consistency
  - Seems like multiple authors
- Recommend broad coverage first then specific security specialties
  - Program protection
    - System security engineering
      - Including architecture and resiliency
    - Software assurance
    - Cybersecurity
    - Anti-tamper
    - Supply Chain risk management
    - General program security
- Detailed requirements should be included within each of the security specialties
- Presence of system security or holistic program protection within Sections L and M

Review of a Sample RFP

First-glance SOW outline looks promising:



Cybersecurity / System Security has a Presence!

Deeper Review

3.1.7 Security

3.1.7 SECURITY

The contractor shall ensure coverage, by a Facility Security Officer (FSO) and an Information Assurance Officer/Information System Security Officer (IAO/ISSO), at the contractor and deployment site. The contractor shall prepare and implement a Site Security Management Plan (SSMP) (CDRL A010). The contractor shall work with the site commander on coordination of facility access required by the contractor and its sub-contractors. The contractor shall provide the Government access to all existing security-related data and documentation.

3.1.7.1 INFORMATION SECURITY

The contractor shall ensure that cleared subcontractor facilities shall schedule and conduct annual Information Security Program Reviews (ISPRs) and self-inspections. Serious deficiencies at the subcontractor location shall be reported to the contractor ...

Deeper Review

3.1.7 Security

3.1.7.2 Program Protection

The contractor shall plan and implement an Acquisition System Protection program encompassing acquisition security, **program protection, supply chain risk management and systems security engineering** for this contract based upon the requisite Program Protection Plan (PPP) and threat documents provided by XXX. The contractor shall generate, update, maintain and implement a Program Protection Implementation Plan (PPIP) (CDRL A011) which will be a stand-alone document for this contract. The PPIP shall include compliance implementation planning provided PPP, **DoDI 5200.39, DoDI 5200.44**, DoD 5200.1-M, SI 538-02, DoDM 5200.01, **DoDI 8500.01**, DoD 5200.8-R, CJCSI 6510.01F, CJCSI 3210.01B, and CNSSP 11. The contractor shall provide inputs to and support Government security analyses, including **system security analyses**, the **System Vulnerability Analysis (SVA), Operations Security (OPSEC) Plan, System Security Engineering (SSE)** requirements analysis, and **Cybersecurity/Computer Network Defense (CND) technical assessments.** The contractor shall support government Protection Assessment Reviews (PAR), security audits and **Program Protection Working Groups**. The contractor shall develop Program Protection training plans and conduct contractor training of **how to assess criticality of technologies** and **mitigate Critical Program Information (CPI) risks** from known or postulated threats IAW government issued PPPs. The contractor shall conduct a CPI assessment. The contractor shall conduct annual self-assessments to evaluate program adherence to PPIP and processes (ADP 004).

Deeper Review

3.1.7 Security

3.1.7.2 Program Protection (cont.)

The contractor shall develop and implement security policy and procedures. The contractor shall provide self-assessment reports to the YYY program office and YYY Industrial Security Office no later than 30 days after the completion of the assessment. The contractor shall provide government updates on implementing the XXX SSE requirements the MMM ES. The contractor shall maintain weapon system security features using established System Security Engineering processes DoD 5200.1-M Acquisition Systems Protection Program, DoDI 5000.2, Defense Acquisition Guidebook, MIL-HDBK-1013/1A Design Guidelines for Physical Security of Facilities, DoDM 5200.01 Information Security Program, DoD 5200.08R Physical Security Program, Committee on National Security Systems Advisory Memorandum (CNSSAM) TEMPEST 1-13 RED/BLACK Installation Guidance, Committee on National Security Systems 387 (CNSS) Advisory Memorandum Tempest 01-02, National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, Common Criteria and National Security Telecommunications and Information Systems Security Policy (NSTISSP) Number 11. The contractor shall develop SSE requirements, System Connection Authorization Requirements documents, and Security Accreditation Agreements documents. The contractor shall comply with security requirements IAW DoDI 8500.01 (Cybersecurity), DoDI 8510.01 (Risk Management Framework for DoD Information Technology), and the NSA Guide for Addressing Malicious Code Risk, and be accredited by the Authorizing Official (AO) prior to operation. The contractor shall provide a Technology Control Plan (TCP) for concurrence to MMM EIR, before submitting to Defense Security Services (DSS) for approval, within 90 days of contract award, if a TCP is required.

Deeper Review

3.1.7 Security

3.1.7.4 SUPPLY CHAIN RISK MANAGEMENT (SCRM)

The contractor shall assist the government in conducting a Criticality Analysis IAW DoDI 5200.44 immediately following the Software/M&S PDR to identify XYZ mission critical functions and Information and Communications Technology (ICT) critical components of the ZZZ system elements as requested. The Prime contractor shall submit to and participate in unannounced government audits into their supply chain activities no more three times per year –unless unacceptable supply chain practices are identified by the Government. The contractor shall demonstrate 1.) Visibility into its supply chain for critical components and materials. 2.) Understanding of the risks to that supply chain

3.) Implementation or plans to implement risk mitigations to counter those risks documented in the PPIP.

For all subcontracts involving the procurement of Critical Components identified in the Government PPP, the Prime contractor shall flow down requirements for supply chain risk management detailed in section below. The Prime contractor shall ensure vulnerabilities and discrepancies identified by subcontractors and lower tier vendors are reported to the XXX Supply Chain Risk Management/Trusted Systems and Networks Integration Council.

The Prime contractor shall only procure logic bearing components identified on the Critical Components List from vendors accredited by the Defense Microelectronic Activity (DMEA) (http://www.dmea.osd.mil/trustedic.html) or request an exception in writing prior to procurement to the ZZZ COTR and YYY with a justification as to why the component could not be procured from an accredited DMEA supplier. The contractor shall continuously monitor the Program Critical Components List for impact of YYY SCRM Advisories, Government-Industry Data Exchange Program (GIDEP) Alerts, and similar information from other programs.

Deeper Review

Supply Chain Risk Management (cont)

3.1.7.4 SUPPLY CHAIN RISK MANAGEMENT (SCRM)

The contractor shall prepare an SCRM Impact Statement (ADP 005) for each ZZZ SCRM Advisory for which a response is required containing the following:

a. ZZZ SCRM Advisory Number,

b. Points of Contact for Information,

c. Confirmation of the presence of the affected component,

d. System and subassemblies impacted,

e. Description of the function performed by the component,

f. Physical locations of the component,

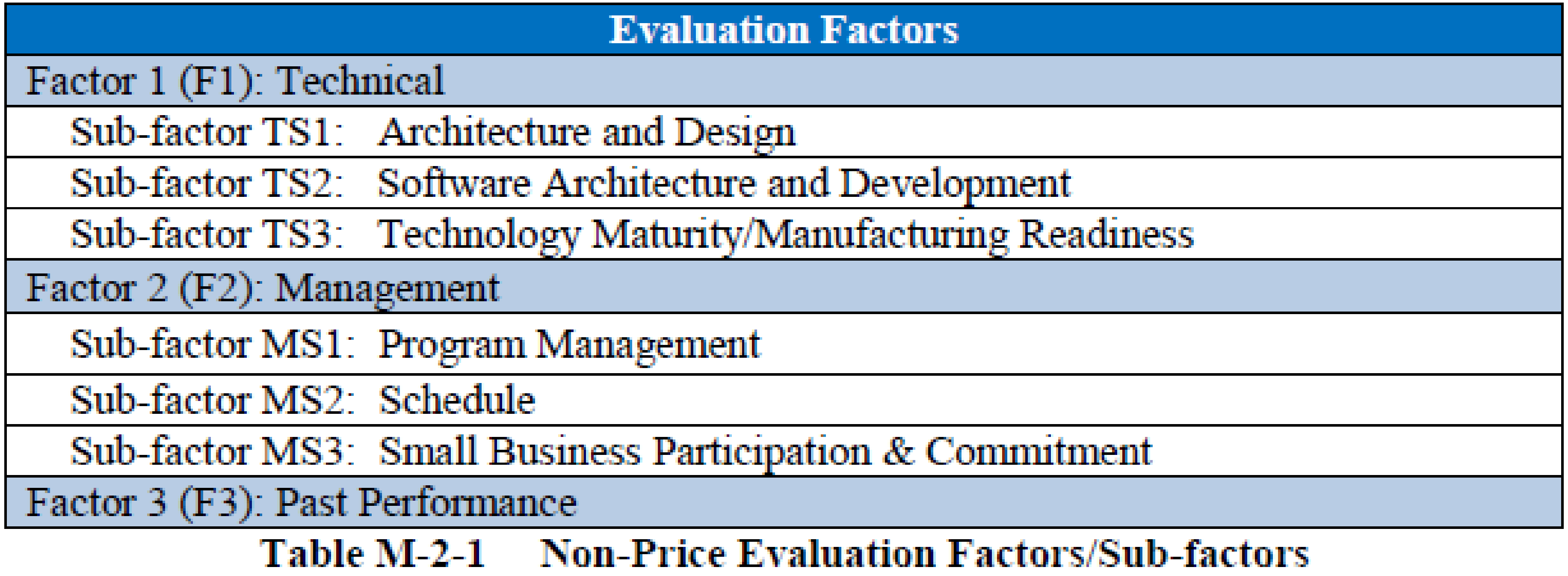
g. Status of the component

Impact statements shall be submitted to the ZZZ SCRM Advisory Coordinator listed on the advisory. The contractor shall follow the response instructions listed on the advisory.

The provisions of this SOW shall be included in the solicitations and subcontracts for all suppliers, suitably modified to identify the security risks suppliers must address to ensure the protection of CPI and critical components within the supply chain.

Raytheon

Section M, Factor and Sub-factor Weighting



Evaluation Factors
Factor 1 (F1): Technical
Sub-factor TS1: Architecture and Design
Sub-factor TS2: Software Architecture and Development
Sub-factor TS3: Technology Maturity/Manufacturing Readiness
Factor 2 (F2): Management
Sub-factor MS1: Program Management
Sub-factor MS2: Schedule
Sub-factor MS3: Small Business Participation & Commitment
Factor 3 (F3): Past Performance

Table M-2-1 Non-Price Evaluation Factors/Sub-factors

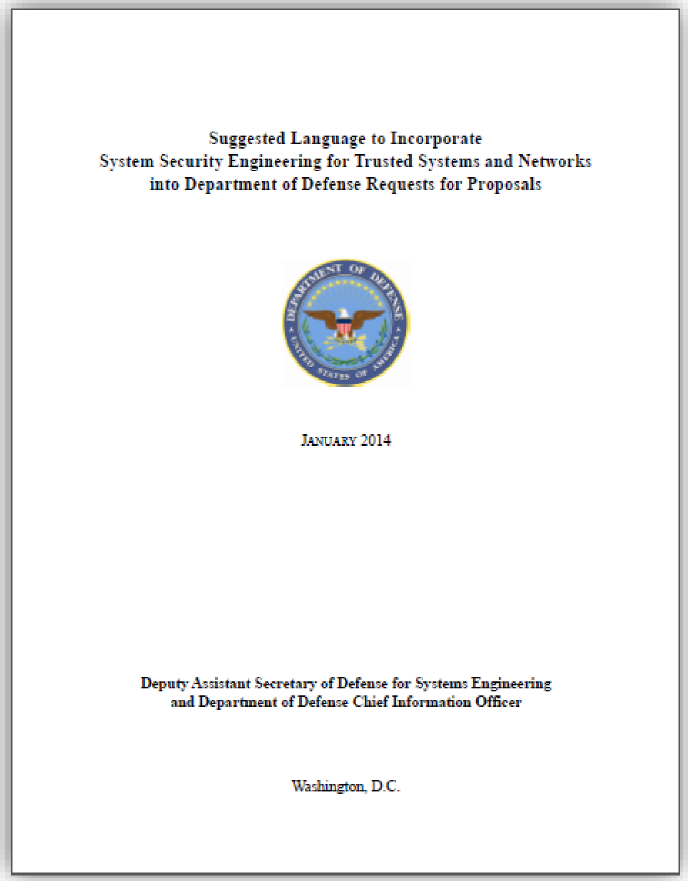
Increases in weight/importance

Security must be included within the evaluation criteria if you want anything related to System Security Engineering, Software Assurance, Cybersecurity, Security Relevant Supply Chain Risk Management, Cyber Resiliency, Cybersecurity Testing, Anti-tamper, etc., etc., etc.

Opportunity for Improvement

- Flow and consistency
  - Seems like multiple authors
- Recommend broad coverage first then specific security specialties
  - Program protection
    - System security engineering
      - Including architecture and resiliency
    - Software assurance
    - Cybersecurity
    - Anti-tamper
    - Supply Chain risk management
    - General program security
- Detailed requirements should be included within each of the security specialties
- Presence of system security or holistic program protection within Sections L and M

Sample of Existing Proposal Guidance

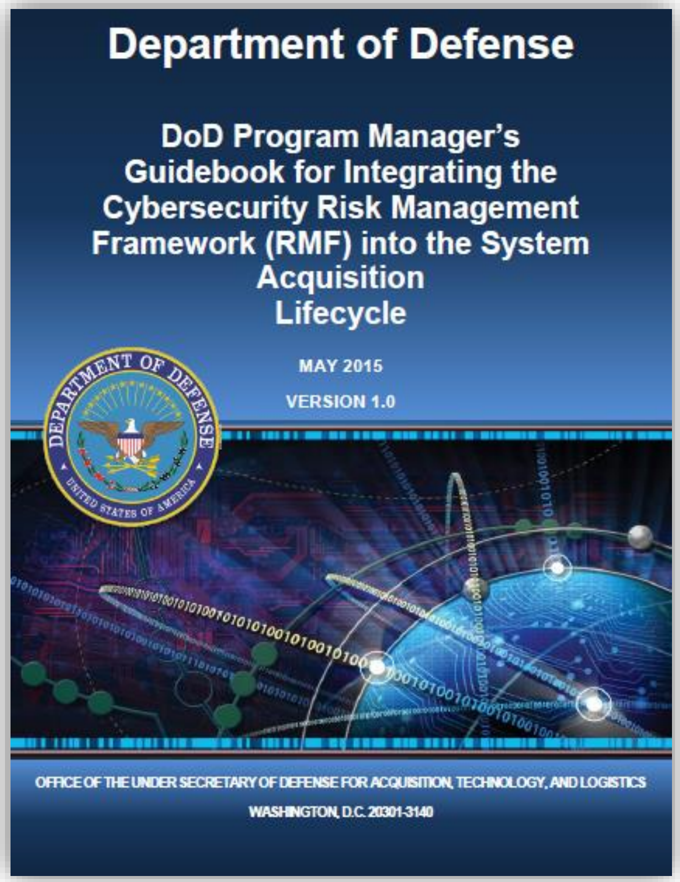


Suggested Language to Incorporate
System Security Engineering for Trusted Systems and Networks
into Department of Defense Requests for Proposals

JANUARY 2014

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

Washington, D.C.



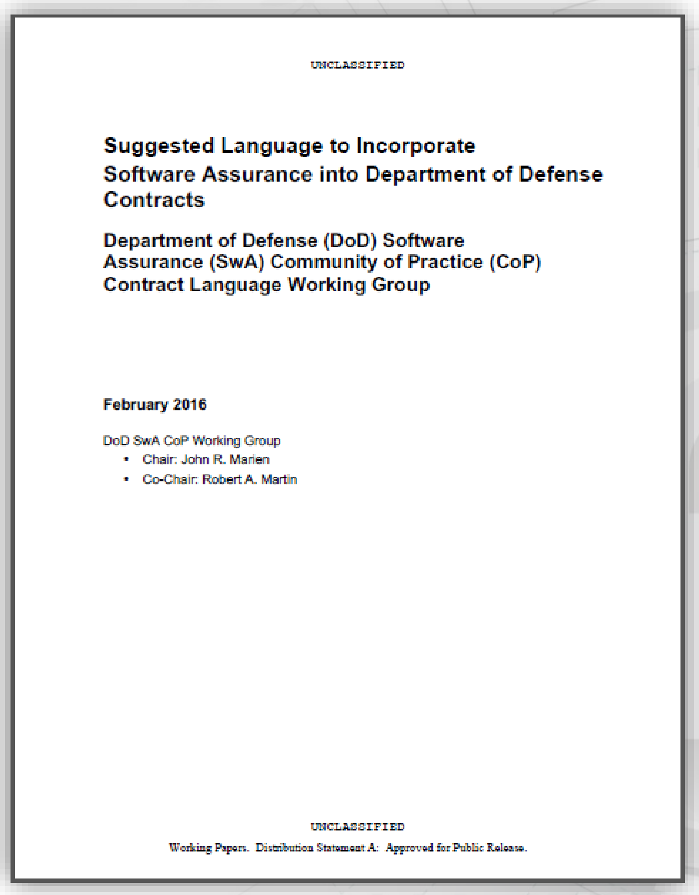
Department of Defense

DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle

MAY 2015

VERSION 1.0

OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
WASHINGTON, D.C. 20301-3140



UNCLASSIFIED

Suggested Language to Incorporate
Software Assurance into Department of Defense
Contracts

Department of Defense (DoD) Software
Assurance (SwA) Community of Practice (CoP)
Contract Language Working Group

February 2016

DoD SwA CoP Working Group
- Chair: John R. Marien
- Co-Chair: Robert A. Martin

UNCLASSIFIED

Working Papers. Distribution Statement A: Approved for Public Release.

http://www.acq.osd.mil/se/initiatives/init_pp-sse.html
Detailed excerpts in backup slides.

Channel the Energy and Contribute to the Solution

- There isn't a lack of acquisition proposal guidance
  - Too much guidance has led to similar results as a lack of guidance
  - Lots of well intentioned rice bowls contributing to perspective specific guidance
- We need a holistic integrated framework for program protection proposal guidance
- Start by developing a holistic program protection presence within Sections L and M
  - This outline can be the foundation to develop the details of the security specialty requirements across the life-cycle within the SOW
- The requirements details can be tailored per program
- We don't have a technology problem

Driving a holistic approach and consistency within Sections L and M could potentially be one of the most impactful actions this community could take

Proposed

Language for Sections L and M

Raytheon

- **Goal** is to ensure cyber resiliency and system security presence within every DoD platform and embedded system proposal
- Considerations:
  - Consistent with existing DoD policy
  - Agnostic to service or DoD customer
  - Agnostic to platform type
  - Flexibility to support legacy and “new start” programs
  - Concise language to minimize impact to proposal page counts
  - Tied to existing performance metrics and KPP

Raytheon

Consistent with DoD 5000.02

DoDI 5000.02, January 7, 2015, Change 2, 02/02/2017, 99 Enclosure 3

13. Program Protection

Program protection is the integrating process for managing risks to DoD warfighting capability from foreign intelligence collection; from hardware, software, and cyber vulnerability or supply chain exploitation; and from battlefield loss throughout the system life cycle. Where a DoD capability advantage derives from a DoD-unique or critical technology, program protection manages and controls the risk that the enabling technology will be lost to an adversary. Where a DoD capability advantage derives from the integration of commercially available or custom-developed components, program protection manages the risk that design vulnerabilities or supply chains will be exploited to destroy, modify, or exfiltrate critical data, degrade system performance, or decrease confidence in a system. Program protection also supports international partnership building and cooperative opportunities objectives by enabling the export of capabilities without compromising underlying U.S. technology advantages.

Consistent with DoD 5000.02

Raytheon

DoDI 5000.02, January 7, 2015, Change 2, 02/02/2017, 99 Enclosure 3 (cont)

13. Program Protection

a. PPP. Program managers will employ system security engineering practices and prepare a PPP to guide their efforts and the actions of others to manage the risks to critical program information and mission-critical functions and components associated with the program.

b. Countermeasures. Program managers will describe in their PPP the program's critical program information and mission-critical functions and components; the threats to and vulnerabilities of these items; the plan to apply countermeasures to mitigate associated risks; and planning for exportability and potential foreign involvement. Countermeasures should include anti-tamper, exportability features, security (including cybersecurity, operations security, information security, personnel security, and physical security), secure system design, supply chain risk management, software assurance, anti-counterfeit practices, procurement strategies, and other mitigations in accordance with DoD Instruction 5200.39 (Reference (ai)), DoD Instruction 5200.44 (Reference (aj)), and DoD Instruction 8500.01 (Reference (x)). Program managers will submit the program's Cybersecurity Strategy as part of every PPP. Countermeasures should mitigate or remediate vulnerabilities throughout the product life cycle, including design, development, developmental and operational testing, operations, sustainment, and disposal.

PROPOSED

Acquisition Instructions to Industry

- Section L
  - Present the system security view of the platform architecture which enables system resiliency in a cyber contested environment
  - Present the critical mission thread analysis methodology which identifies the system mission critical functions and system mission critical components (hardware, software, and firmware) directly effecting KPPs.
  - Present the system security risk assessment methodology
  - Present the system security risk mitigation and countermeasure approach
  - Present the verification and validation approach to prove effectiveness of system security and system survivability in a cyber contested environment
  - Present how system security has been integrated into lifecycle considerations

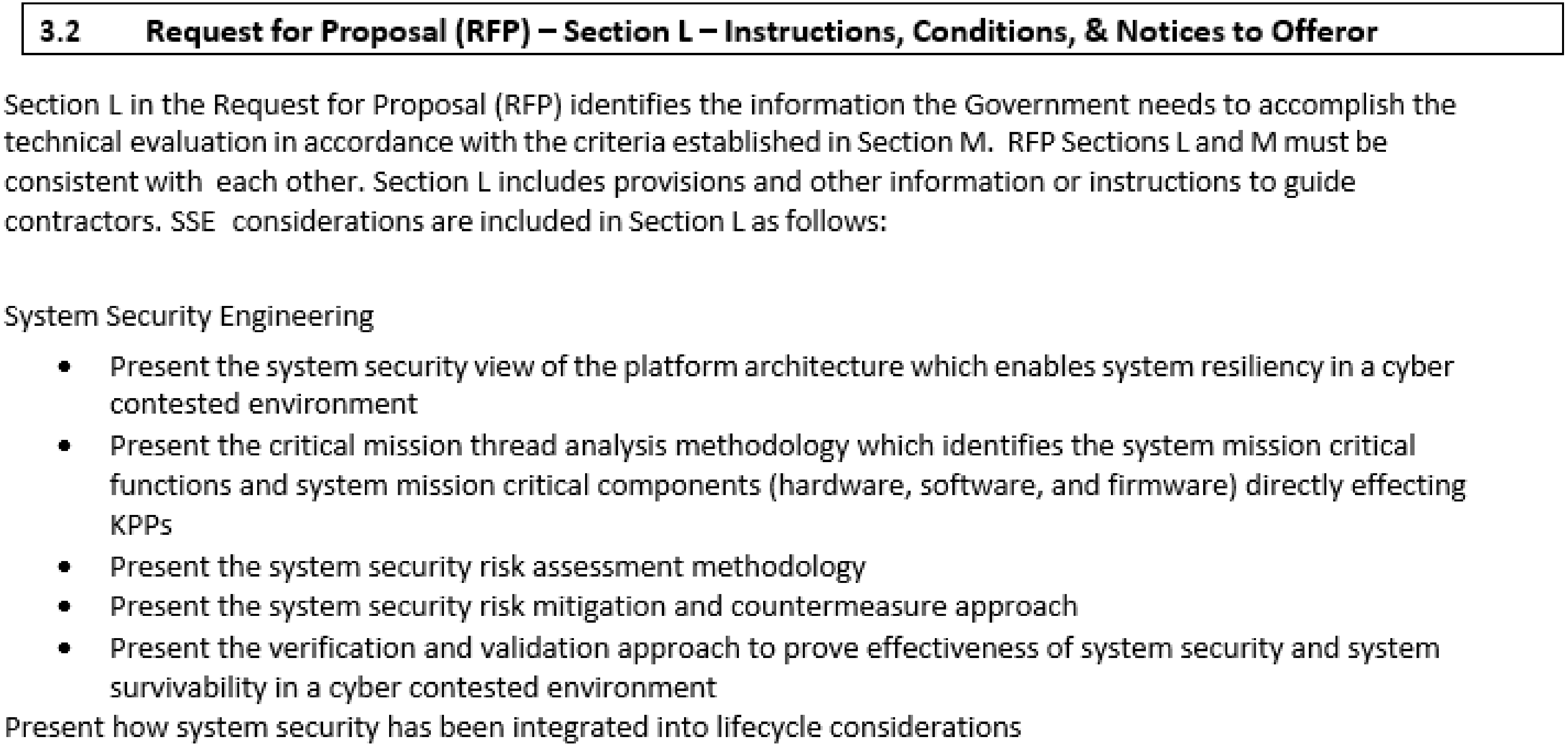
PROPOSED

Acquisition Instructions to Industry

Raytheon

- Section M *(one-to-one mapping to section L)*
  - The proposal demonstrates that the system security view of the platform architecture provides sufficient details of the approach to support (future) assessments of cyber resiliency, system security, and system survivability to meet the KPPs while operating in a cyber contested environment
  - The proposal demonstrates that the critical mission thread analysis methodology directly contributes to the identification of system mission critical functions and system mission critical components (hardware, software and firmware) identification
  - The proposal demonstrates that the system security risk assessment methodology directly contributes to the system security risk mitigation approach
  - The proposal demonstrates the system security risk mitigation approach supports the decision making process to reduce the system security risks impacting KPPs
  - The proposal demonstrates that the verification and validation approach will provide assurance that the system security requirements have been meet
  - The proposal demonstrates that system security lifecycle considerations have been included in the overall system lifecycle plan

NDIA SSE Committee Review & Final Recommendation



3.2 Request for Proposal (RFP) – Section L – Instructions, Conditions, & Notices to Offeror

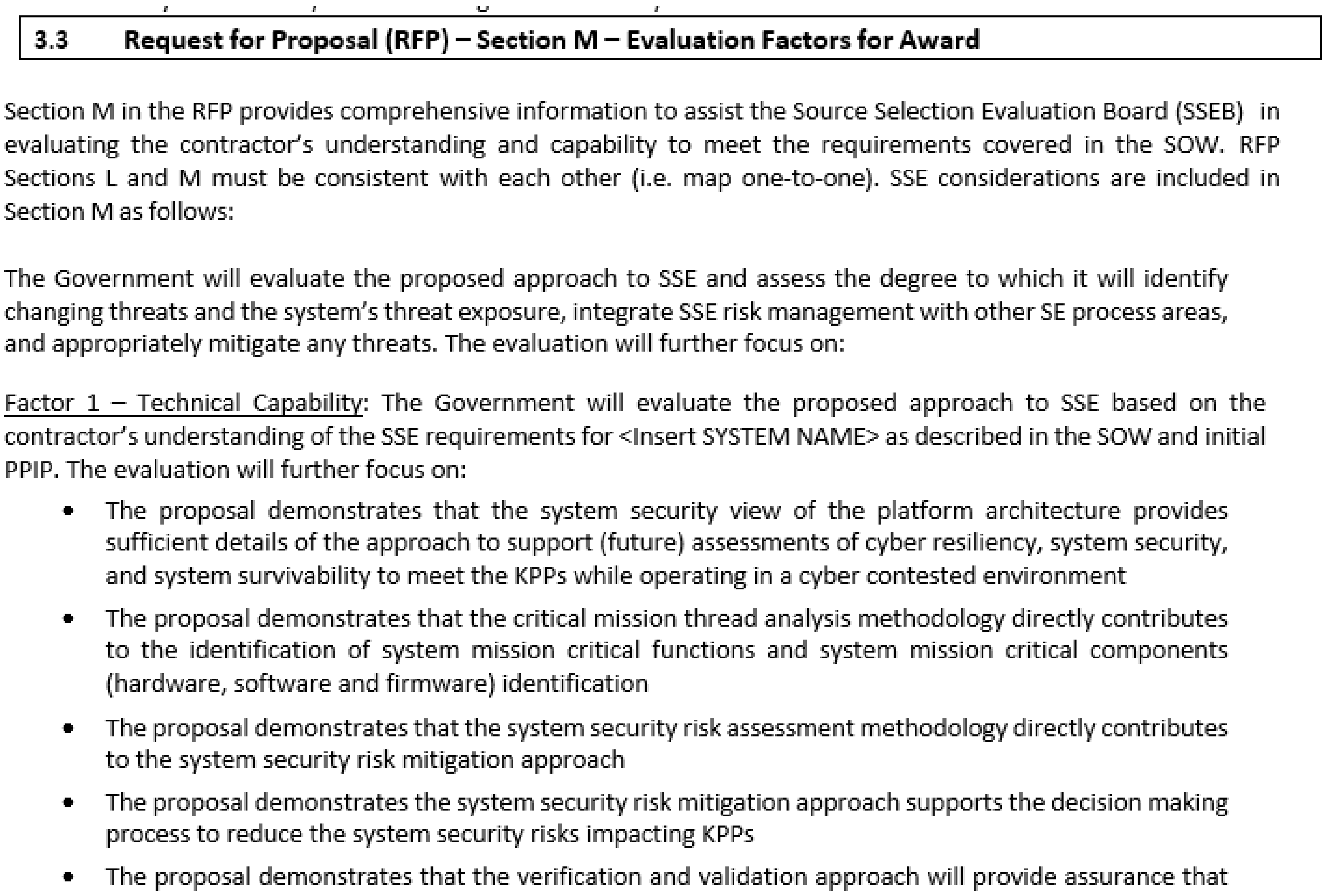
Section L in the Request for Proposal (RFP) identifies the information the Government needs to accomplish the technical evaluation in accordance with the criteria established in Section M. RFP Sections L and M must be consistent with each other. Section L includes provisions and other information or instructions to guide contractors. SSE considerations are included in Section L as follows:

System Security Engineering

- Present the system security view of the platform architecture which enables system resiliency in a cyber contested environment
- Present the critical mission thread analysis methodology which identifies the system mission critical functions and system mission critical components (hardware, software, and firmware) directly effecting KPPs
- Present the system security risk assessment methodology
- Present the system security risk mitigation and countermeasure approach
- Present the verification and validation approach to prove effectiveness of system security and system survivability in a cyber contested environment

Present how system security has been integrated into lifecycle considerations

NDIA SSE Committee Review & Final Recommendation



3.3 Request for Proposal (RFP) – Section M – Evaluation Factors for Award

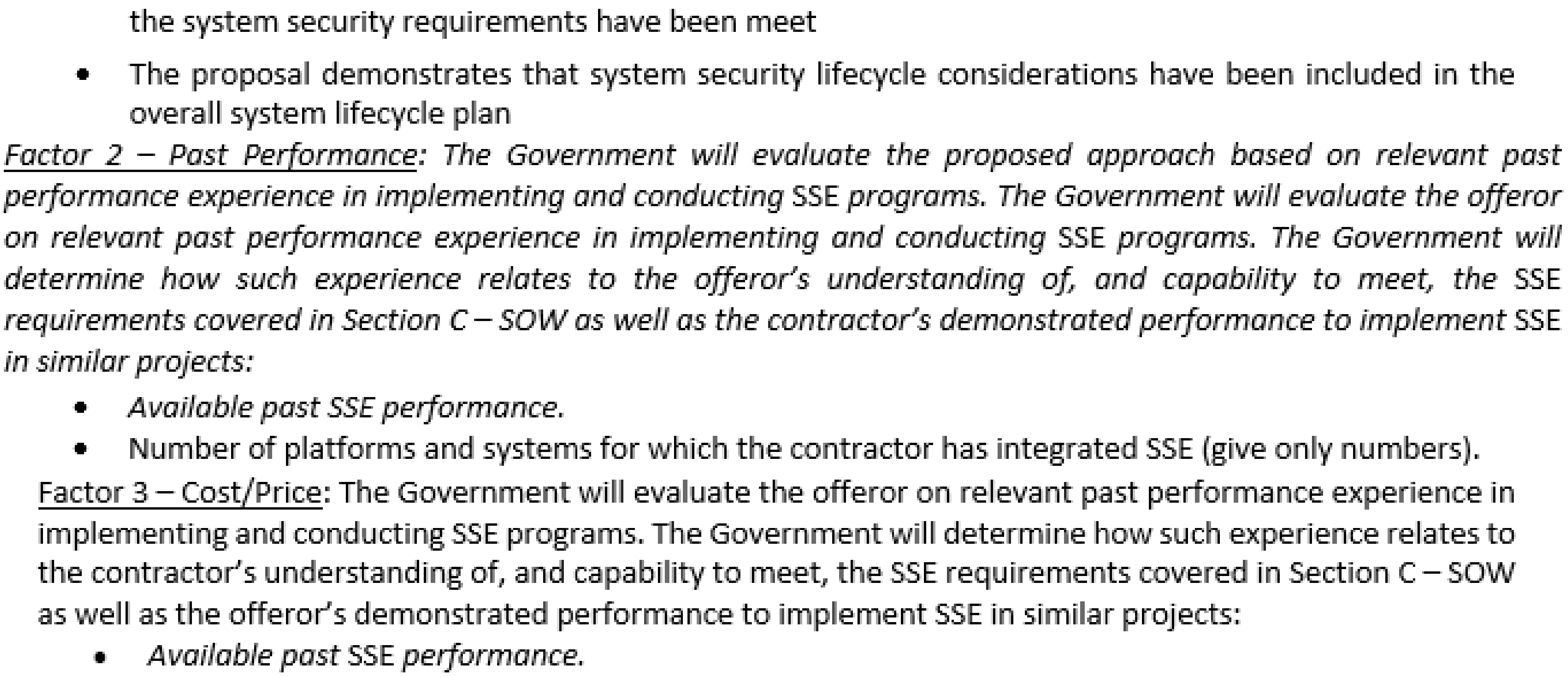
Section M in the RFP provides comprehensive information to assist the Source Selection Evaluation Board (SSEB) in evaluating the contractor's understanding and capability to meet the requirements covered in the SOW. RFP Sections L and M must be consistent with each other (i.e. map one-to-one). SSE considerations are included in Section M as follows:

The Government will evaluate the proposed approach to SSE and assess the degree to which it will identify changing threats and the system's threat exposure, integrate SSE risk management with other SE process areas, and appropriately mitigate any threats. The evaluation will further focus on:

Factor 1 – Technical Capability: The Government will evaluate the proposed approach to SSE based on the contractor's understanding of the SSE requirements for <Insert SYSTEM NAME> as described in the SOW and initial PPIP. The evaluation will further focus on:

- The proposal demonstrates that the system security view of the platform architecture provides sufficient details of the approach to support (future) assessments of cyber resiliency, system security, and system survivability to meet the KPPs while operating in a cyber contested environment
- The proposal demonstrates that the critical mission thread analysis methodology directly contributes to the identification of system mission critical functions and system mission critical components (hardware, software and firmware) identification
- The proposal demonstrates that the system security risk assessment methodology directly contributes to the system security risk mitigation approach
- The proposal demonstrates the system security risk mitigation approach supports the decision making process to reduce the system security risks impacting KPPs
- The proposal demonstrates that the verification and validation approach will provide assurance that

NDIA SSE Committee Review & Final Recommendation



the system security requirements have been meet

- The proposal demonstrates that system security lifecycle considerations have been included in the overall system lifecycle plan

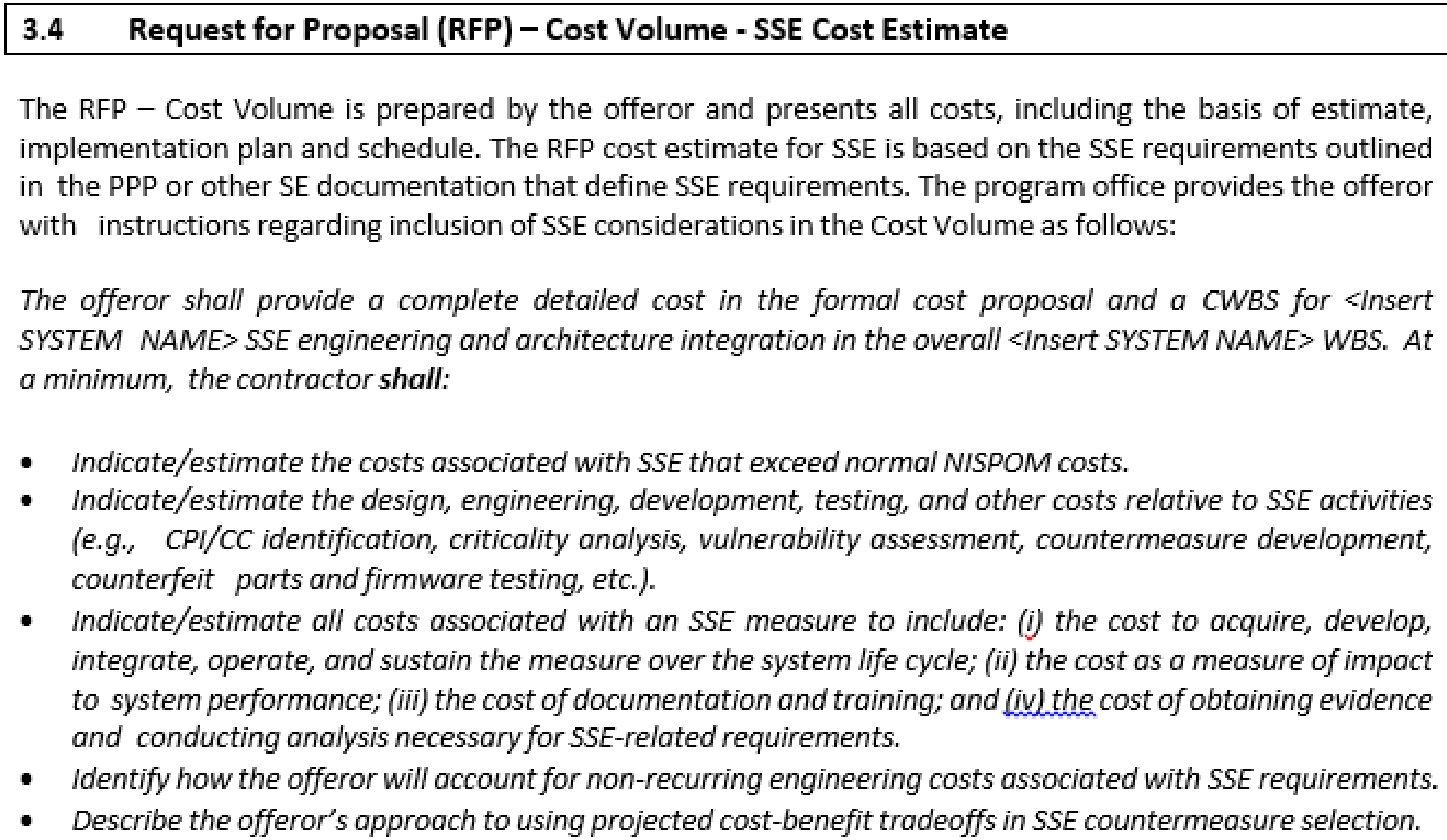
Factor 2 – Past Performance: The Government will evaluate the proposed approach based on relevant past performance experience in implementing and conducting SSE *programs. The Government will evaluate the offeror on relevant past performance experience in implementing and conducting* SSE *programs. The Government will determine how such experience relates to the offeror's understanding of, and capability to meet, the* SSE *requirements covered in Section C – SOW as well as the contractor's demonstrated performance to implement* SSE *in similar projects:*

- *Available past SSE performance.*
- Number of platforms and systems for which the contractor has integrated SSE (give only numbers).

Factor 3 – Cost/Price: The Government will evaluate the offeror on relevant past performance experience in implementing and conducting SSE programs. The Government will determine how such experience relates to the contractor's understanding of, and capability to meet, the SSE requirements covered in Section C – SOW as well as the offeror's demonstrated performance to implement SSE in similar projects:

- *Available past* SSE *performance.*

NDIA SSE Committee Review & Final Recommendation



3.4 Request for Proposal (RFP) – Cost Volume - SSE Cost Estimate

The RFP – Cost Volume is prepared by the offeror and presents all costs, including the basis of estimate, implementation plan and schedule. The RFP cost estimate for SSE is based on the SSE requirements outlined in the PPP or other SE documentation that define SSE requirements. The program office provides the offeror with instructions regarding inclusion of SSE considerations in the Cost Volume as follows:

The offeror shall provide a complete detailed cost in the formal cost proposal and a CWBS for <Insert SYSTEM NAME> SSE engineering and architecture integration in the overall <Insert SYSTEM NAME> WBS. At a minimum, the contractor ***shall:***

- *Indicate/estimate the costs associated with SSE that exceed normal NISPOM costs.*
- *Indicate/estimate the design, engineering, development, testing, and other costs relative to SSE activities (e.g., CPI/CC identification, criticality analysis, vulnerability assessment, countermeasure development, counterfeit parts and firmware testing, etc.).*
- *Indicate/estimate all costs associated with an SSE measure to include: (i) the cost to acquire, develop, integrate, operate, and sustain the measure over the system life cycle; (ii) the cost as a measure of impact to system performance; (iii) the cost of documentation and training; and (iv) the cost of obtaining evidence and conducting analysis necessary for SSE-related requirements.*
- *Identify how the offeror will account for non-recurring engineering costs associated with SSE requirements.*
- *Describe the offeror's approach to using projected cost-benefit tradeoffs in SSE countermeasure selection.*

Final Thoughts

- Perception versus reality
- Terminology problem. I don’t think this can be solved with more policy and guidance. This is a culture challenge.
  - System security
  - Cybersecurity
  - System security plan
  - Cybersecurity strategy
  - Holistic program protection
- Draft RFP is too late
  - Industry is shy to ask specific cyber/system security specific questions
- Need to identify who can drive consistency in standard proposal structure?
  - Is this something we can drive per Service (AF, Navy, Army, MDA)

Backup