



**DEPARTMENT OF DEFENSE**  
**Defense Contract Management Agency**

**INSTRUCTION**

**Software Acquisition Management**

**Engineering and Analysis Directorate**  
**DCMA-EA**

**DCMA-INST 203**  
**June 25, 2013**

---

**1. PURPOSE.** This Instruction:

- a. Replaces the existing DCMA Instruction (DCMA-INST) 203, “Software Acquisition Management” (Reference (a)).
- b. Incorporates the immediate policy change announced through DCMA Memorandum #12-238, Policy Change Notice, DCMA Instruction: “Software Acquisition Management,” (Reference (b)).
- c. Establishes policy, assigns responsibilities, and provides instruction for Software Acquisition Management (SAM) surveillance in carrying out DCMA Contract Administration Service functions.
- d. Is established in compliance with DoD Directive 5105.64 (Reference (c)) and all references listed.

**2. APPLICABILITY.** This Instruction applies to all DCMA activities performing SAM functions. Exceptions to this Instruction for classified contracts/programs, due to security requirements, shall be processed in accordance with (IAW) supplemental instructions maintained by the Special Programs Directorate.

**3. MANAGERS’ INTERNAL CONTROL PROGRAM.** IAW the DCMA-INST 710, “Managers’ Internal Control Program” (Reference (d)), this Instruction is subject to evaluation and testing. The process flowcharts are located at Appendices A, B, E, and G.

**4. RELEASABILITY – UNLIMITED.** This Instruction is approved for public release.

**5. PLAS CODES.**

- a. 071D – Software Surveillance Planning
- b. 071E – Execute Program/Facility Software Surveillance Plan
- c. 071F – Take Action as Appropriate
- d. 071Z – Any/Other 071 Tasks Not Listed/Required Above
- e. Other National Program Code: SW001 Software Support

**6. POLICY RESOURCE WEB PAGE.** <https://home.dcma.mil/POLICY/203r>

**7. EFFECTIVE DATE.** By order of the Director, DCMA, this Instruction is effective immediately.



Karron E. Small  
Executive Director  
Engineering and Analysis Directorate

## TABLE OF CONTENTS

**REFERENCES**.....9

### **CHAPTER 1 – POLICY**

1.1. Policy .....10  
    1.1.1. Software Acquisition Management (SAM) Mission.....10  
    1.1.2. SAM Functional Series .....10  
    1.1.3. SAM Process.....10  
1.2. Processes Excluded from the SAM Mission.....10  
    1.2.1. Written or Verbal Certifications .....10  
    1.2.2. Independent Verification and Validation (IV&V).....10  
    1.2.3. Deviations and Waivers .....11

### **CHAPTER 2 – ROLES AND RESPONSIBILITIES**

2.1. Software Engineering and Acquisition Management (SEAM) Center Representative..12  
2.2. CMO Director .....12  
2.3. Software Point of Contact (SW POC) .....12  
2.4. Software Professional (SP) .....12

### **CHAPTER 3 – SOFTWARE SURVEILLANCE PLANNING**

3.1. Software Surveillance Planning Overview .....14  
    3.1.1. Overarching Process Description.....14  
    3.1.2. Template Requirements .....14  
3.2. Software Contract Criticality (SCC).....16  
    3.2.1. Sub-process Description .....16  
    3.2.2. Determine SCC for Cost.....16  
    3.2.3. Determine SCC for Schedule.....16  
    3.2.4. Determine SCC for Technical.....17  
    3.2.5. Document Results .....17  
3.3. Letter of Delegation (LOD) Not Received .....17  
    3.3.1. Sub-process Description .....17  
    3.3.2. Request LOD from Higher Level SP .....18  
    3.3.3. Surveillance Not Required.....18  
    3.3.4. Contact the SEAM Center for Assistance.....18  
    3.3.5. Document Results .....18  
3.4. Contract/LOD Review .....19  
    3.4.1. Sub-process Description .....19  
    3.4.2. LOD Review .....19  
    3.4.3. Contract/Subcontract Review .....19  
    3.4.4. Review Statement of Work (SOW) .....21  
    3.4.5. Handling Discrepancies/Deficiencies .....22  
    3.4.6. Post Award Recommendation.....22

3.4.7. Document Results .....	22
3.5. Review DCMA/Suppliers' Historical Data .....	22
3.6. Review Available Planning Products.....	23
3.6.1. Planning Products .....	23
3.6.2. Documenting Supplier Planning Products .....	23
3.6.3. Documenting Acquisition Customer Planning Products .....	23
3.7. Identify DCMA Concerns Regarding Supplier Capability/Performance .....	23
3.7.1. Performance Areas.....	23
3.7.2. Risk Assessment .....	23
3.7.3. Document Results .....	23
3.8. Identify and Plan .....	24
3.8.1. Sub-process Description .....	24
3.8.2. Identify Core Technical, Cost, and Schedule Tasks/Activities.....	24
3.8.3. Identify CMO Unique Tasks/Activities .....	25
3.8.4. Document Results .....	26
3.9. Program Measures .....	26
3.9.1. Sub-process Description .....	26
3.9.2. No Measures Required.....	27
3.9.3. Identify Contractually Imposed Measures .....	27
3.9.4. Document Core Measures.....	27
3.9.5. Identify CMO Unique Measures.....	28
3.9.6. Document CMO Unique Measures.....	28
3.9.7. Identify Customer Unique Measures .....	28
3.9.8. Document Customer Unique Measures .....	28
3.9.9. Document Program Measures Engagement.....	28
3.9.10. Determining "Surveillance Frequency Needed for Program Measures.....	28
3.9.11. Document Data/Measure Specification .....	28
3.10. Identify Customer Unique Elements.....	29
3.10.1. Sub-process Description .....	29
3.10.2. Initiate Communications and Exchange Planning Information .....	29
3.10.3. Identify Customer POCs.....	30
3.10.4. Present the Tasks/Activities Documented in the SSP.....	30
3.10.5. Prime Contract Communications.....	30
3.10.6. Subcontract Communications .....	31
3.10.7. Identify Customer Reporting Requirements .....	31
3.10.8. Follow-up on Issues/Concerns .....	32
3.10.9. Review Acquisition Documents .....	32
3.10.10. Assess Customer Unique Tasks/Activities .....	32
3.10.11. Engage/Raise Issue .....	32
3.10.12. Raise Customer Unique Issues to Management.....	32
3.10.13. Document Customer Unique Engagement.....	32
3.10.14. Determining "Surveillance Frequency Needed" for Customer Unique Tasks/Activities .....	32
3.10.15. Document Results .....	33
3.11. DCMA Internal Performance Measures .....	33
3.12. Software Resource Estimation.....	33

3.12.1.	Sub-process Description .....	33
3.12.2.	Estimate Hours Per Task/Activity and Total Hours – Needed .....	33
3.12.3.	Assess Workload Documented in the SSP.....	34
3.12.4.	Resources Available.....	34
3.12.5.	Resources Not Available.....	35
3.12.6.	Adjust Other SSPs .....	35
3.12.7.	Determine Level of Effort (LOE) .....	36
3.12.8.	Document Results .....	36
3.13.	Complete the Software Surveillance Plan.....	36
3.13.1.	Sub-process Description .....	36
3.13.2.	Complete the Front Matter Section.....	36
3.13.3.	Non-editable Purpose.....	38
3.13.4.	Complete the Program/Contract Software Development Overview Section.....	38
3.13.5.	Software Development Risk(s).....	38
3.13.6.	Terms and Acronyms .....	39
3.13.7.	Validate Core Work .....	39
3.13.8.	Validate CMO Unique Work.....	39
3.13.9.	Validate Customer Unique Work.....	39
3.13.10.	Validate Program Measures Work.....	39
3.13.11.	Validate Instructions .....	39
3.13.12.	Complete a Software Surveillance Schedule .....	39
3.13.13.	Document Letter(s) of Delegation (LOD) .....	40
3.13.14.	Prepare the SSP for Formal Approval .....	40
3.13.15.	Engage in Surveillance .....	40
3.14.	Software Surveillance Plan (SSP) Approval.....	40
3.14.1.	Sub-process Description .....	40
3.14.2.	SW POC Review and Approval.....	41
3.14.3.	SEAM Center Feedback .....	41
3.15.	Customer Notification.....	42
3.15.1.	Sub-process Description .....	42
3.15.2.	Submit SSP to the Customer.....	42
3.15.3.	Raise to CMO Management to Resolve.....	42
3.16.	Issue Letter of Delegation (LOD) .....	43
3.16.1.	Sub-process Description .....	43
3.16.2.	Determine if an LOD is Required.....	43
3.16.3.	No LOD Required.....	43
3.16.4.	Issue LOD for DoD Related Work .....	44
3.16.5.	Issue LOD for Non-DoD Related Work .....	44
3.16.6.	Determine if the LOD is Accepted or Rejected .....	45
3.17.	Creating a Facility Software Surveillance Plan (Facility SSP).....	45
3.17.1.	Overarching Process Description.....	45
3.17.2.	Identify the Common Institutionalized Processes.....	46
3.17.3.	Document the Common Institutionalized Processes.....	47
3.17.4.	Document Facility SSP Surveillance Schedule(s) .....	47
3.17.5.	Contracts List Tab.....	47
3.17.6.	Complete the Facility SSP .....	47

3.17.7. Update the Revision History for each Contract, Program, or Lite SSP .....	47
3.17.8. Review All SSPs .....	48
3.17.9. Finalize Facility SSP .....	48
3.17.10. Finalize Contract, Program, or Lite SSPs .....	48
3.18. Requirements for Review Cycle .....	48
3.18.1. Annual Review Required .....	48
3.18.2. Immediate Review Required .....	48
3.18.3. Contract/Program Complete .....	48

## **CHAPTER 4 – EXECUTE THE SOFTWARE SURVEILLANCE PLAN**

4.1. Execute the Software Surveillance Plan Overview .....	50
4.1.1. Overarching Process Description .....	50
4.1.2. Required Template .....	50
4.2. Process Review .....	50
4.2.1. Sub-process Description .....	50
4.2.2. Determine Technique .....	51
4.2.3. Process Proofing Technique .....	51
4.2.4. Process Compliance Technique .....	52
4.2.5. Take Action as Appropriate .....	52
4.2.6. Document Results .....	53
4.2.7. Determine SSP Impact .....	53
4.3. Software Product Examination .....	53
4.3.1. Sub-process Description .....	53
4.3.2. Determine Product to Examine .....	53
4.3.3. Conduct Product Examination .....	54
4.3.4. Take Action as Appropriate .....	54
4.3.5. Document Results .....	55
4.3.6. Determine SSP Impact .....	55
4.4. Formal Reviews and Audits .....	55
4.4.1. Sub-process Description .....	55
4.4.2. Obtain Review/Audit Requirements .....	56
4.4.3. Ensure Supplier is Tracking Entrance Criteria .....	56
4.4.4. Participate in the Formal Review/Audit .....	57
4.4.5. Ensure Supplier is Tracking Exit Criteria and Resolving Action Items (AIs) .....	57
4.4.6. Report as Appropriate .....	57
4.4.7. Take Action as Appropriate .....	57
4.4.8. Document Results .....	58
4.4.9. Determine SSP Impact .....	58
4.5. Data Collection and Analysis .....	58
4.5.1. Sub-process Description .....	58
4.5.2. Collect and Analyze Data/Measures .....	59
4.5.3. Obtain the Data/Measures .....	59
4.5.4. Analyze Data/Measures .....	59
4.5.5. Take Action as Appropriate .....	60
4.5.6. Document Results .....	60

4.5.7. Determine SSP Impact.....	60
4.6. Accept Product.....	60
4.6.1. Sub-process Description .....	60
4.6.2. SPDP Certification.....	61
4.6.3. Verify Time, Method, and Place of Acceptance.....	61
4.6.4. Determine Acceptance Criteria.....	61
4.6.5. Evaluate Product Against Acceptance Criteria.....	61
4.6.6. Accept the Product.....	61
4.6.7. Take Action as Appropriate .....	61
4.6.8. Document Results .....	62
4.6.9. Determine SSP Impact.....	62

## CHAPTER 5 – TAKE ACTION AS APPROPRIATE

5.1. Take Action as Appropriate Overview .....	63
5.1.1. Overarching Process Description.....	63
5.1.2. Overarching Process Flowchart .....	63
5.2. Corrective Action Request (CAR).....	63
5.2.1. Sub-process Description .....	63
5.2.2. Sub-process Flowchart.....	63
5.2.3. Contractual Noncompliance Identified.....	63
5.2.4. Document Results .....	63
5.2.5. Determine SSP Impact.....	63
5.3. Continuous Improvement Opportunity (CIO) .....	64
5.3.1. Sub-process Description .....	64
5.3.2. Sub-process Flowchart.....	64
5.3.3. Continuous Improvement Opportunity Identified .....	64
5.3.4. Generate CIO and Document Actions Taken .....	64
5.3.5. Document Results .....	64
5.3.6. Determine SSP Impact.....	64
5.4. Report to Customer .....	64
5.4.1. Sub-process Description .....	64
5.4.2. Timely Reporting of Actual/Potential Impacts .....	65
5.4.3. Routine Reporting to Customer .....	65
5.4.4. Document Results .....	65
5.4.5. Determine SSP Impacts .....	66

## APPENDICES

Appendix A. Software Acquisition Management Mission Process Flowchart.....	67
Appendix B. Software Surveillance Planning Process Flowcharts .....	68
Appendix C. Software Risk Assessment .....	82
Appendix D. Data/Measure Life Cycle.....	87
Appendix E. Execute the Software Surveillance Plan Process Flowcharts.....	88
Appendix F. Process Review and Product Examination Goals.....	94
Appendix G. Take Action as Appropriate Process Flowcharts .....	100

**TABLES**

Table 1	Likelihood.....	83
Table 2	Consequence .....	84
Table 3	5 x 5 Risk Matrix .....	85
Table 4	Data/Measures Life-Cycle .....	87
Table 5	Process Review Goals.....	94
Table 6	Product Examination Goals .....	96

**GLOSSARY**

Definitions.....	104
Acronyms.....	106

## REFERENCES

- (a) DCMA-INST 203, “Software Acquisition Management,” December 2009 (hereby canceled)
- (b) DCMA Memorandum #12-238, Policy Change Notice, DCMA Instruction: “Software Acquisition Management,” August 2, 2012 (hereby canceled)
- (c) DoD Directive 5105.64, “Defense Contract Management Agency (DCMA),” January 10, 2013
- (d) DCMA-INST 710, “Managers’ Internal Control Program,” September 19, 2012
- (e) DCMA-PAM 55.2, “Engineering and Analysis guidance for hiring: Software Acquisition Management Resources,” February 20, 2013
- (f) DCMA-INST 501, “Policy Program,” September 20, 2012
- (g) DCMA Training Guide, “Software Professional Development Program (SPDP),” February 2010
- (h) DCMA-INST 205, “Major Program Support,” January 7, 2013
- (i) Part 700 of title 15, Code of Federal Regulations, “Defense Priorities and Allocations System (DPAS)”
- (j) DoD 4400.1-M, “Department of Defense Priorities and Allocation Manual,” February 21, 2002
- (k) DCMA “Delegation eTOOL”
- (l) DCMA “Electronic Contract Administration Request System (ECARS) eTOOL”
- (m) FAR 42.302(a), “Contract Administrative Functions”
- (n) FAR 42.202(f), “Special Surveillance”
- (o) DCMA “Electronic Data Workflow (EDW) Contract Data Workflow (CDW)” System
- (p) DCMA-INST 118, “Contracts – Initial Receipt and Review,” October 1, 2010
- (q) FAR 46.3, “Contract Clauses,” (aka: Government access rights/Inspection clauses)
- (r) DFARS 227.71, “Rights in Technical Data”
- (s) DFARS 227.72, “Rights in Computer Software and Computer Software Documentation”
- (t) FAR 24.1, “Protection of Privacy and Freedom of Information”
- (u) DFARS 239.71, “Security and Privacy for Computer Systems”
- (v) DCMA “Electronic Document Access (EDA)” System
- (w) DCMA “Contracts Receipt and Review (CRR) eTOOL”
- (x) FAR 42.502, “Selecting Contracts for Postaward Orientation”
- (y) DCMA-PAM 55.1, “Compiling, Approving, Submitting, and Closing Out the Software Surveillance Plan (SSP),” February 20, 2013
- (z) DCMA-INST 809, “Records Management,” May 1, 2009
- (aa) DCMA-INST 1201, “Corrective Action Process,” December 10, 2012
- (ab) DCMA enterprise “Corrective Action Request (CAR) eTOOL”
- (ac) DoD, “Risk Management Guide for DoD Acquisition,” August 2006

## CHAPTER 1

### POLICY

**1.1. POLICY.** This Instruction is applicable to all DCMA personnel assigned to perform technical surveillance on contracts involving the development or maintenance of software.

1.1.1. Software Acquisition Management (SAM) Mission. Ensure that our customers receive software products and/or systems with embedded software that meet or exceed contractual specifications/requirements, and provide our customers with the knowledge to allow them to make informed milestone and other on-going decisions relative to software cost, schedule, and technical performance.

1.1.2. SAM Functional Series. The SAM mission is performed by computer engineers (General Schedule (GS)-854), and information technology specialists (GS-2210), herein referred to as the Software Professional (SP). Guidance for hiring personnel within these series can be found in DCMA-PAM 55.2, "Engineering and Analysis guidance for hiring: Software Acquisition Management Resources" (Reference (e)), located under "Pamphlets" in the Guidance section on the Policy Resource Page.

1.1.3. SAM Process. The overarching process flowchart for performing the "Software Acquisition Management (SAM) Mission" can be found in Appendix A.

### 1.2. PROCESSES EXCLUDED FROM THE SAM MISSION.

1.2.1. Written or Verbal Certifications. DCMA Operations Directorate, regions, contract management offices (CMO), and SPs shall not issue, or provide to the supplier or suppliers' subcontractor(s) any written or verbal notification of any kind stating or implying any official DCMA certification or recognition that the supplier or suppliers' subcontractor(s) has/have obtained a specified level of competency/maturity based on any industry accepted/recognized capability model, such as the Capability Maturity Model Integrated (CMMI).

1.2.1.1. DCMA SPs may participate in capability or maturity assessments (such as the Standard CMMI Appraisal Method for Process Improvement (SCAMPI) methods A, B, or C).

1.2.1.2. When performing independent CMMI based surveillance or assessments, the SP is limited to identification and reporting of weaknesses and strengths observed.

1.2.2. Independent Verification and Validation (IV&V). DCMA Operations Directorate, regions, CMOs, and SPs shall not accept a request from an Acquisition Customer for the Operations Directorate, regions, CMO, or SP to be the responsible agent for conducting IV&V on a software development effort without obtaining the expressed written approval and authorization from the Director, DCMA.

1.2.2.1. Responsibility for IV&V is normally conducted by an agent specified in the contract. The agent may be identified as the Acquisition Customer's technical staff, an

independent agent within the suppliers' organization, or an independent services provider contracted by the Acquisition Customer or the supplier.

1.2.2.2. When the Acquisition Customer's technical staff has been identified in the contract as the responsible agent for conducting IV&V, DCMA SPs may support the Acquisition Customer's IV&V efforts as an advisor.

1.2.3. Deviations and Waivers. Any requests for deviations or waivers from this policy are to be submitted in accordance with DCMA-INST 501, "Policy Program" (Reference (f)).

## CHAPTER 2

### ROLES AND RESPONSIBILITIES

**2.1. SOFTWARE ENGINEERING AND ACQUISITION MANAGEMENT (SEAM) CENTER REPRESENTATIVE.** The SEAM Center representative is responsible for:

2.1.1. Reviewing Software Surveillance Plans (SSP) submitted to the SEAM Center for compliance to this Instruction, and providing feedback to the submitting SP.

2.1.2. Data mining the submitted SSPs to obtain information that can be used to assess agency wide workload, risk, performance, and identify need for policy improvements.

**2.2. CMO DIRECTOR.** The CMO director (or designee) is responsible for assigning an individual with the authority to perform the responsibilities specified in paragraph 2.3.

**2.3. SOFTWARE POINT OF CONTACT (SW POC).** The SW POC is responsible for:

2.3.1. Managing and issuing control numbers for SSPs developed for new contracts.

2.3.2. In coordination with the SP, reviewing the SSP to validate software resource estimation workload requirements and allocating resources to the SSP.

2.3.3. Reviewing all SSPs for accuracy, completeness, and compliance to this policy.

2.3.4. Approving all SSPs by digitally signing them, and submitting them to the SEAM Center.

2.3.5. Representing CMO management to resolve issues with internal and external customers for out-of-scope software surveillance tasks/activities the SP has been requested to perform.

**2.4. SOFTWARE PROFESSIONAL (SP).** The SP is responsible for:

2.4.1. Developing an SSP for each contract, subcontract, purchase order (PO), delivery order (DO), or other form of agreement they are assigned, submitting the SSP to the local SW POC for review and approval, and keeping the SSP up-to-date.

2.4.2. Executing the surveillance tasks/activities documented in the approved SSP IAW its embedded quarterly surveillance schedule.

2.4.3. Pending results of their surveillance activities, taking action as appropriate to include:

2.4.3.1. Issuing a Corrective Action Request (CAR) to the contractor when they independently identify contractual noncompliance's.

2.4.3.2. When appropriate, issuing a Continuous Improvement Opportunity (CIO) recommendation to the contractor when they independently observe a process/product that could be improved that is **not** subject to a contractual noncompliance.

2.4.3.3. Keeping the customer informed by providing status of the contractor's performance in meeting the terms of the contract, and reporting potential impacts on cost, schedule, and technical performance.

2.4.3.4. Enrolling in and actively pursuing certification as described in DCMA Training Guide, "Software Professional Development Program (SPDP)" (Reference (g)), located under the Training section on the Policy Resource Page.

## CHAPTER 3

### SOFTWARE SURVEILLANCE PLANNING

#### 3.1. SOFTWARE SURVEILLANCE PLANNING OVERVIEW.

3.1.1. Overarching Process Description. This chapter provides instruction on how to develop an SSP and is divided into two parts as follows:

- Part I - Describes the steps that are to be followed by the SP for planning and documenting the SSP (see paragraphs 3.2. through 3.16.)
- Part II - Provides the steps for planning and documenting an optional Facility SSP (see paragraph 3.17.)

3.1.1.1. The overarching process flowchart for “Software Surveillance Planning” can be found at Appendix B.

3.1.1.2. **NOTE:** While the process flowchart is depicted as being linear, the actual implementation of the activities may occur in parallel. For example, the SP may determine the Software Contract Criticality (see paragraph 3.2.) while conducting the Contract/Letter of Delegation (LOD) Review process (see paragraph 3.4.).

3.1.2. Template Requirements. For all contracts, subcontracts, POs, or other forms of agreement involving deliverable software (whether standalone, or embedded in the system, or end item component), the SP shall select and implement one of the following SSP templates:

3.1.2.1. Contract SSP. This is the default template that shall be used by the SP unless either the Program SSP or Lite SSP templates can be qualified for selection and implementation. This template addresses all SAM mission requirements for a single prime/subcontract.

3.1.2.2. Program SSP: This template may be selected and implemented by the SP to plan all SAM mission requirements for contracts/programs when the SP must, in addition to this Instruction, also adhere to DCMA-INST 205, “Major Program Support” (Reference (h)). This template may also be selected and implemented by the SP whenever the program/contract is expected to include the issuance of multiple related contracts, subcontracts, POs, DOs, or other forms of agreement for a single supplier/subcontractor within a single CMO. Exception: The SP shall not comingle DoD and non-DoD related work into a single Program SSP.

3.1.2.3. Lite SSP. This is a hybrid template that addresses all SAM mission requirements for a single contract, subcontract, PO, DO, or other form of agreement for a single supplier/subcontractor, for a single customer within a single CMO. It may be selected and implemented by the SP only for short term contracts when the entire software effort is 6 months or less.

3.1.2.4. The first worksheet tab in each of the above SSP templates is titled “Helper Guide” and it includes guidance on how to document the required planning information within the selected and implemented SSP template.

3.1.2.5. All Contract, Program, or Facility SSPs shall represent a 12-month planning life cycle.

3.1.2.6. All Lite SSPs shall represent from one 1 to a maximum of 6 months planning life cycle.

3.1.2.7. All Contract, Program, Lite, or Facility SSPs shall adhere to the review requirements described in paragraph 3.18.

3.1.2.8. Marking Requirements. All Contract, Program, Lite, or Facility SSPs shall adhere to the following:

3.1.2.8.1. Any task/activity identified in the SSP that will not occur during the 12-month planning cycle (6 months for Lite), the “Task/Activity Surveillance Status” cell shall be marked “N/A for this planning cycle” and all remaining cells for that task/activity shall be left blank.

3.1.2.8.2. Any task/activity identified in the SSP that has already occurred and will not be engaged in during the 12-month planning cycle (6 months for Lite), the “Task/Activity Surveillance Status” cell shall be marked “COMPLETED” and all remaining cells for that task/activity shall be left blank.

3.1.2.8.3. For Non-DoD Work. The SP shall ensure that any core technical, cost, schedule, or program measure related task/activity pre-identified in the SSP that was **not** required to be performed by the customer in the Memorandum of Agreement or Memorandum of Understanding (MOA/MOU), LOD, or **not** included as part of a host-nation/international agreement is **not** engaged in for surveillance. Thus, for any task/activity fitting this description, the SP shall mark the “Task/Activity Surveillance Status” cell with the term “WITHHELD by Customer/Delegating CMO” to denote this fact, and all remaining cells for that task/activity shall be left blank.

3.1.2.8.4. For DoD Work. The SP shall ensure that any core technical, cost, schedule, or program measure related task/activity pre-identified in the SSP that was specifically “Withheld” in writing by the customer, is **not** engaged in for surveillance. Thus, for any task/activity fitting this description, the SP shall mark the “Task/Activity Surveillance Status” cell with the term “WITHHELD by Customer/Delegating CMO” to denote this fact, and all remaining cells for that task/activity shall be left blank.

3.1.2.9. The Contract, Program, and Lite SSP templates are located under “Surveillance Planning” in the Policy Templates section on the Policy Resource Page.

### 3.2. SOFTWARE CONTRACT CRITICALITY (SCC).

3.2.1. Sub-process Description. This paragraph describes how the SP determines the SCC, which is a complexity rating that determines from a contract/project perspective, the core level of DCMA involvement. For each contract, subcontract, PO, DO, or other form of agreement, the SCC rating is determined. The SCC is broken down into three categories: Technical, Cost, and Schedule with a rating of high, moderate, or low for each category.

3.2.1.1. The SCC ratings shall be used in the planning process to determine the basis for DCMA surveillance levels, whether to issue LOD for subcontract/inter-divisional work, and to determine if an LOD should have been received for subcontract/inter-divisional work.

3.2.1.2. The sub-process flowchart for “Software Contract Criticality (SCC)” can be found at Appendix B.

3.2.2. Determine SCC for Cost. Contracts, subcontracts, POs, DOs, or other forms of agreement shall be reviewed by the SP to determine the SCC rating for cost using the following criteria:

3.2.2.1. If the contract is firm fixed price (FFP), the cost risk is low to the government. Therefore, for all FFP contracts (regardless of the dollar value) the SCC for cost shall be rated low.

3.2.2.2. If the contract is not FFP, and the contract cost is less than \$250,000, the SCC for cost shall be rated low.

3.2.2.3. If the contract is not FFP, and the contract cost is equal to or more than \$250,000, but less than \$20 million there is an increased risk to the government; therefore, the SCC for cost shall be rated moderate.

3.2.2.4. If the contract is not FFP, and the contract cost is greater than \$20 million, there is significant risk to the government; therefore, the SCC for cost shall be rated high.

3.2.3. Determine SCC for Schedule. Criteria for determining the SCC for schedule is derived from part 700 of title 15, Code of Federal Regulations, “Defense Priorities and Allocations System (DPAS)” (Reference (i)), a regulation that assures timely availability of industrial resources to meet current national defense and emergency preparedness program requirements, and to provide an operating system to support rapid industrial response in a national emergency. DoD 4400.1-M, “Department of Defense Priorities and Allocation Manual” (Reference (j)), provides the guidance for DoD activities for implementation of DPAS. All contracts, subcontracts, POs, DOs, or other forms of agreement in support of an authorized program are given a DPAS rating of either DX, DO, or not rated. Contracts, subcontracts, POs, DOs, or other forms of agreement shall be reviewed by the SP to determine the SCC rating for schedule using the following criteria:

3.2.3.1. A DX rating is assigned to those programs of the highest national priority. If the DPAS rating is DX, the SCC for schedule shall be rated high.

3.2.3.2. A DO rating is assigned to those programs that are vital to national defense. If the DPAS rating is DO, the SCC for schedule shall be rated moderate.

3.2.3.3. An unrated order is normally a commercial order, or a DoD order that is not ratable. If there is no DPAS rating, the SCC for schedule shall be rated low.

3.2.4. Determine SCC for Technical. The appropriate contractual documents must be reviewed to determine the SCC for technical performance based on the intended use of the software. Usually the statement of work (SOW) will describe the intended use of the software, and sometimes will also identify some type of technical risk. Contracts, subcontracts, POs, DOs, or other forms of agreement shall be reviewed by the SP to determine the SCC rating for technical using the following criteria:

3.2.4.1. If a failure of the software could result in loss of human life, the SCC for technical shall be rated high. Examples of this would be software for aircraft flight controls, life support systems, and nuclear weapons systems.

3.2.4.2. If a failure of the software could result in an environmental hazard, the SCC for technical shall be rated high. An example of this software would be the controlling and transferring of hazardous materials such as petroleum products, and nuclear waste.

3.2.4.3. If a failure of the software could result in a critical security breach, the SCC for technical shall be rated high. An example of this type of software would be the handling and clearing of classified communications codes.

3.2.4.4. If a failure of the software could result in the loss of a combat/rescue mission, or the loss of equipment, the SCC for technical criticality shall be rated moderate. A loss of combat mission example would be a failure of a weapons system that results in a mission abort. A loss of equipment failure example would be software that allowed an over speed condition of an aircraft engine where the engine suffered damage but not total failure.

3.2.4.5. If the software failure would not result in loss of human life, loss of mission, or loss of equipment, the SCC for technical shall be rated low.

3.2.5. Document Results. The SCC ratings for the technical, cost, and schedule categories shall be documented in the “Basic Prime Contract Summary Information” and/or the “Basic Subcontract Summary Information” section(s) within the Software Requirements Report (SRR) tab of the implemented SSP template.

### **3.3. LETTER OF DELEGATION (LOD) NOT RECEIVED.**

3.3.1. Sub-process Description. This paragraph describes what to do when a contractor the SP is cognizant of has received a contract, subcontract, PO, DO, or other form of agreement from a higher level supplier, and the SP cognizant of the higher level supplier has **not** requested supporting contract administrative services by issuing an LOD to them. This paragraph also describes how it is determined by the SP at the higher level supplier if an LOD should be issued.

3.3.1.1. LODs for DoD related work are issued and received via the DCMA Delegation eTOOL (Reference (k)).

3.3.1.2. LODs for non-DoD related work are issued and received via the DCMA Electronic Contract Administration Request System (ECARS) (Reference (l)). Non-DoD related work is received from Federal agencies, foreign governments, and international organizations.

3.3.1.2. The sub-process flowchart for “Letter of Delegation (LOD) Not Received” can be found at Appendix B.

3.3.2. Request LOD from Higher Level SP. When the SP becomes aware that a supplier in their cognizance has received a contract, subcontract, PO, DO, or other form of agreement from a higher level supplier and an LOD has not been received from the SP cognizant of the higher level supplier, the SP shall make contact with the higher level SP and request that an LOD be issued, and adhere to the following:

3.3.2.1. If the higher level SP decides to issue an LOD, continue to paragraph 3.4.

3.3.2.2. If the higher level SP decides not to issue an LOD, the SP must review the contract, subcontract, PO, DO, or other form of agreement to determine the SCC ratings for technical, cost, and schedule (see paragraph 3.2.).

3.3.3. Surveillance Not Required. If the technical, cost, and schedule SCC ratings are all low, then surveillance and/or an LOD is not required. These facts shall be documented by the SP, and thus ends the requirement for them to perform surveillance on that contract, subcontract, PO, DO, or other form of agreement.

3.3.4. Contact the SEAM Center for Assistance. If any of the SCC ratings are not low, and the higher level SP still decides not to issue an LOD, the SEAM Center shall be contacted for further assistance.

3.3.4.1. If SEAM Center assistance results in the higher level SP issuing an LOD, continue to paragraph 3.4.

3.3.4.2. If SEAM Center assistance does **not** result in the higher level SP issuing an LOD then surveillance is not required. The SPs effort shall end on that contract, subcontract, PO, DO, or other form of agreement.

3.3.5. Document Results. The SP shall document the surveillance decision and any correspondence with the higher level SP and/or the SEAM Center.

### **3.4. CONTRACT/LOD REVIEW.**

3.4.1. Sub-process Description. This paragraph provides instruction for the SP to follow when performing contract, subcontract, PO, DO, or other form of agreement/LOD review. DCMA SPs need to become knowledgeable of the technical requirements within the contract, subcontract, PO, DO, or other form of agreement, and/or the LOD (to include any applicable Quality Assurance Letters of Instruction (QALIs), and/or MOA/MOU) to gain a clear understanding of work to be performed by the supplier/subcontractor, and the work the customer is asking them to do to support their acquisition process. This allows the SP to efficiently plan their surveillance activities.

3.4.1.1. A detailed technical review of the documents described above provides the foundation for acquiring this knowledge. In the contract, subcontract, PO, DO, or other form of agreement, items to review include the SOW, the Contract Data Requirements List (CDRL), technical item description(s)/data package(s), system requirements, delivery schedule, cost controls, task orders, contract exhibits, and attachments. The review is primarily a matter of fact gathering.

3.4.1.2. The sub-process flowchart for “Contract/LOD Review” can be found at Appendix B.

3.4.2. LOD Review. When applicable, the SP shall review the LOD and document the “Acquisition Customer’s Instructions” and/or the “Delegating CMO’s Instructions” sections within the SRR tab of the implemented SSP template. The purpose of this review is to ascertain:

3.4.2.1. If any software surveillance related Federal Acquisition Regulation (FAR) 42.302(a), “Contract Administrative Functions” (Reference (m)), are withheld by the customer.

3.4.2.2. If any unique software surveillance related tasks/activities for the SP to perform are required by the customer.

3.4.2.3. For a major system acquisition, if FAR 42.202(f), “Special Surveillance,” (Reference (n)) has been designated by the customer for high risk or critical subsystems or components.

3.4.2.4. Reporting requirements (e.g., Special topics, reporting frequency, and report distribution).

3.4.3. Contract/Subcontract Review. Prime contracts for DoD related work are received via the Electronic Data Workflow (EDW) Contract Data Workflow (CDW) system (Reference (o)), and subcontracts are typically received with an LOD via the Delegation eTOOL, (Reference (k)). For non-DoD related work, contracts, subcontracts, POs, DOs, or other forms of agreements are typically received with an LOD via ECARS (Reference (l)). When a contract is not in EDW

CDW, or a contract/subcontract/PO/DO/other form of agreement is not received with the LOD, they may be obtained directly from the supplier or the subcontractor as applicable.

3.4.3.1. Determine Contract Type. The SP needs to be aware of the type of contract they are performing surveillance on as it has impact on certain clauses required to be in the contract. Contract types include, but are not limited to: FFP, Cost Plus Fixed Fee, Cost Plus Award Fee, Cost Plus Incentive Fee, and Basic Order Agreement. DCMA-INST 118, “Contracts – Initial Receipt and Review” (Reference (p)), has an overview of the various types of contracts.

3.4.3.1.1. FFP contracts are considered low cost risk to the government as the supplier has agreed to provide the product(s) or service(s) in question for the amount specified in the contract.

3.4.3.1.2. Cost Plus contracts contain a higher cost risk to the Government.

3.4.3.1.3. Note that DCMA SPs may be requested to provide input to the award committee regarding supplier performance on incentive type contracts.

3.4.3.2. The SP shall document the following information in the Basic Prime Contract Summary Information, and/or in the Basic Subcontract Summary Information section(s) within the SRR tab of the implemented SSP template:

- Acquisition customer organization name, code, and address
- Acquisition customer point of contact (POC) and phone
- Contract number, contract type (FFP, Cost Plus, etc.)
- Program/project name and acronym
- Date contract/subcontract/PO/DO/other form of agreement received by CMO
- Date contract/subcontract/PO/DO/other form of agreement received by SP
- Total contract dollar value
- Total software dollar value (If known)
- Contract period of performance (start and end dates)
- Software development period of performance (start and end dates)
- If the software period of performance is less than or equal to 6 months; and if so, number of months
- Technical risk if stated in the contract (the rating and reference)
- Acquisition category for contract (e.g., ACAT I, II, III, Other)
- Current acquisition phase of the contract (e.g., Material Solution Analysis (MSA), Technology Development (TD), Engineering and Manufacturing Development (E&MD), Production and Deployment (P&D), Operations and Support (O&S))
- Supplier name, address, cage code
- CMO organization name, organization code, and address
- Software POC, phone, and email
- If applicable, the DCMA CAR POC, phone, and email
- Brief overview of the software development work to be performed by the contractor/subcontractor

3.4.3.3. The SP shall document the software Inspection and Acceptance (I&A) points in the “Inspection/Acceptance Points” section of the SRR tab within the implemented SSP template; and, shall document all software deliverables (as found in the CDRLs, contract line item numbers (CLIN), the SOW, contract attachments, contract enclosures, etc.), to include their respective I&A points in the “Software Deliverables/Non-Deliverables” section of the SRR tab within the implemented SSP template.

3.4.3.3.1. All property/products delivered to the Government must be identified in a CLIN. During contract review, the SP shall determine whether the software being acquired is a stand-alone contract CLIN, or if it will be delivered embedded in the system, end item component, or as firmware. This may require a technical dialog with the customer or supplier to better understand the configuration of the product and its work breakdown structure (as applicable).

3.4.3.3.2. The CDRLs will contain the details of all data/documents to be delivered by the supplier to include: place of delivery, how it is to be delivered, authority (aka: data item description (DID)), and time and place of I&A. In some cases, the supplier may be required to develop a CDRL data/document but not physically deliver it. Data/documents identified in the CDRLs should also be linked directly to requirements in the SOW, or to other parts of the contract. The SP shall identify, review, and document all CDRLs associated with software, including any CDRLS needed for surveillance planning purposes. **NOTE:** When DCMA is not listed as a recipient of the CDRL data/document requirement, the SP will need to gain access to the data/document via the supplier’s databank/media control system.

3.4.4. Review Statement of Work (SOW). From the SOW the SP will gain a complete understanding of the contractual requirements, the work to be performed, products to be developed, the schedule (or where the schedule is located), and required meetings and reviews. The information listed below is typically found in the SOW but may also be found in other parts of the contract. The SP shall document the following in the appropriate sections within the SRR tab of the implemented SSP template:

- Software related SOW paragraphs or sub-paragraphs
- Government access rights clauses (e.g., clauses required by FAR 46.3, “Contract Clauses” (Reference (q))). (See paragraphs 3.4.4.1. and 3.4.4.2.)
- Technical data rights clauses (e.g., clauses required by Defense Federal Acquisition Regulation Supplement (DFARS) 227.71, “Rights in Technical Data” (Reference (r)); DFARS 227.72, “Rights in Computer Software and Computer Software Documentation” (Reference (s)); FAR 24.1, “Protection of Privacy and Freedom of Information,” (Reference (t)); and DFARS 239.71, “Security and Privacy for Computer Systems” (Reference (u))). (See paragraphs 3.4.4.1. and 3.4.4.2.)
- Key milestones/events (including formal reviews and audits such as but not limited to: Preliminary/Critical Design Review (PDR/CDR), Test Readiness Review (TRR), Functional/Physical Configuration Audits (FCA/PCA))
- Applicable software development specifications, standards, and development methods or models to be implemented

- Contractually imposed measures (such as but not limited to: software size, defects, technical performance measures (TPM), and earned value (EV))
- Special areas of interest (such as but not limited to: critical software items, security, safety, open systems, and software reuse)
- Software related non-developmental items (NDI) (such as but not limited to: commercial off-the-shelf (COTS), and Government off-the-shelf (GOTS))
- Government-furnished material (GFM) (such as but not limited to: Government-furnished equipment (GFE), and Government-furnished information)
- Software specific risks
- Work breakdown structure (WBS) (when available/required)
- Computer software configuration items (CSCI) or software items (SI)

3.4.4.1. The SP shall assure that the proper provisions for “Government Access Rights” and “Technical Data Rights” are included in the contract, subcontract, PO, DO, or other form of agreement.

3.4.4.2. If the SP determines that any required software related FAR/DFARS clause(s) is/are missing, or is/are incorrectly included, or any of the contractual specifications are deficient, the SP shall take action to resolve them as described in paragraph 3.4.5.

3.4.5. Handling Discrepancies/Deficiencies. The SP shall annotate any discrepancies/deficiencies found in the contract and follow up with the area contract officer for resolution. Per DCMA-INST 118, “Contracts – Initial Receipt and Review” (Reference (p)), contract deficiencies discovered by DCMA after contract award should be discussed with the Supplier when appropriate, and the SP shall create a Contract Deficiency Report (CDR) by logging into the Electronic Document Access (EDA) System (Reference (v)), and using the CDR tool (aka: EDA-CDR tool). Additionally, the SP shall document this within the “Contract Discrepancies/Deficiencies” section of the SRR tab of the implemented SSP template.

3.4.6. Post Award Recommendation. As required by DCMA-INST 118 (Reference (p)), based on the results of the SPs detailed technical review, the SP shall determine if a Post Award Orientation (PAO) should be conducted. If so, the SP shall make the recommendation within the Contracts Receipt and Review (CRR) eTOOL (Reference (w)). Additionally, the SP shall document this within the “Post Award Recommendation” section of the SRR tab of the implemented SSP template. The SP should refer to FAR 42.502, “Selecting Contracts for Postaward Orientation” (Reference (x)), for guidance on how to determine if a PAO should be conducted.

3.4.7. Document Results. As the SP conducts their detailed technical review of the contract, subcontract, PO, DO, other form of agreement, and/or LOD, the SP shall document their findings in the appropriate sections of the SRR tab within the implemented SSP template.

**3.5. REVIEW DCMA/SUPPLIERS’ HISTORICAL DATA.** When DCMA has administered contracts, subcontracts, POs, DOs, or other forms of agreement and has knowledge and/or records regarding how the supplier has performed in the past, the SP must consider this history as input for software risk assessment when developing their SSP. Additionally, the SP shall

document this information in the “Supplier Historical Performance” section of the SRR tab within the implemented SSP template.

**3.6. REVIEW AVAILABLE PLANNING PRODUCTS.** The SP must review supplier and Acquisition Customer planning documents as they become available to gain insight into the supplier’s approach for developing the software, and the acquisition customer’s approach for managing the acquisition.

3.6.1. Planning Products. Supplier/Acquisition Customer planning products may be available in hard copy/electronic format, and supplier specific products may or may not be deliverable. Examples of these documents include:

- Preliminary Software Development Plan (SDP)
- Preliminary Software Quality Assurance Plan (SQAP)
- Program schedules (such as but not limited to Integrated Master Plan (IMP) and Integrated Master Schedule (IMS))
- Work Breakdown Structure (WBS)
- Test and Evaluation Master Plan (TEMP)

3.6.2. Documenting Supplier Planning Products. Information gleaned from supplier planning products that are germane to the SPs surveillance planning shall be documented in the “Available Supplier Planning Documents” section of the SRR tab within the implemented SSP template.

3.6.3. Documenting Acquisition Customer Planning Products. Information gleaned from Acquisition Customer planning products that are germane to the SPs surveillance planning shall be documented in the “Available Customer Planning Documents” section of the SRR tab within the implemented SSP template.

**3.7. IDENTIFY DCMA CONCERNS REGARDING SUPPLIER CAPABILITY/ PERFORMANCE.** Based on the results of performing a detailed contract, subcontract, PO, DO, or other form of agreement review, the SP should identify any concerns indicating potential risk relative to the supplier’s capability or performance in developing the software as part of their surveillance planning activities.

3.7.1. Performance Areas. Example capability or performance areas to be considered by the SP include but are not limited to:

- Potential staffing turnovers
- Lack of experience in the specific domain technology being acquired
- Compressed development schedule

3.7.2. Risk Assessment. The SP must consider this capability or performance factor as input for software risk assessment when developing their SSP.

3.7.3. Document Results. DCMA concerns regarding the suppliers' capability or performance shall be documented by the SP in the "Supplier Capability" section of the SRR tab within the implemented SSP template.

### 3.8. IDENTIFY AND PLAN.

3.8.1. Sub-process Description. This step in the surveillance planning process is focused on identifying the surveillance activities that must be performed by the SP in order to provide effective support to the customer. It should be noted that the tasks/activities performed by the SP are influenced by the contractual requirements imposed on the supplier/subcontractor, and also by DCMA internal business practices. This sub-process describes how to determine and document:

- The mandatory level of core technical, cost, and schedule tasks/activities to engage in for software surveillance
- Any CMO unique tasks/activities that need to be performed
- The "Surveillance Frequency Needed" in which the tasks/activities will be engaged

3.8.1.1. This sub-process also prepares the SP for performing the "Identify Customer Unique Elements" sub-process as described in paragraph 3.10.

3.8.1.2. The sub-process flowchart for "Identify and Plan" can be found at Appendix B.

3.8.2. Identify Core Technical, Cost, and Schedule Tasks/Activities. The mandatory core technical, cost, and schedule tasks/activities that the SP is required to engage in are pre-determined and can be found within the "SSP Worksheet" tab within the implemented SSP template.

3.8.2.1. For DoD related work, the core technical, cost, or schedule tasks/activities that the SP is **not** required engage in based on the SCC rating are automatically grayed out within the "SSP Worksheet" and include the words "NOT REQUIRED." Additionally, the instruction found at paragraph 3.1.2.3. relative to DoD Work is applicable.

3.8.2.2. For non-DoD related work, the core technical, cost, or schedule tasks/activities the SP is **not** required to engage in are **not** based on the SCC ratings. They are, however, based on the instruction found at paragraph 3.1.2.3. relative to non-DoD work. That is for non-DoD related work, the SP performs only those tasks/activities required by the Acquisition Customer.

3.8.2.2.1. None of the core technical, cost, and schedule pre-defined tasks/activities will be automatically grayed out and marked "NOT REQUIRED."

3.8.2.2.2. The SP will need to determine which tasks/activities are required based on the LOD, MOA/MOU, or other form of agreement with the Acquisition Customer.

3.8.2.3. Perform Software Risk Assessment. The SP shall perform a software risk assessment to determine and document the Likelihood level, Consequence level, and their

Rationale for each applicable core technical, cost, and schedule element within the “SSP Worksheet” tab in the implemented SSP template. **NOTE:** Once the SP has entered their “Likelihood” and “Consequence,” the worksheet will automatically calculate a weighted risk rating (WRR). While performing the software risk assessment, the SP must at minimum consider as input any germane information they recorded within the SRR tab in the implemented SSP template to include (but not limited to):

- Any software risks identified in the contract/WBS
- Special areas of interest
- NDI and GFM
- Supplier capability
- Customer specified risks or issues

3.8.2.4. Document Engagement. The SP shall enter the required information in the “Optional Surveillance Notes” (if desired), “Task/Activity Surveillance Status,” and “Surveillance Frequency Needed” fields for each applicable core technical, cost, and schedule task/activity.

3.8.2.5. Determining the “Surveillance Frequency Needed” for Core Technical, Cost, and Schedule Tasks/Activities. The SP must as objectively as possible determine the “Surveillance Frequency Needed” for each task/activity based on the WRR; therefore the following guidance shall be applicable:

3.8.2.5.1. Tasks/activities associated with core technical, cost, and schedule elements determined to be in the high risk range (WRR is between 20 and 25) should be engaged in to the maximum extent reasonable.

3.8.2.5.2. Tasks/activities associated with core technical, cost, and schedule elements determined to be in the moderate risk range (WRR is between 12 and 19) should be engaged in at a reasonable level less than that if it were high risk, and greater than that if it were low risk.

3.8.2.5.3. Tasks/activities associated with core technical, cost, and schedule elements determined to be in the low risk range (WRR is between 1 and 11) should be engaged in as minimally as reasonable.

3.8.2.6. The SP shall refer to “Step #2: Complete the SSP Worksheet Tab” found within the “Helper Guide” worksheet tab in the implemented SSP template, and the scenario at Appendix C, Software Risk Assessment, as guides when executing paragraphs 3.8.2.3. through 3.8.2.5.

3.8.3. Identify CMO Unique Tasks/Activities. The CMO unique tasks/activities that the SP may potentially engage in are pre-determined and can be found in the SSP Worksheet tab within the implemented SSP template. Additionally, the SP may add more tasks/activities to this section by selecting an appropriate task/activity code from the “Element Category” pick-list, and entering a description for the task/activity.

3.8.3.1. Document Engagement. For each applicable pre-defined and SP added task/activity, the SP shall document the task/activity “Surveillance Status, Surveillance Frequency Needed, Surveillance Frequency Allocated;” and if applicable, the “CMO Estimated Hours Per Task/Activity” fields.

3.8.3.2. Determining the “Surveillance Frequency Needed” for CMO Unique Tasks/Activities. The SP shall as objectively as possible determine the “Surveillance Frequency Needed” for each CMO unique task/activity based on schedule, requirement, or best judgment.

3.8.2.3. The SP shall refer to “Step #2: Complete the SSP Worksheet” tab found within the “Helper Guide” tab in the implemented SSP template as a guide when executing paragraphs 3.8.3.1. and 3.8.3.2.

3.8.4. Document Results. The core technical, cost, schedule, and CMO unique tasks/activities shall be documented by the SP within the “SSP Worksheet” tab in their appropriate sections of the implemented SSP template.

### **3.9. PROGRAM MEASURES.**

3.9.1. Sub-process Description. This paragraph describes how the SP identifies and documents data/measures to be collected, analyzed, and reported. To successfully support the customer, maintain insight of program status, determine health of software related development processes for technical, cost, and schedule, the SP needs to identify data/measures that will be collected and analyzed during the course of software surveillance.

3.9.1.1. The SP shall document the “Measure Category, Contract Reference (if any), Task/Activity Surveillance Status, Surveillance Frequency Needed;” and if applicable, the “CMO Estimated Hours Per Task/Activity” within the “Program Measures” section of the “SSP Worksheet” tab in the implemented SSP template, which is divided into the following subsections:

3.8.1.1.1. SW14.1 – Core Measures. Based on the SCC rating, the minimum set of pre-defined measures that are to be collected and analyzed by the SP.

3.8.1.1.2. SW14.2 – Standalone Measures. Any software related measure identified in the contract that is not already identified as a core measure.

3.8.1.1.3. SW14.3 – Technical Performance Measures (TPMs). Any software related TPM identified in the contract.

3.8.1.1.4. SW14.4 - CMO Unique Measures. Any measure defined by the SP that can be self-generated, or that is readily available from the contractor. CMO unique measures are **not** required, but may be collected and analyzed at the discretion of the SP.

3.8.1.1.5. SW14.5 – Customer Unique Measures. Any measure the customer requests the SP to collect and analyze that has not already been defined as a “Core Measure, Contractually Imposed - Standalone Measure,” or “Contractually Imposed - TPM.”

3.9.1.2. Required Template. For each data/measure documented in the “Program Measures” section of the “SSP Worksheet” in the implemented SSP template, the SP shall select an appropriate “Data/Measure Analysis Specification - Data/Measure Analysis Results (DMAS/DMAR)” template to implement, and IAW guidance within its “Helper Guide” tab, document the details within the “DMAS Worksheet” tab of how the data/measure will be collected, analyzed, and reported. The SP may combine multiple data/measures into a single DMAS/DMAR when it is efficient.

3.9.1.3. The identified data/measures should cover and support all phases of the software development life-cycle. Multiple measures within a given phase could provide visibility and insight into potential problems. A matrix showing the life-cycle for typical data/measures can be found in Appendix D.

3.9.1.4. The DMAS/DMAR templates are located under “Data/Measure” in the Policy Templates section on the Policy Resource Page.

3.9.1.5. The sub-process flowchart for “Program Measures” can be found at Appendix B.

3.9.2. No Measures Required. When the contractual period of performance is 6 months or less, the SP is **not** required to plan for or engage in surveillance activities for program measures. The period of performance is too short for measures to be a useful tool for the purposes of the SAM mission. However, if there are measures contractually imposed on the supplier, the SP shall verify the supplier is collecting and analyzing the required measures.

3.9.3. Identify Contractually Imposed Measures. Contractually imposed measures include but are not limited to Standalone Measures, TPMs, and Earned Value Measures. When contractually imposed measures were identified during the detailed contract review (see paragraph 3.4.4.), the SP documented them within the “Contractually Imposed Measures” section of the SRR tab in the implemented SSP template. Concurrent with this, the template built pick-lists for those measures that the SP can now select as appropriate to document them in the “Standalone Measures” and “TPM” subsections of the “Program Measures” section of the “SSP Worksheet” of the implemented SSP template. **NOTE:** Some contractually imposed measures may also map directly to the “Core Measure;” if they do, the SP does not need to duplicate them.

3.9.3.1. SCC Low. When the technical, cost, and schedule SCC ratings are all low, the SP shall use whatever supplier software measures are available to attain insight into the health of the program. If there are no supplier measures available then the SP is **not** required to collect, analyze, and report on the “Program Measures.” When a measure is not available, the “Task/Activity Surveillance Status” field shall be marked “N/A for this Program/Contract.”

3.9.3.2. SCC High or Moderate. When any technical, cost, or schedule SCC rating is high or moderate, the SP shall collect, analyze, and report on all of the core “Program Measures.”

3.9.4. Document Core Measures. The pre-identified “Core Measures” are generic, but key for providing insight into technical, cost, and schedule performance. For example, “Software Size” is typically measured in source lines of code or function points. The SP will need to determine how the supplier is collecting software size and other software measures that are typically identified in the suppliers SDP, measurement plan, or equivalent. This is further explained in the process for “Data Collection and Analysis” as found in paragraph 4.5.

3.9.5. Identify CMO Unique Measures. While not required, the SP may determine if additional software measures should be self-generated (or obtained, collected, and analyzed) based the supplier’s historical performance, capability, and/or the SPs software risk assessments. The additional software measures identified by the SP are those that are **not** already identified as a “Core Measure,” contractually imposed “Standalone Measure/TPM,” or a “Customer Unique Measure.” The SP should consider the following when identifying additional measures (this is not a comprehensive list):

- Project specific concerns (constraints)
- Project related key issues/concerns
- Software development issues/concerns
- Issues that represent levels of risk that threaten the Supplier’s ability to meet goals, responsibilities, or commitments
- Planned-decision points (milestones)
- External requirements/Product acceptance criteria
- Information needs

3.9.6. Document CMO Unique Measures. Any unique measure(s) identified by the SP shall be documented within the “SW14.4 - CMO Unique Measures” subsection of the “Program Measures” section in the “SSP Worksheet” tab of the implemented SSP template.

3.9.7. Identify Customer Unique Measures. When the Customer has requested the SP to collect and analyze any additional measure(s) not already defined as a “Core Measure,” contractually imposed “Standalone Measure/TPM,” or a “CMO Unique Measure.”

3.9.8. Document Customer Unique Measures. The SP shall document the measure(s) within the “Customer Unique Measure” subsection of the “Program Measures” section in the “SSP Worksheet” tab of the implemented SSP template.

3.9.9. Document Program Measures Engagement. IAW the “Helper Guide” tab found within the implemented SSP template, the SP shall document the “Task/Activity Surveillance Status, Surveillance Frequency Needed;” and if applicable, the “CMO Estimated Hours Per Task/Activity,” for the “Program Measures” section of the “SSP Worksheet” tab of the implemented SSP template.

3.9.10. Determining “Surveillance Frequency Needed” for Program Measures. The SP shall determine the “Surveillance Frequency Needed” for each task/activity based on contractual reporting requirements, and/or best judgment, and/or customer schedule or specification (as directed).

3.9.11. Document Data/Measure Specification. The details for how each data/measure will be collected, analyzed, and reported, (all measures documented within the “Program Measures” section of the “SSP Worksheet” tab of the implemented SSP template) shall be documented by the SP within the “DMAS” worksheet tab of the implemented DMAS/DMAR template(s).

### **3.10. IDENTIFY CUSTOMER UNIQUE ELEMENTS.**

3.10.1. Sub-process Description. This paragraph describes how the SP identifies and documents tasks/activities the customer has required/requested the SP to perform. To successfully support the customer, the SP needs to be able to articulate the surveillance tasks/activities planned to be performed, fully identify and understand the customers’ needs, and maintain two-way communications. The primary purpose of sub-process is to continue the fact gathering effort for planning and finalizing the SSP.

3.10.1.1. Having completed the initial steps of the surveillance planning process, the SP is now ready to:

- Present the draft SSP (and Facility SSP if applicable) to the customer
- Identify any unforeseen customer concerns that need to be addressed in the SSP
- Determine if the customer requires any unique tasks/activities to be performed by the SP

3.10.1.2. If a Program Support Team (PST) has been established by the CMO, the process described herein may be conducted jointly with other PST members or independently by the SP.

3.10.1.3. The sub-process flowchart for “Identify Customer Unique Elements” can be found at Appendix B.

3.10.2. Initiate Communications and Exchange Planning Information. An initial DCMA and customer planning meeting shall be requested by the SP. If the meeting does take place, it may be conducted by the most convenient method such as: video teleconference (VTC), telephone, or combination of telephone and email, etc.

3.10.2.1. Customer Unfamiliar With DCMA Services. Since internal DCMA customers are operating under the same policy as the supporting CMO, they are familiar with DCMA policy and mission. However, program management office (PMO) personnel may be unfamiliar with DCMA policy and mission. When this is the case, it is highly recommended that a high level overview of DCMA policy and mission be provided to the PMO personnel. This should include how surveillance tasks/activities (e.g., core technical, cost, schedule, and customer

unique tasks/activities) are identified by the SP, and how the tasks/activities provided benefit the customer.

3.10.2.2. Discuss Contract/Program Perspective. Regardless of who the customer is, the SP shall:

3.10.2.2.1. Discuss with intent to resolve, any software related concerns that may impact software surveillance planning (e.g., contractual, historical supplier performance, WBS elements).

3.10.2.2.2. Determine if the customer has any real or perceived software development risk concerns (e.g., program risk relative to technical, cost, or schedule performance; supplier or subcontractor risk).

3.10.2.2.3. Identify any requested customer unique tasks/activities (see paragraphs 3.10.5.2. or 3.10.6.2.) .

3.10.2.2.4. Identify any requested customer unique measures (see paragraphs 3.10.5.2. or 3.10.6.3.).

3.10.2.2.5. Identify customer reporting requirements (see paragraph 3.10.7.).

3.10.2.3. Provide DCMA Points of Contact (POC) to the Customer. The SP shall ensure the customer is provided all CMO software POC information, including: title, function, email address, and phone number.

3.10.3. Identify Customer POCs. The SP shall obtain a customer POC listing that includes pertinent software technical resources supporting the contract, subcontract, PO, DO, or other form of agreement, including but not limited to: title, function, email address, and phone number.

3.10.3.1. DCMA and Customer POC Matrix. The SP shall add DCMA and customer software POCs to the “Key Software Points of Contact (POC)” table found in the “SSP Document” tab of the implemented SSP template. A primary reason for establishing the POC listing at this level is to ensure that functional elements within DCMA and the customer organization have access to their respective counterparts; and to communicate with and promulgate technical issues. This POC listing shall be kept current.

3.10.4. Present the Tasks/Activities Documented in the SSP. The SP shall provide to the customer an overview of the following to determine if the customer has any additional needs or recommendations for software surveillance:

- The SCC ratings including rationale for the ratings
- The planned software surveillance tasks/activities for the core technical, cost, schedule, and CMO Unique
- The results of their software risk assessments for the core technical, cost, and schedule elements including rationale for the assessments

- The planned Core Measures, contractually imposed Standalone Measures/TPMs, and CMO Unique Measures, as/if applicable
- The general reporting method(s) used for keeping the customer informed

3.10.5. Prime Contract Communications. When the SSP is for a prime contract, the following is performed:

3.10.5.1. The SP shall request the appropriate acquisition planning documents from the Acquisition Customer (e.g., Systems Engineering Plan (SEP), PMO Risk Management Plan (RMP), and TEMP).

3.10.5.2. Guiding the Acquisition Customer to ensure the need is above and beyond the documented core technical, cost, schedule and/or CMO unique tasks/activities, the SP shall determine if the Acquisition Customer has any unique tasks/activities to be performed by the SP (such as: customer requires 100 percent software test witnessing).

3.10.5.3. Guiding the Acquisition Customer to ensure the need is above and beyond any Core Measure, contractually imposed Standalone Measure/TPM, or CMO Unique Measures, the SP shall determine if the Acquisition Customer has any unique measures to be collected, analyzed, and reported. This information will be used as latent input for paragraph 3.10.

3.10.6. Subcontract Communications. When a subcontract has been received, the following is performed:

3.10.6.1. For all subcontracts, POs, DOs, or other forms of agreement, if it is determined to be necessary for surveillance planning, the SP shall request appropriate acquisition planning documents through the delegating DCMA SP (e.g., SEP, PMO RMP, and TEMP).

3.10.6.2. If any customer unique tasks/activities are identified in the LOD and they were not required by the Acquisition Customer, the SP shall discuss with the delegating DCMA SP the rationale and need for them, and determine if the work could be verified by the delegating DCMA SP at their level instead of the subcontract level. **NOTE:** When a customer unique task/activity is required by the Acquisition Customer at the subcontract level as opposed to it being a customer unique task/activity required by the DCMA delegating SP, it shall be performed by the supporting SP as required.

3.10.6.3. If any customer unique measures are identified in the LOD and they were not required to be flowed-down to the subcontract level by the Acquisition Customer, the SP shall discuss with the delegating DCMA SP the rationale and need for them, and determine if the work could be verified by the delegating DCMA SP at their level instead of the subcontract level. **NOTE:** When a customer unique measure is required by the Acquisition Customer at the subcontract level as opposed to it being a customer unique measure required by the DCMA delegating SP, it shall be performed by the supporting SP as required.

3.10.6.4. Note that in some cases, an LOD for a subcontract may be received directly from the Acquisition Customer instead of from a delegating DCMA SP.

3.10.7. Identify Customer Reporting Requirements. The SP shall identify what the customers' reporting requirements are, and add the information to the "Acquisition Customer's Instruction" and/or the "Delegating CMO's Instruction" section(s) within the implemented SSP template.

3.10.8. Follow-up on Issues/Concerns. During initial communications with the customer/delegating DCMA SP, issues or concerns may come up that could not be immediately addressed by the parties involved. When this situation occurs, the SP shall track and follow-up with the customer/delegating DCMA SP until resolution is obtained.

3.10.9. Review Acquisition Documents. When made available, the SP should review Acquisition Customer planning documents to gain further insight to the PMOs contract/program concept and their perception of risks. This review will aid in determining if all customer identified program/contract risks/concerns have been considered when planning core technical, cost, schedule, CMO unique, and customer unique tasks/activities. Documents to consider for review may include (but are not limited to) the TEMP, SEP, IMP, IMS, Computer Resources Life Cycle Management Plan (CRCLMP), Program Management Plan (PMP), and PMO RMP.

3.10.10. Assess Customer Unique Tasks/Activities. Each customer unique requested task/activity (to include any customer unique measure) that has been identified shall be assessed to determine the following:

- Is the task/activity within scope of the DCMA SAM mission?
- Is the task/activity within the CMOs competency?
- Is the task/activity appropriate based on the SCC ratings?

3.10.11. Engage/Raise Issues. If the answer to all of the questions in paragraph 3.10.10. is "yes", continue to paragraph 3.10.13. If the answer to any of the questions in paragraph 3.10.10. is "no", the SP shall continue to paragraph 3.10.12., and proceed as directed by management.

3.10.12. Raise Customer Unique Issues to Management. The SW POC shall review any issues related to customer unique tasks/activities (to include any customer unique measure(s)) raised to them by the SP, and make every attempt to resolve the issue at the CMO level. In rare cases the resolution may require advice or support from the SEAM Center. Whatever the situation, the SW POC should either instruct the SP to perform the customer unique task/activity or measure, or provide some other suitable resolution.

3.10.13. Document Customer Unique Engagement. Following guidance found in the "Helper Guide" tab within the implemented SSP template, the SP shall document the required "Element Category/MEASURE(S), Description, Task/Activity Surveillance Status, Surveillance Frequency Needed, Surveillance Frequency Allocated;" and if applicable, the "CMO Estimated Hours Per Task/Activity," in the "Customer Unique Elements" and "Customer Unique Measures" sections within the "SSP Worksheet" tab of the implemented SSP template.

3.10.14. Determining “Surveillance Frequency Needed” for Customer Unique Tasks/Activities. The SP shall document the “Surveillance Frequency Needed” for each customer unique task/activity or measure based on the customer/delegating DCMA SPs schedule, specification, or as directed.

3.10.15. Document Results. Customer unique tasks/activities shall be documented by the SP in the “Customer Unique Elements” section within the “SSP Worksheet” tab of the implemented SSP template.

**3.11. DCMA INTERNAL PERFORMANCE MEASURES.** This section is reserved.

### **3.12. SOFTWARE RESOURCE ESTIMATION.**

3.12.1. Sub-process Description. This paragraph describes the method that is used by the SP in coordination with the SW POC to assess and document the “Total Hours – Needed” to perform all of the surveillance tasks/activities documented in the SSP.

3.12.1.1. The implemented SSP template automatically provides an estimate in the “Hours Per Task/Activity” column for each task/activity (except for those that were not pre-defined, or were manually added by the SP), but the estimates can be changed by the SP (see paragraph 3.12.2.1.).

3.12.1.2. The FTE Hours shown at the bottom of each subsection within the “SSP Worksheet” are automatically summed-up in the “SSP Resources” tab of the implemented SSP template, providing the “Total Hours - Needed.” The SP, in coordination with the SW POC, then assesses the “Total Hours – Needed” and determines if there are adequate CMO resources available to execute the work documented in the SSP.

3.12.1.3. The sub-process flowchart for “Software Resource Estimation” can be found at Appendix B.

3.12.2. Estimate Hours Per Task/Activity and Total Hours – Needed. For each task/activity identified in the respective core technical, cost, schedule, CMO unique, customer unique, and program measures element sections within the SSP Worksheet, the SP, in coordination with SW POC, shall estimate as accurately as possible the number of hours it will take to execute each respective task/activity.

3.12.2.1. By default, the implemented SSP template automatically enters an estimate in the “Hours Per Task/Activity” cells for all pre-defined tasks/activities; which can be overridden by the SP or SW POC by entering their own estimate in the “CMO Estimated Hours Per Task/Activity” fields. **NOTE:** For all tasks/activities manually added by the SP, the “SSP Worksheet” will **not** automatically provide any “Hours Per Task/Activity” estimations; therefore, the SP will need to enter an estimate for them in the “CMO Estimated Hours Per Task/Activity” fields. The “Total Hours – Needed” for the tasks/activities will then be automatically calculated, and summed at the bottom of each respective subsection. The sum

from each subsection is automatically carried forward and entered into the appropriate cells within the “SSP Resources” tab of the implemented SSP template.

3.12.2.2. The following formulas are used for calculations in the SSP Worksheet:

- Total Hours Needed = Surveillance Frequency Needed x Hours Per Task/Activity
- CMO Allocated Hours = Surveillance Frequency Allocated x Hours Per Task/Activity
- CMO Unallocated Hours = Total Hours Needed – CMO Allocated Hours

3.12.2.3. Once the “Hours Per Task/Activity” have been determined for all core technical, cost, schedule, CMO unique, customer unique, and program measures elements tasks/activities, the SP, in coordination with the SW POC, shall review the “Total Hours – Needed” and “Total FTE’s Needed” information located at the bottom of the “SSP Resources” tab to ascertain what the total resource requirements are for the SSP. (**NOTE:** For informational purposes, a full-time equivalent (FTE) is considered to be equivalent to 1632 hours/year. This number is the result of 2080 hours/year minus overhead).

3.12.3. Assess Workload Documented in the SSP. The SP, in coordination with the SW POC, shall assess the “Total Hours – Needed” and “Total FTE’s Needed” and determine if CMO software functional resources are available to accomplish the work as documented in the SSP.

3.12.3.1. If the CMO has the available software functional resources to execute the workload documented in the SSP, continue to paragraph 3.12.4.

3.12.3.2. If the CMO does not have the available software functional resources to execute the full workload documented in the SSP, the SP, in coordination with the SW POC, shall perform a more in-depth sanity check for all tasks/activities to ensure the entries for Surveillance Frequency Needed and Hours Per Task/Activity are indeed valid and accurate, and shall **only** make adjustments if not.

3.12.3.2.1. If after performing this in-depth sanity check it results in the CMO having enough software functional resources available to execute the workload documented in the SSP, the SP continues to paragraph 3.12.4.

3.12.3.2.2. If after performing this in-depth sanity check it does **not** result in the CMO having the available software functional resources to execute the workload documented in the SSP, the SP continues to paragraph 3.12.5.

3.12.4. Resources Available. When the SP in coordination with the SW POC have determined the needed software resources available to fully execute the “Total Hours - Needed” and “Total FTE’s Needed,” the entire workload requirements are allocated to the SSP as described below:

3.12.4.1. The SP shall enter the same existing number from the “Surveillance Frequency Needed” cells into the “Surveillance Frequency Allocated” cells for each task/activity.

3.12.4.2. The result will be that each task/activity documented within the “SSP Worksheet” will be fully allocated with 100 percent of its software functional resourcing requirements (the “CMO Allocated Hours” will be equal “Total Hours Needed”).

3.12.4.3. The “CMO Unallocated Hours” for each task/activity documented in the SSP will be equal to zero (“0”).

3.12.4.4. The SP is done with “Software Resource Estimation” and continues to paragraph 3.13.

3.12.5. Resources Not Available. The SP and/or the SW POC shall **not** readjust the numbers in the “Surveillance Frequency Needed” or “Hours Per Task/Activity” cells in the SSP as they represent the required work as driven by risk, contractual requirements and complexity, and were validated in paragraph 3.12.3.2. The SP, in coordination with the SW POC, shall attempt to staff the workload documented in the SSP based on the number of hours that CMO software functional resources are available as described below.

3.12.5.1. Starting with the lowest risk rated (those in the green zone) tasks/activities first, enter a reasonable bare minimum (non-zero) number in the “Surveillance Frequency Allocated” column that is less than the “Surveillance Frequency Needed” column for the low risk tasks/activities. Then re-review the “SSP Resources” tab to determine if the “Total Hours - Needed” and “Total FTE’s Needed” can now be supported with the available CMO software functional resources. If they can, continue to paragraph 3.12.4. If not, then proceed to paragraph 3.12.5.2.

3.12.5.2. Proceeding with the moderate risk rated tasks/activities (those in the yellow zone), enter a reasonable bare minimum (non-zero) number in the “Surveillance Frequency Allocated” column that is less than the “Surveillance Frequency Needed” column for the moderate risk tasks/activities. Then re-review the “SSP Resources” tab to determine if the “Total Hours – Needed” and “Total FTE’s Needed” can now be supported with the available CMO software functional resources. If they can, continue to paragraph 3.12.4. If not, then proceed to paragraph 3.12.5.3.

3.12.5.3. Proceeding with the high risk rated tasks/activities (those in the red zone), enter a reasonable bare minimum (non-zero) number in the “Surveillance Frequency Allocated” column that is less than the “Surveillance Frequency Needed” column for the high risk Tasks/Activities. Then re-review the “SSP Resources” tab to determine if the “Total Hours – Needed” and “Total FTE’s Needed” can now be supported with the available CMO software functional resources. If they can, continue to paragraph 3.12.4. If not, then proceed to paragraph 3.12.6.

3.12.6. Adjust Other SSPs. If after executing the process described in paragraphs 3.12.5.1. through 3.12.5.3. the workload documented in the SSP still cannot be supported by the available CMO software functional resources, other in-house SSPs should be assessed to determine if they can be adjusted to free up software functional resource hours that can be applied to the workload

documented in the subject SSP. If the results of this assessment effort provide the additional hours needed so that the workload documented in the subject SSP can now be supported with the available CMO software functional resources, continue to paragraph 3.12.4. If not, then proceed to paragraph 3.12.7.

3.12.7. Determine Level of Effort (LOE). When the procedures described in paragraphs 3.12.5. and 3.12.6. fail to result in a the CMOs ability to staff the workload documented in the SSP, the SP in coordination with the SW POC shall determine the LOE that can be applied to the subject SSP. Similar to the process performed in paragraphs 3.12.5.1. through 3.12.5.3., begin zeroing out the “Surveillance Frequency Allocated” starting with the lowest risk tasks/activities. The SP shall work upward, through the moderate tasks/activities, and then the high tasks/activities, until a point is reached where the “Total Hours – Needed” and “Total FTE’s Needed” can be supported with the available CMO software functional resources. When the SP has completed this this process, the SP continues to paragraph 3.13.

3.12.8. Document Results. The resourcing allocated to the SSP shall be documented by the SP in the “Surveillance Frequency Allocated” field for each task/activity within the “SSP Worksheet” tab of the implemented SSP template.

### **3.13. COMPLETE THE SOFTWARE SURVEILLANCE PLAN.**

3.13.1. Sub-process Description. This paragraph describes how the SP compiles the SSP template from a draft to a formal document that is ready for local approval. This process includes procedures for ensuring the SSP:

- Transitions from a “draft” document into a completed “formal” plan
- Is submitted submission to the SW POC formal review and approval

3.13.1.1. Supplemental guidance for this process is described in DCMA-PAM 55.1, “Compiling, Approving, Submitting, and Closing Out the Software Surveillance Plan (SSP),” (Reference (y)), which is located under Pamphlets in the Guidance section on the Policy Resource Page.

3.13.1.2. The sub-process flowchart for “Complete the Software Surveillance Plan” can be found at Appendix B.

3.13.2. Complete the Front Matter Section. IAW guidance in the “Helper Guide” tab found within the selected SSP template, the SP shall document the front matter section of the SSP contained in the “SSP Document” tab of the selected SSP template. This worksheet contains the “Signature/Cover Page, Table of Contents (TOC), Revision History, Key Software Points of Contact (POC), SSP Purpose,” and the “Software Development Overview” sections.

3.13.2.1. Obtain Control Number. For SSPs developed by the SP on a new contract, subcontract, PO, DO, or other form of agreement received by the CMO, the SP obtains a control number from the software POC and enters it into the “Control Number” field on the “Signature/Cover Page” within the “SSP Document” tab of the implemented SSP template. For

existing SSPs that are being updated, the SP shall continue to use the original control number that was first issued to it.

3.13.2.2. Update Table of Contents (TOC). The TOC is fixed and cannot be modified except for entering information for any attachments that may be included as part of the final document. The SP shall ensure that whenever there are attachments for the SSP, they are documented in the “Attachments” section of the TOC within the “SSP Document” tab of the implemented SSP template.

3.13.2.3. Update Revision History. For SSPs developed by the SP on a new contract, subcontract, PO, DO, or other form of agreement they are considered to be in draft mode until their initial release. While in draft mode, the version number for the SSP in the “Revision History” table will remain “0.0”, and the “Date” field shall be completed by the SP by entering the date the document was created/last edited. Formal SW POC review and approval of the SSP is **not** required while it is in draft mode.

3.13.2.3.1. Initial Release. For SSPs developed by the SP on a new contract, subcontract, PO, DO, or other form of agreement that is ready to transition from draft mode to formal initial release, the SP enters into the “Date” field for “Initial Release” within the “Revision History” table the date the document is submitted to the SW POC for review and approval.

3.13.2.3.2. Subsequent Releases. Whenever the SP has changed/updated a SW POC reviewed and approved SSP, in the next available row in the “Revision History” table, the SP updates the “Major” or “Minor” “Revision” number field(s), selects from the pick-list in the “Purpose” field a reason for the update/change, enters in the “Description” field a brief explanation for the revision, enters in the “Date” field the date the revision was made, and resubmits the SSP to the SW POC for review and approval.

3.13.2.3.2.1. Major Change/Update: The SP changes the whole number in the “Major” field to the next incremental numerical value, and changes the fraction number in the “Minor” field to zero (“0”). A major change is defined any of the following:

3.13.2.3.2.1.1. Change/update required by the SSP annual review process (see paragraph 3.18.).

3.13.2.3.2.1.2. A change/update that increases or decreases the overall DCMA Software Resource requirements of the previously approved SSP by 20 percent or more from (see paragraph 3.12.).

3.13.2.3.2.1.3. Any change/update made because of significant degradation or improvement in Supplier performance (Risk levels have either increased/decreased).

3.13.2.3.2.4. All other changes/updates are considered to be minor.

3.13.2.3.2.2. Minor Change/Update: The SP does not change the whole number in the “Major” field, but changes the fractional number in the “Minor” field to the next incremental number. However there is an exception: If the current “Minor” fractional number field is nine (“9”), the SP shall instead increment the “Major” number field, and reset the “Minor” number field to zero (“0”).

3.13.2.3.3. Update Points of Contact (POC). During the “Identify Customer Elements” process described in paragraph 3.10., the key DCMA and customer software POCs were added to the “Key Software Points of Contact (POC)” listing matrix found in the “SSP Documents” tab of the selected SSP template. The SP shall now identify and add the key “Supplier” software POCs and ensure this POC listing for DCMA, customer, and supplier is kept current.

3.13.3. Non-editable Purpose. The context of the “Contract/Program - Software Surveillance Plan Purpose” section within the “SSP Document” tab in the selected SSP template shall **not** be edited/modified by the SP/SW POC. It provides a standard description of the SAM surveillance planning process and purpose as defined by DCMA policy.

3.13.4. Complete the Program/Contract Software Development Overview Section. During execution of the process described in paragraph 3.4., the SP added a short “Overview” in the SRR tab of the selected SSP template describing the effort to be performed by the supplier or subcontractor. For the Contract/Lite SSP templates, this short “Overview” is automatically copied from the SRR tab into the “Program/Contract Software Development Overview” section of the “SSP Document” tab. However, in the “Program SSP” template, because there are multiple SRR tabs (therefore, an “Overview” is in each SRR tab), none are automatically copied into the “SSP Document” tab. Therefore, whenever the SP has implemented the “Program SSP” template, the SP shall manually add an appropriate “Overview” to the “Program/Contract Software Development Overview” section of the “SSP Document” tab.

3.13.5. Software Development Risk(s). The SP shall document a minimum of one and maximum of five key risks for the contract/program within the “Key Risks” tab found in the implemented SSP template to include:

3.13.5.1. Part I, Key Software Development Risks:

3.13.5.1.1. Key Risk Element Category. The SP selects from the pick-list a descriptor that associates the identified risk with a process area (such as, SQA for Software Quality Assurance, or SCM for Software Configuration Management).

3.13.5.1.2. Description. The SP enters a description for the risk.

3.13.5.1.3. Likelihood. Referencing the Table A within the “Key Risk” tab, the SP selects from the pick-list a level for the probability the risk will become an issue (realized).

3.13.5.1.4. Consequence. Referencing the Table B within the “Key Risk” tab, the SP selects from the pick-list a level for the severity of the risk if it becomes an issue (realized).

3.13.5.1.5. Rationale. The SP enters a rationale supporting the Likelihood and Consequence level selections.

3.13.5.2. Part II, How the Key Software Development Risks will be Monitored. The SP enters an description of the tasks/activities that will be performed to ensure the identified risks are monitored while executing the tasks/activities identified within the selected SSP template.

3.13.6. Terms and Acronyms. The SP shall enter into the table within the “Terms” tab any terms (and their associated definitions) needed, and/or enter into the table within the “Acronyms” tab any acronyms (and their associated description) needed within the implemented SSP template.

3.13.7. Validate Core Work. The SP shall review and ensure that the core “Technical, Cost,” and “Schedule” sections of the “SSP Worksheet” within the implemented SSP template are complete and accurate.

3.13.8. Validate CMO Unique Work. The SP shall review and ensure that the “CMO Unique Elements” section of the “SSP Worksheet” within the implemented SSP template is complete and accurate.

3.13.9. Validate Customer Unique Work. The SP shall review and ensure that the “Customer Unique Elements” section of the “SSP Worksheet” within the implemented SSP template is complete and accurate.

3.13.10. Validate Program Measures Work. The SP shall review and ensure that the “Program Measures Elements” section of the “SSP Worksheet” within the implemented SSP template is complete and accurate.

3.13.11. Validate Instructions. The SP shall review and ensure that the “Reporting Requirements” fields in the “Acquisition Customer’s Instructions” and/or the “Delegating CMO’s Instruction” sections of the “SRR” tab within the implemented SSP template are complete and accurate.

3.13.12. Complete a Software Surveillance Schedule. The “Surveillance Schedule Q1” through “Surveillance Schedule Q4” tabs in the Contract, Program, Facility SSP templates, and the “Surveillance Schedule Q1” and “Surveillance Schedule Q2” tabs in the Lite SSP template are provided so that the SP can document when they will engage in the tasks/activities documented within the “SSP Worksheet” tab of the implemented SSP template. The SP shall utilize these surveillance scheduling tabs to document on a quarterly basis when each task/activity identified within the “SSP Worksheet” will be engaged in as described below:

3.13.12.1. The “Surveillance Schedule(s)” are dynamic, and shall be kept current.

3.13.12.2. The SP is **not** required to schedule tasks/activities for more than one quarter at a time. Only the active surveillance schedule needs to be included within the formal SW POC approved SSP.

3.13.12.3. If subcontractors are involved and the SP has issued and LODs to supporting CMOs (see paragraph 3.13.13.), in the “CMO Unique Elements” section of “SSP Worksheet” tab within the implemented SSP template, the SP shall manually add a task/activity line item for managing “input” from the supporting CMO for each LOD issued (the line item will be automatically copied to the surveillance schedule(s)).

3.13.13. Document Letter(s) of Delegation (LOD). For any subcontracted software development work identified that the SP has issued (or will issue) an LOD to a supporting CMO, the following is applicable:

3.13.13.1. LODs Planned. LODs that have been, or will be issued by the SP shall be documented in the “LODs Planned/Issued” section within the “SSP Worksheet” of the implemented SSP template, to include the following information:

- Subcontractor name, address, and cage code
- Date the LOD issued
- eTOOL (Delegation/ECARS) # - The Delegation or ECARS system generated reference number
- LOD status: The SP selects from the pick-list either “Accepted,” “Rejected,” “Pending,” or “Other”
- Supporting CMO name, address, and Department of Defense Activity Address Code (DODAAC )
- Supporting software POC name, phone, and email
- A “Brief” summary of the work being performed by the subcontractor
- A “Brief” summary of the tasks/activities delegated to the supporting CMO
- Additional comments (if any)

3.13.13.2. LODs Issued. Whenever the SP issues an LOD to a supporting CMO, the SP shall update the SSP by creating a line item for managing the LOD in the “CMO Unique Elements” section within the “SSP Worksheet” tab in the implemented SSP template.

3.13.14. Prepare the SSP for Formal Approval. Save the implemented SSP template, then execute the process for converting the template into a formal portable document format (PDF) document ready for the SW POCs review and approval as described in DCMA-PAM 55.1, “Compiling, Approving, Submitting, and Closing Out the Software Surveillance Plan (SSP)” (Reference (y)), located under “Pamphlets” in the Guidance section on the Policy Resource Page. Upon completion of the process, the SP shall submit the SSP to the SW POC for formal review and approval.

3.13.15. Engage in Surveillance. Once the SSP is submitted to the SW POC, even though it may be in review cycle and has not yet been formally approved, the SP shall immediately begin executing the tasks/activities identified in the SSP.

### **3.14. SOFTWARE SURVEILLANCE PLAN (SSP) APPROVAL.**

3.14.1. Sub-process Description. This paragraph describes how the PDF version of the SSP is formally reviewed, approved, or rejected within the CMO. The expectation is that:

3.14.1.1. The SSP will be reviewed and approved or rejected by the SW POC as described in paragraph 3.14.2.

3.14.1.2. The SW POC approved SSP will be submitted to the SEAM Center as described in paragraph 3.14.2.3.

3.14.1.3. The sub-process flowchart for “Software Surveillance Plan (SSP) Approval” can be found at Appendix B.

3.14.2. SW POC Review and Approval. Upon receipt of the PDF version of the SSP from the authoring SP, the SW POC shall review the SSP to ensure that it is in compliance with paragraphs 3.1. through 3.13. and shall either reject or approve it as described in paragraphs 3.14.2.1. and 3.14.2.2.

3.14.2.1. Rejected Plans. When the SW POC rejects a Contract, Program, Lite, or Facility SSP, the SP is to resolve the issue that is causing the rejection and shall resubmit the SSP to SW POC for approval.

3.14.2.2. Approved SSP. All approved SSPs shall be digitally signed by the SW POC as described in DCMA-PAM 55.1, “Compiling, Approving, Submitting, and Closing Out the Software Surveillance Plan (SSP)” (Reference (y)), located under “Pamphlets” in the Guidance section on the Policy Resource Page.

3.14.2.3. Submit to SEAM Center. All SSPs approved by the SW POC shall be submitted to the SEAM Center as described in DCMA-PAM 55.1, “Compiling, Approving, Submitting, and Closing Out the Software Surveillance Plan (SSP)” (Reference (y)), located under “Pamphlets” in the Guidance section on the Policy Resource Page.

3.14.3. SEAM Center Feedback. All SSPs submitted to the SEAM Center will be data mined by a staff specialist for workload, risk assessment, other performance related information, and will include verification that the SSP is compliant to paragraphs 3.1. through 3.13. When issues or concerns are found in the SSP by the SEAM Center staff specialist, the process described in paragraphs 3.14.3.1. and 3.14.3.2. will be followed.

3.14.3.1. Minor Issues or Concerns. For minor compliance issues/concerns found in a submitted SSP, the authoring SP and the SW POC will be notified of the issue/concern, and the authoring SP shall resolve the issue/concern whenever the next SSP change/update is executed.

3.14.3.2. Major Issues or Concerns. For major compliance issue/concern found in a submitted SSP, the authoring SP and the SW POC will be notified of the issue/concern. The

authoring SP shall immediately resolve the issue/concern, and resubmit the SSP with the required corrections to SW POC for review and approval or rejection. When the corrected SSP has been approved by the SW POC, it shall be submitted to the SEAM Center as described in paragraph 3.14.2.3. within 20 calendar working days of the notification.

### **3.15. CUSTOMER NOTIFICATION.**

3.15.1. Sub-process Description. This paragraph describes how the SW POC approved SSP will be submitted to the customer.

3.15.1.1. The objective for providing the SSP to the customer is to ensure that the customer and their respective technical staff have full insight into DCMA's plan of action for performing the SAM mission in support of the acquisition effort.

3.15.1.2. The sub-process flowchart for "Customer Notification" can be found at Appendix B.

3.15.2. Submit SSP to the Customer. Once the SSP has been formally approved by the SW POC, it shall be submitted to the customer.

3.15.2.1. Customer Submission Exceptions. In some cases, the customer may not desire to receive a copy of the SSP, or may only desire a "bare bones" version of the SSP depicting only the tasks/activities to be engaged in. When this is the case, the SP shall follow the process described in DCMA-PAM 55.1, "Compiling, Approving, Submitting, and Closing Out the Software Surveillance Plan (SSP)," (Reference (y)), located under "Pamphlets" in the Guidance section on the Policy Resource Page.

3.15.2.2. Customer Feedback Regarding Tasks/Activities. If after receiving a copy of the SSP the customer provides feedback that requests adjustments be made to the SSP that are within scope of the SAM mission, the SP shall change/update the plan accordingly, resubmit the SSP to the SW POC for formal approval, resubmit the adjusted SSP to the customer, and resubmit the adjusted SSP to the SEAM Center as described in paragraph 3.14. Some examples of within scope adjustments are:

- The customer originally wanted software surveillance status reports on a monthly basis, but now wants them on a quarterly basis
- The customer has now identified a specific software safety or security requirement as a key risk, and has requested the SP to monitor it and ensure it is being mitigated by the supplier

3.15.3. Raise to CMO Management to Resolve. When a customer provides feedback on an SSP that requires an adjustment that is not within our mission, competency, or not appropriate based on the SCC rating, the SP shall raise those concerns to the SW POC for resolution.

3.15.3.1. Example: The SCC rating for technical is low, and the SP originally planned to only “monitor” software testing, and the customer is requesting the SP to perform 100 percent software test “witnessing”.

3.15.3.2. Implement Resolution. The SP shall implement the SW POCs resolution(s). If the resolution requires adjustments be made to the SSP, the SP shall update the SSP accordingly, resubmit the SSP to the SW POC for formal approval, resubmit the adjusted SSP to the customer, and resubmit the adjusted SSP to the SEAM Center as described in paragraph 3.14.2.3.

### **3.16. ISSUE LETTER OF DELEGATION (LOD).**

3.16.1. Sub-process Description. This paragraph describes how the SP determines when an LOD needs to be issued.

3.16.1.1. This paragraph also explains which application is used when issuing the LOD to the supporting SP cognizant of the subcontractor based on whether the subcontract is for DoD or non-DoD related work.

3.16.1.2. The sub-process flowchart for “Issue Letter of Delegation (LOD)” can be found at Appendix B.

3.16.2. Determine if an LOD is Required. An LOD shall be issued by the SP when:

3.16.2.1. The DoD Acquisition Customer has specifically directed that LODs are to be issued for subcontracts.

3.16.2.2. For Non-DoD Related Work. There is an existing MOA/MOU or other form of agreement in place that requires LODs to be issued for subcontracts.

3.16.2.3. For DoD Related Work. There are tasks/activities specified by the Acquisition Customer that are required to be flowcharted-down to the subcontract level.

3.16.2.4. For DoD Related Work. There are deliverable products being developed or services being provided by the subcontractor cannot be validated by the SP.

3.16.3. No LOD Required. An LOD is not required to be issued by the SP when:

3.16.3.1. For DoD Related Work. The deliverable products being developed or services being provided by the subcontractor can be fully validated by the SP at their level. An example would be the subcontractor is required to deliver a draft and final software requirements specification (SRS) to the higher level supplier for acceptance. In this case, the SP at the higher level supplier would be able to gain access to the required document from their higher level supplier and validate it.

3.16.3.2. For DoD Related Work. The Acquisition Customer has specifically withheld the SPs authority to issue LODs.

3.16.3.3. For DoD Related Work: The SCC ratings for the subcontract are all low.

3.16.3.4. For Non-DoD Related Work: There is an existing MOA/MOU or other form of agreement in place that does not require LODs to be issued for subcontracts.

3.16.4. Issue LOD for DoD Related Work. All LODs for DoD related work shall be issued by the SP using the Delegation eTOOL (Reference (k)).

3.16.4.1. The request for support will include any customer unique tasks/activities required to be flowcharted-down to the subcontract level, and surveillance for only those core technical, cost, schedule tasks/activities, and “Program Measures” that cannot be verified by the delegating SP at their higher level.

3.16.4.2. The LOD shall include as an attachment, an appropriate SSP template with the following information documented in the applicable worksheet tabs:

3.16.4.2.1. SRR Tab. The “Acquisition Customer’s Instructions” section completed (if applicable), and the “Delegating CMO’s Instruction” section completed.

3.16.4.2.2. SRR Tab. The “Basic Prime Contract Summary Information” section completed representing the delegating SPs higher level contract/subcontract.

3.16.4.2.3. SRR Tab. The delegating SPs estimated SCC ratings for the subcontract documented in the “Basic Subcontract Summary Information” section.

3.16.4.2.4. SSP Worksheet Tab. The “Task/Activity Surveillance Status” field for each core technical, cost, and schedule task/activity being requested marked as: “REQUIRED by Customer/Delegating CMO.”

3.16.4.2.5. SSP Worksheet Tab. When applicable, the “Element Category, and Description” fields for any customer unique tasks/activities required to be flowcharted-down to the subcontract level are to be documented in the “Customer Unique Elements” section, and, the “Task/Activity Surveillance Status” field for each marked as: “Active, being engage.”

3.16.4.2.6. SSP Worksheet Tab. The “Task/Activity Surveillance Status” field for each “Program Measure” task/activity being requested marked as: “REQUIRED by Customer/Delegating CM.”

3.16.5. Issue LOD for Non-DoD Related Work. All LODs for non-DoD related work (such as National Aeronautics and Space Administration (NASA), General Services Administration (GSA), international organizations/foreign governments) shall be issued by the SP using the ECARS, (Reference (l)).

3.16.5.1. The request for support will include any customer unique tasks/activities required to be flowcharted-down to the subcontract level, and surveillance for only those core

technical, cost, schedule customer unique, and “Program Measures” tasks/activities specifically required by the Acquisition Customer that cannot be performed at the delegating SPs higher level (or as otherwise directed or specified in the MOA/MOU, or other form of agreement).

3.16.5.2. The LOD shall include as an attachment, an appropriate SSP template with the following information documented in the applicable worksheet tabs:

3.16.5.2.1. SRR Tab. The “Acquisition Customer’s Instructions” section completed (if applicable), and the “Delegating CMO’s Instruction” section completed.

3.16.6.2.2. SRR Tab. The “Basic Prime Contract Summary Information” section completed representing the delegating SPs higher level contract/subcontract.

3.16.6.2.3. SRR Tab. The delegating SPs estimated SCC ratings for the subcontract documented in the “Basic Subcontract Summary Information” section.

3.16.6.2.4. SSP Worksheet Tab. The “Task/Activity Surveillance Status” field for each core technical, cost, and schedule task/activity being requested marked as: “REQUIRED by Customer/Delegating CMO.”

3.16.6.2.5. SSP Worksheet Tab. When applicable, the “Element Category, and Description” fields for any customer unique tasks/activities required to be flowcharted-down to the subcontract level are to be documented in the “Customer Unique Elements” section, and, the “Task/Activity Surveillance Status” field for each marked as: “Active, being engaged.”

3.16.6.2.6. SSP Worksheet Tab: When applicable, the “Task/Activity Surveillance Status” field for each “Program Measure” task/activity being requested marked as: “REQUIRED by Customer/Delegating CMO.”

3.16.6. Determine if the LOD is Accepted or Rejected. Once the LOD has been issued to the Supporting CMO, the delegating SP shall follow-up to determine if the LOD has been accepted, accepted with limitations, or rejected by the supporting CMO.

3.16.6.1. Accepted/Accepted with Limitations. If the LOD is accepted, or accepted with limitations, the delegating SP shall ensure it is added to their respective higher level SSP as described in paragraph 3.13.13.

3.16.6.2. Rejected. If the LOD is rejected, the delegating SP shall contact the supporting CMO to determine the reason, and resolve the issue if possible. In some cases, the CMO might not have the available resources to perform the LOD. If it is ascertained that the supporting CMO has the available resources to perform the LOD, yet has still rejected it, the delegating SP should:

- Contact the SEAM Center for assistance and take whatever action is advised
- Document and keep records of the final results

### 3.17. CREATING A FACILITY SOFTWARE SURVEILLANCE PLAN (FACILITY SSP).

3.17.1. Overarching Process Description. This paragraph describes how the SP develops and maintains the optional Facility SSP if the CMO elects to implement it. A Facility SSP can cover multiple customers and contracts, and the process for completing the Facility SSP described includes:

- Ensuring the Facility SSP includes only the tasks/activities from each Contract, Program, or Lite SSP that are “common processes” institutionalized by the supplier across multiple programs
- Ensuring each Contract, Program, or Lite SSP is updated to reflect the common institutionalized processes that are moved into the Facility SSP

3.17.1.1. Facility SSP Template Overview. Similar to the Contract, Program, or Lite SSP templates, the Facility SSP template is divided into the following software surveillance planning sections:

- Core technical, cost, schedule, and CMO unique elements
- Surveillance schedules for four quarters of planning (Q1 through Q4 tabs)
- Excludes the “Customer Unique Elements” and “Program Measures Elements” “SSP Worksheet” sections because they contain program/contract specific tasks/activities that must remain within the Contract, Program, or Lite SSPs
- Includes a “Contract List” tab not found in the other SSP templates

3.17.1.2. The Facility SSP template is located under “Templates” in the Policy Templates section on the Policy Resource Page.

3.17.1.3. The process flowchart for “Creating a Facility Software Surveillance Plan (Facility SSP)” can be found at Appendix B.

3.17.2. Identify the Common Institutionalized Processes. A standalone Facility SSP shall not be implemented in lieu of a Contract, Program, or Lite SSP. A Facility SSP is optional, and shall only be implemented at the CMOs discretion when:

- Multiple Contract, Program, or Lite SSPs already exist
- For the programs/contracts the multiple SSPs cover, the supplier/subcontractor executes common institutionalized processes

3.17.2.1. Processes **not** executed by the supplier/subcontractor the same way from one program/contract to another, are **not** common institutionalized process and shall **not** be included in the Facility SSP. Example: For contracts A, B, C, and D, the supplier/subcontractor uses procedure X for executing their SQA function. On contract E, the supplier/subcontractor uses procedure Y for executing the SQA function. Thus, for contract E, the SQA process would not be considered a common institutionalized process as it is unique to contract E and therefore the tasks/activities within the associated SSP for SQA processes cannot be moved into the Facility

SSP (thereby remaining in-tact within contract E's respective Contract, Program, or Lite SSP as stated below).

3.17.2.2. Processes that are **not** common institutionalized process shall remain in their respective Contract, Program, or Lite SSPs, including all contract/program specific:

- Tasks/activities or processes
- CMO unique tasks/activitie
- Customer unique tasks/activities
- Program Measures

3.17.2.3. As is the restriction for the Program SSP, the SP shall not comingle both DoD and Non-DoD related work into a Facility SSP.

3.17.3. Document the Common Institutionalized Processes. Through review of each Contract, Program, or Lite SSP, that may qualify to be added to the Facility SSP, the SP shall:

3.17.3.1. Determine which core technical, cost, and schedule tasks/activities amongst the multiple Contract, Program, or Lite SSPs are common institutionalized processes to be documented in the Facility SSP, and mark the "Task/Activity Surveillance Status" fields for each task/activity: "Covered in the Facility SSP," and delete any data for those tasks/activities from the remaining fields as they are no longer valid within the Contract, Program, or Lite SSPs since technically they have been moved into the Facility SSP.

3.17.3.2. Determine the highest "Software Risk Assessment" amongst the Contract, Program, or Lite SSPs for each technical, cost, and schedule element that was marked "Covered in the Facility SSP," and use those "Software Risk Assessments" within the Facility SSP.

3.17.3.3. Within the Facility SSP template, for each core technical, cost, schedule, and CMO unique task/activity, mark the "Task/Activity Surveillance Status" fields for each task/activity: "Covered in the Contract, Program, or Lite SSP," for any task/activity that is **not** considered part of the Facility SSP (not a common institutionalized process), and delete any data from the remaining fields – as they are not valid within the Facility SSP (since they remain in the respective Contract, Program, or Lite SSPs).

3.17.4. Document Facility SSP Surveillance Schedule(s). The SP shall use the guidelines described in paragraph 3.13.12. to document their engagement in tasks/activities covered by the Facility SSP.

3.17.5. Contracts List Tab. The SP shall ensure that within the "Contract List" tab in the Facility SSP template that the required information for each Contract, Program, or Lite SSP added to the Facility SSP is documented.

3.17.6. Complete the Facility SSP. Utilizing the "Helper Guide" tab found within the Facility SSP template for guidance, and the process described in paragraphs 3.1. 3.15., the SP shall complete all of the worksheet tabs within the Facility SSP.

3.17.7. Update the Revision History for each Contract, Program, or Lite SSP. The SP shall use the process defined in paragraph 3.13.2.3. to update the “Revision History” table for each Contract/Program/Lite SSP that was added to the Facility SSP.

3.17.8. Review All SSPs. Proof the Facility and each of the associated Contract, Program, or Lite SSPs to ensure they are complete and accurate.

3.17.9. Finalize Facility SSP. When the SP has completed the Facility SSP, it shall be transitioned from draft to a formal PDF as generally described in paragraph 3.13., and submitted to the SW POC for formal review and approval as generally described in paragraph 3.14.

3.17.10. Finalize Contract, Program, or Lite SSPs. For each Contract, Program, or Lite SSP that was added to the Facility SSP, when the SP has completed them, they shall be transitioned from draft to formal PDFs as generally described in paragraph 3.13., and presented to the SW POC for formal review and approval as generally described in paragraph 3.14.

### **3.18. REQUIREMENTS FOR REVIEW CYCLE .**

3.18.1. Annual Review Required. At minimum, all Contract, Program, and Facility SSPs shall be reviewed by the SP on an annual basis to determine the need for changes/updates. This review shall be documented in the Contract, Program, or Facility SSP “Revision History” table as a “Major” change/update as described in paragraph 3.13.2.3. **NOTE:** For the SSP Lite, it has a maximum life cycle of 6 months, and would no longer be a valid SSP at the end of the sixth month.

3.18.2. Immediate Review Required. Any significant changes in the suppliers’ performance, and/or the contract requirements shall require an immediate review of the Contract, Program, Lite, or Facility SSP by the SP to determine the need for changes/updates (regardless of how much time has passed). This review shall be documented in the Contract, Program, Lite, or Facility SSP “Revision History” table as a “Major” change/update as described in paragraph 3.13.2.3. Examples of significant changes include (but are not limited to):

3.18.2.1. Major changes to existing supplier processes that could impact performance that have not yet been reviewed or proofed by DCMA.

3.18.2.2. Supplier technical, cost, or schedule performance has denigrated to unacceptable levels.

3.18.2.3. Supplier technical, cost, or schedule performance has significantly improved, and risk has decreased.

3.18.2.4. A contractual modification that has re-baselined the Software Development Schedule, or added more requirements to the development effort.

3.18.3. Contract/Program Complete. When the supplier/subcontractor has completed the program/contract, the SP shall:

3.18.3.1. Archive program/contract related records as detailed in DCMA-INST 809, “Records Management,” (Reference (z)).

3.18.3.2. Support the contract closeout process as requested.

3.18.3.3. Document and maintain “Lessons Learned.” (This information may be kept in any format, and shall be used by the SP when developing SSPs for the subject Supplier for new/follow-on contracts.)

3.18.3.4. Execute the “Software Contract Ends/Cancelled/Stop-Work” process described in DCMA-PAM 55.1, “Compiling, Approving, Submitting, and Closing Out the Software Surveillance Plan (SSP)” (Reference (y)), located under “Pamphlets” in the Guidance section on the Policy Resource Page.

## CHAPTER 4

### EXECUTE THE SOFTWARE SURVEILLANCE PLAN

#### 4.1. EXECUTE THE SOFTWARE SURVEILLANCE PLAN OVERVIEW.

4.1.1. Overarching Process Description. Execution of the tasks/activities documented in the Contract, Program, Lite, or Facility SSP commences once the SP has completed the development of the plan(s) even while they are in the SW POC approval cycle. The processes described in this chapter guide the SP in how to plan, perform, and follow-up on engagement.

4.1.1.1. The tasks/activities are engaged in by the SP using one or more of the following techniques/methods:

- Process Reviews (see paragraph 4.2.)
- Product Examinations (see paragraph 4.3.)
- Formal Reviews/Audits (see paragraph 4.4.)
- Collecting and Analyzing Data (see paragraph 4.5.)
- Accepting Product (see paragraph 4.6.)

4.1.1.2. The SP shall engage in the documented surveillance tasks/activities identified in the Contract, Program, Lite, or Facility SSP(s) IAW their respective Software Surveillance Schedule(s).

4.1.1.4. The overarching process flowchart for “Execute the Software Surveillance Plan” can be found at Appendix E.

4.1.1.5. **NOTE:** While the overarching process flowchart is depicted as being linear, often the implementation of these techniques/methods occur in parallel. For example, the SP may perform a Product Examination (see paragraph 4.3.) as part of a Process Review (see paragraph 4.2.) to determine that the process is being followed and is producing the expected product.

4.1.2. Required Template. The results of each software surveillance task/activity performed shall be documented as described herein. Furthermore, the SP shall record an entry for all software surveillance tasks/activities performed, to include those that were not planned, in the Software Surveillance Record (SSR) Log located under “Other” in the Policy Templates section on the Policy Resource Page.

#### 4.2. PROCESS REVIEW.

4.2.1. Sub-process Description. The SP examines processes to determine their adequacy, ensure they are being followed, determine if they are effective, and determine if they produce the expected results. The technique for conducting process reviews is basically the same for all processes. However, the purpose of the review varies with the process under review (target process). Examples of target processes/products and the associated goals for each are included

in Appendix F. The SP uses the Contract, Program, Lite, or Facility SSP to determine the target process to be assessed and the technique(s)/method(s) to be used.

4.2.1.1. There are two techniques/methods for conducting a process review:

4.2.1.1.1. Proofing. Assesses the adequacy of the process. This technique/method affords the opportunity to examine in detail a process through its various stages to assess how effectively and accurately contract requirements are flowcharted into process inputs and how well the process incorporates requirements into process outcomes.

4.2.1.1.2. Compliance. Assesses the suppliers' adherence to the process. This technique/ method would be executed to obtain confidence that established practices are in place and are being followed.

4.2.1.2. The sub-process flowchart for "Process Review" can be found at Appendix E.

4.2.2. Determine Technique. The SP shall determine if process proofing or process compliance is to be performed. Per the Contract, Program, Lite, or Facility SSP, the SP shall determine the software process to be reviewed. Examples of processes and the associated goals for each process are included in Appendix F.

4.2.2.1. There are times when an in-depth process review needs to be performed that addresses all of the process inputs, outputs and steps to be accomplished to evaluate the process suitability, adequacy and effectiveness. Proofing may be performed at the facility level if the supplier has institutionalized common processes.

4.2.2.2. Indicators that proofing should be performed include:

4.2.2.2.1. Supplier has little or no experience developing software intensive systems for DoD entities.

4.2.2.2.2. Supplier process has not been proofed.

4.2.2.2.3. Adverse trends have been noted (for example, risk has substantially increased).

4.2.2.2.4. Significant changes or modifications to an existing process have occurred (in this case, the SP may elect to only proof those aspects of the process that were changed).

4.2.3. Process Proofing Technique. When the SP has concerns regarding the adequacy of the target process, it shall be proofed. The SP shall obtain and review any process related contractual requirement(s), supplier procedures, and other supporting artifacts, and:

4.2.3.1. Develop a flowchart and/or a sequence of events (list of process operations or steps), or use the supplier's flowchart to identify key process characteristics for evaluation.

4.2.3.2. Evaluate the process flowchart to determine if it follows a logical order and exhibits the expected process attributes.

4.2.3.3. Walk through the process to ensure it reflects the expected flowchart.

4.2.3.4. Review process inputs to ensure they meet contractual/procedural requirements.

4.2.3.5. Examine the process outputs and determine if they result in conforming products.

4.2.3.6. Evaluate the supplier's implementation of the process (to include ensuring the supplier is following the process and that the process is executable).

4.2.3.7. Analyze the supplier's process output data over time to determine if the process is in control, demonstrates repeatability, and produces the expected results.

4.2.4. Process Compliance Technique. When the SP has confidence in the adequacy of the target process (e.g., prior Supplier history has shown the process to be effective; the process has already been proofed; trend data indicates a controlled process that is followed and results in conforming products), the SP shall:

4.2.4.1. Determine the depth and scope of review.

4.2.4.2. Obtain appropriate process documents/artifacts to be reviewed.

4.2.4.3. Determine the key process characteristics to be evaluated (this could include the key characteristics that were identified during process proofing).

4.2.4.4. Evaluate supplier's compliance to those process characteristics to ensure they are being followed.

4.2.5. Take Action as Appropriate. Based on the results of the process review for proofing or compliance, the SP takes one or more of the following actions when applicable:

4.2.5.1. If a contractual non-compliance or failure on the part of the supplier to follow the process is observed while conducting a process review, the SP shall issue a CAR (see paragraph 5.1.).

4.2.5.2. If a process improvement opportunity is observed while conducting a process review, the SP should issue a CIO (see paragraph 5.2.).

4.2.5.3. If a trend is observed while conducting a process review that could affect technical, cost, or schedule performance, the SP shall report the observations to the customer (see paragraph 5.3.).

4.2.6. Document Results. Whenever a task/activity related to a process review is executed, the SP shall enter a line item record for it into the SSR Log, and create a standalone document in user format (e.g., email, formal/informal report, journal record) containing the detailed results of the process review that includes at minimum:

- Supplier name (and link to applicable SSP (e.g., control number, project name))
- Name of task/activity performed
- Date task/activity performed
- SPs assessment of the process reviewed
- Name of the individual who performed the process review
- How long it took to perform the process review (Task/Activity Actual Hours)
- If the task/activity satisfies an applicable audit standard
- Surveillance technique(s)/method(s) performed (e.g., Process Review, Formal Review/Audit, Product Examination, Data Collection and Analysis, Accept Product)
- As applicable: The number of attributes reviewed, number of observations made, number of defects found, type of defects, action taken (CAR, CIO, report to customer, other), control number for CAR/CIO (if applicable)
- Any supporting artifacts/documentation

4.2.7. Determine SSP Impact. The SP shall determine if results of the process review indicate that the Contract, Program, Lite, or Facility SSP should be updated. If so, the SP shall revisit the appropriate section of the SSP to make any needed adjustments (see chapter 3).

### **4.3. SOFTWARE PRODUCT EXAMINATION.**

4.3.1. Sub-process Description. The SP conducts software product examinations to determine if deliverable and non-deliverable products produced by the supplier meet contractual requirements (e.g., specification, format, content, performance requirements). Software products are defined as any tangible output or service that result from a process and/or an output that is delivered to the customer.

4.3.1.1. Example products include: schedules, work packages, code, documents (e.g., SRS, SDP, SQAP), and design artifacts (e.g., data flowchart diagrams, architecture diagrams).

4.3.1.2. Key software related target products and the associated goals for each product are included in Appendix F.

4.3.1.3. The sub-process flowchart for “Software Product Examination” can be found at Appendix E.

4.3.2. Determine Product to Examine. As documented in the Contract, Program, Lite, or Facility SSP, the SP shall determine the software product(s) that are to be examined.

4.3.2.1. Product Examination Criteria. The SP shall determine and document the review criteria for the product being examined, to include:

4.3.2.1.1. Obtaining contractual product requirements and supplier criteria from procedures, plans, drawings, and DIDs for use in identifying the evaluation criteria.

4.3.2.1.2. Determine the key product characteristics to be examined. For example, key product characteristics for an SDP could be conformance of the document to a DID, inclusion of certain product attributes, consistency, and completeness. If the Supplier has a documented product checklist, the SP may elect to use the information provided in the checklist as an input in determining product examination criteria.

4.3.2.2. Product Examination Technique. The SP shall determine and document the appropriate examination technique to be used to examine the product. A thorough product examination may require a combination of several techniques. Examination techniques include:

4.3.2.2.1. Inspection. Examination of items through observation and use of judgment to evaluate conformity to specified requirements. In the software area, this could include inspection of a product to determine conformance to a DID or a physical inspection of media.

4.3.2.2.2. Testing. Conformity evaluation by observation and judgment accompanied as appropriate by measurement or analysis.

4.3.2.2.3. Witnessing: Observation of the Supplier or subcontractor performing an inspection or test. Witness of a testing event to verify that the supplier is checking software, to verify that it satisfies its requirements and to detect errors and evaluating a software item (e.g., system, subsystem, unit) features (e.g., functionality, performance) against the given set of system requirements.

4.3.2.2.4. Verification: Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

4.3.3. Conduct Product Examination. The SP shall obtain the product(s) to be examined (which may be softcopy or hardcopy). **NOTE:** DCMA is not always identified in the contract as a party to receive a deliverable/non-deliverable product (however, the supplier must provide the SP with access to it for examination). Once the product(s) have been obtained, the SP shall:

4.3.3.1. Ensure the product is controlled as appropriate and is uniquely identified.

4.3.3.2. Ensure the product is consistent with applicable requirements.

4.3.3.3. Perform the product examination (determine if product meets requirements within scope of examination) to determine it meets the key characteristics identified (see paragraph 4.3.2.1.).

4.3.4. Take Action as Appropriate. Based on the results of the product examination, the SP takes one or more of the following actions when applicable:

4.3.4.1. If a contractual non-compliance or failure on the part of the supplier to meet the product specifications/requirements is observed while conducting a product examination, the SP shall issue a CAR (see paragraph 5.1.).

4.3.4.2. If a process improvement opportunity is observed while conducting a product examination, the SP should issue a CIO (see paragraph 5.2.).

4.3.4.3. If a trend is observed while conducting a product examination that could affect technical, cost, or schedule performance, the SP shall report the observations to the customer (see paragraph 5.3.).

4.3.5. Document Results. Whenever a task/activity related to a product examination is executed, the SP shall enter a line item record for it into the SSR Log, and create a standalone document in user format (e.g., email, formal/informal report, journal record) containing the detailed results of the product examination that includes at minimum:

- Supplier name (and link to applicable SSP (e.g., control number, project name))
- Name of task/activity performed
- Date task/activity performed
- SPs assessment of the product examined
- Name of the individual who performed the product examination
- How long it took to perform the product examination (task/activity actual hours)
- If the task/activity satisfies an applicable audit standard
- Surveillance technique(s)/method(s) performed (e.g., Process Review, Formal Review/Audit, Product Examination, Data Collection and Analysis, Accept Product)
- As applicable: The number of attributes reviewed, number of observations made, number of defects found, type of defects, action taken (CAR, CIO, report to customer, other), control number for CAR/CIO (if applicable)
- Any supporting artifacts/documentation

4.3.6. Determine SSP Impact. The SP shall determine if results of the product examination indicate that the Contract, Program, Lite, or Facility SSP should be updated. If so, the SP shall revisit the appropriate section of the SSP to make any needed adjustments (see chapter 3).

#### **4.4. FORMAL REVIEWS AND AUDITS.**

4.4.1. Sub-process Description. Throughout the course of performing SAM, the SP will need to participate in various formal reviews and audits. This paragraph describes what the SP will need to do to prepare for, participate in, and follow-up in relation to formal reviews and audits.

4.4.1.1. Example formal reviews and audits include (but are not limited to):

- System/Software Requirements Review (SRR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Test Readiness Review (TRR)

- Physical Configuration Audit (PCA)
- Functional Configuration Audit (FCA)

4.4.1.2. The sub-process flowchart for “Formal Reviews and Audits” can be found at Appendix E.

4.4.2. Obtain Review/Audit Requirements. The SP shall identify applicable requirements related to the target review/audit including entrance and exit criteria, supplier/customer procedures for conducting the review/audit, and related schedules/plans. Requirements may be found in the contract, supplier’s plans and procedures, or communications/letters from the customer. If this information is not available, the SP should contact the customer for direction. If the entrance/exit criteria have not been execute paragraph 4.4.7.

4.4.3. Ensure Supplier is Tracking Entrance Criteria. The SP shall ensure that the supplier is tracking the entrance criteria and that progress is made as scheduled.

4.4.3.1. Example entrance criteria and SP Activities for a TRR:

4.4.3.1.1. Entrance Criteria #1. All priority 1 and 2 Software Problem Reports (SPR) are closed 10 days prior to the TRR.

- SP activities:
  - Review open SPRs to ensure the supplier has enough time to close any open priority 1 and 2 SPRs prior to due date
  - Verify all priority 1 and 2 SPRs were resolved 10 days prior to TRR

4.4.3.1.2. Entrance Criteria #2. Software Test Plan (STP) required to be delivered 90 days prior to TRR.

- SP activities:
  - Monitor STP development progress and determine if the supplier is on schedule. If not, determine potential impact to delivery date
  - Verify the STP was delivered 90 days before TRR

4.4.3.2. Example entrance criteria and SP activities for a CDR:

4.4.3.2.1. Entrance Criteria. At least 80 percent of the software design is completed 14 days prior to CDR.

- SP activities:
  - Monitor development progress of the software design modules and determine if the supplier is on schedule, if not, investigate
  - If at least 80 percent of the design is not completed 14 days before CDR, determine impact to the CDR schedule

4.4.3.3. The SP shall continue to monitor until entrance criteria is met. If activities/products are at risk for not being completed as scheduled, the SP shall determine if the supplier has an effective plan of action to meet the entrance criteria.

4.4.3.3.1. If the Supplier has a “get well” plan, continue tracking progress of the entrance criteria to the new plan of action until complete.

4.4.3.3.2. If the Supplier does not have an effective plan of action, take action as appropriate (see paragraph 4.4.7.).

4.4.3.3.3. Provide the Customer with a “go/no go” recommendation along with supporting information in a time frame reasonable for them to take contractual action.

4.4.4. Participate in the Formal Review/Audit. The SP shall participate in the review or audit as reflected in the Contract, Program, Lite, or Facility SSP. The SP may perform different functions/activities during formal reviews/audits including:

- Performing Process Reviews
- Performing Product Examinations
- Gathering Information
- Reviewing presentation materials for validity and accuracy
- Raising questions and concerns as appropriate
- Verifying action items and minutes are accurately captured

4.4.4.1. If the results of the SPs participation in the formal review/audit warrants the SP to take action as appropriate, then go to paragraph 4.4.7.

4.4.4.2. If the results of the SPs participation in the formal review/audit does not warrant the SP to take action as appropriate, continue with paragraph 4.4.5.

4.4.5. Ensure Supplier is Tracking Exit Criteria and Resolving Action Items (AI). The SP shall ensure that the supplier is tracking the exit criteria, closing out any AIs, resolving any issues or defects noted, and continues to monitor supplier activities until all exit criteria has been met.

4.4.5.1. If the exit criteria is not met by established due dates, take action as appropriate (see paragraph 4.4.7.).

4.4.5.2. When all exit criteria has been met, continue with paragraph 4.4.6.

4.4.6. Report as Appropriate. The SP shall report the results of the formal review/audit closeout and status of exit criteria to the stakeholders as appropriate. Stakeholders may include customers, program integrators, local management, or supporting SPs at subcontractor facilities.

4.4.7. Take Action as Appropriate. Based on the results of the verifying entrance/exit criteria or formal review/audit, the SP takes one or more of the following actions when applicable:

4.4.7.1. If a contractual non-compliance or failure on the part of the supplier to meet the product specifications/requirements is observed while verifying entrance/exit criteria or conducting a formal review/audit, the SP shall issue a CAR (see paragraph 5.1.).

4.4.7.2. If a process improvement opportunity is observed while verifying entrance/exit criteria or conducting a formal review/audit, the SP should issue a CIO (see paragraph 5.2.).

4.4.7.3. If a trend is observed while verifying entrance/exit criteria or conducting a formal review/audit that could affect technical, cost, or schedule performance, the SP shall report the observations to the customer (see paragraph 5.3.).

4.4.8. Document Results. Whenever a task/activity related to a formal review/audit is executed, the SP shall enter a line item record for it into the SSR Log, and create a standalone document in user format (e.g., email, formal/informal report, journal record) containing the detailed results of the formal review/audit that includes at minimum:

- Supplier name (and link to applicable SSP (e.g., control number, project name))
- Name of task/activity performed
- Date task/activity performed
- SPs assessment of the formal review/audit.
- Name of the individual who performed the formal review/audit
- How long it took to perform the formal review/audit (Task/Activity Actual Hours)
- If the task/activity satisfies an applicable audit standard
- Surveillance technique(s)/method(s) performed (e.g., Process Review, Formal Review/Audit, Product Examination, Data Collection and Analysis, Accept Product)
- As applicable: The number of attributes reviewed, number of observations made, number of defects found, type of defects, action taken (CAR, CIO, report to customer, other), control number for CAR/CIO (if applicable)
- Any supporting artifacts/documentation

4.4.9. Determine SSP Impact. The SP shall determine if results of the formal review/audit indicate that the Contract, Program, Lite, or Facility SSP should be updated. If so, the SP shall revisit the appropriate section of the SSP to make any needed adjustments (see chapter 3).

## **4.5. DATA COLLECTION AND ANALYSIS.**

4.5.1. Sub-process Description. During the planning process, for each data/measure identified in the “SSP Worksheet” within the implemented SSP, the SP selected a DMAS/DMAR template and used the “DMAS” tab in the template to describe how an identified data/measure will be collected, analyzed, reported, and what actions would be taken by the SP if the thresholds for the data/measure were breached, or were trending negatively. This paragraph describes how the SP will collect, analyze, and report on those data/measures documented in the “Program Measures” section of the SSP and their respective DMAS/DMAR. Data/measures typically include:

- Data/measures that the supplier may implement regarding program progress (e.g. defect data, resourcing data, EV data)
- Data/measures required by the contract
- Data/measures internally generated by DCMA (e.g., CARs, CIOs, Process Trends)
- Data/measures the customer requests the SP to collect, analyze, and report

4.5.1.1. A matrix showing the life-cycle for typical data/measures can be found in Appendix D.

4.5.1.2. The sub-process flowchart for “Data Collection and Analysis” can be found at Appendix E.

4.5.2. Collect and Analyze Data/Measures. The SP shall collect and analyze the data/measures identified in the “Program Measures” section of the implemented SSP template IAW the specification that was described in its corresponding DMAS tab within the DMAS/DMAR template that was created during the software surveillance planning process (see chapter 3). The SP shall now use the “DMAR” tab within the DMAS/DMAR template to document the results of their data collection and analysis efforts. **NOTE:** The SP may combine multiple Data/Measures into a DMAS/DMAR when it is efficient.

4.5.3. Obtain the Data/Measures. The SP shall obtain the data/measures to be evaluated based on the “Frequency” identified in the Surveillance Schedule (Q1 through Q4) tabs as found in the SW POC approved SSP.

4.5.3.1. Supplier data/measure information may be obtained through the suppliers’ process asset library, program management files, integrated product team (IPT) meetings, formal/informal reviews, available SQA data, EV POCs, control account managers, and software development/management tools.

4.5.3.2. DCMA data/measure information is obtained and maintained by the SP (e.g., SSR Log, self-developed tools, and various DCMA eTOOLS).

4.5.4. Analyze Data/Measures. The SP shall perform analysis on the data/measure as described in the “DMAS” tab as found within its associated DMAS/DMAR template to include:

4.5.4.1. Analyzing the data/measures over time to determine trends (both positive and negative).

4.5.4.2. Identifying and comparing analysis on multiple related data/measures to identify trends for determining program health indicators for cost, schedule and technical performance. For example, looking at data/measures for planned versus actual staffing levels indicates that staffing is below that projected. Looking at other related data/measures, planned versus actual software modules completed indicates that the supplier is not developing software modules at the rate expected. The collective analysis of staffing and software modules completed is an indicator of a potential adverse schedule impact.

4.5.4.3. The SP shall use the “DMAR” tab as found within its associated DMAS/DMAR template to capture their respective analysis activities and results.

4.5.5. Take Action as Appropriate. Based on the results of data collection and analysis, the SP takes one or more of the following actions when applicable:

4.5.5.1. If a contractual non-compliance or failure on the part of the supplier is observed as a result of the data collection and analysis effort, the SP shall issue a CAR (see paragraph 5.1.).

4.5.5.2. If a process improvement opportunity is observed as a result of the data collection and analysis effort, the SP should issue a CIO (see paragraph 5.2.).

4.5.5.3. If a trend is observed as a result of the data collection and analysis effort that could affect technical, cost, or schedule performance, the SP shall report the observations to the customer (see paragraph 5.3.).

4.5.6. Document Results. Whenever a task/activity related to data collection and analysis is executed, the SP shall enter a line item record for it into the SSR Log, and complete the “DMAR” tab for the data/measure in its respective implemented DMAS/DMAR template, to include as applicable:

- Supplier name (and link to applicable SSP (e.g., control number, project name))
- Name of task/activity performed
- Date task/activity performed
- SPs assessment of the formal review/audit
- Name of the individual who performed the formal review/audit
- How long it took to perform the formal review/audit (Task/Activity Actual Hours)
- If the task/activity satisfies an applicable audit standard
- Surveillance technique(s)/method(s) performed (e.g., Process Review, Formal Review/Audit, Product Examination, Data Collection and Analysis, Accept Product)  
As applicable: The number of attributes reviewed, number of observations made, number of defects found, type of defects, action taken (CAR, CIO, report to customer, other), control number for CAR/CIO (if applicable)
- Any supporting artifacts/documentation

4.5.7. Determine SSP Impact. The SP shall determine if results of the data collection and analysis effort indicate that the Contract, Program, Lite, or Facility SSP should be updated. If so, the SP shall revisit the appropriate section of the SSP to make any needed adjustments (see chapter 3).

## **4.6. ACCEPT PRODUCT.**

4.6.1. Sub-process Description. This paragraph describes how the SP accepts software related products. If acceptance of the software product is at destination, then the procedure defined herein is not applicable.

4.6.1.1. Software products may be accepted either as a stand-alone CLIN or embedded in the system, end item component, or as firmware.

4.6.1.2. Software products may include (but is not limited to): source code, data, software documentation (e.g., SRS, SDP, SQAP).

4.6.1.3. The sub-process flowchart for “Accept Product” can be found at Appendix E.

4.6.2. SPDP Certification. The SP accepting the product shall be SPDP certified as described in DCMA Training Guide, “Software Professional Development Program (SPDP),” (Reference (g)), located under “Training” on the Policy Resource Page.

4.6.3. Verify Time, Method, and Place of Acceptance. The SP shall verify the time, method (e.g., DD Form 250, Bill of Lading), and place of acceptance for the software product as specified by the contract CLIN/CDRL.

4.6.4. Determine Acceptance Criteria. The SP shall determine the acceptance criteria that will be used to evaluate the product presented.

4.6.5. Evaluate Product Against Acceptance Criteria. The SP shall evaluate the product against the acceptance criteria, ensure that the product is under configuration management, and determine the acceptability of the product. This includes the verification that the documentation trail and supporting data is complete and indicates readiness for acceptance.

4.6.6. Accept the Product. The SP shall verify that software products whether standalone, embedded the system, end item component, or as firmware have met all criteria for acceptance.

4.6.6.1. If the product meets acceptance criteria, the SP shall accept the product.

4.6.6.2. If the software product whether standalone, embedded the system, end item component, or as firmware is being accepted by someone other than the SP, the SP shall indicate the acceptability of the product to the person accepting it.

4.6.6.3. Products submitted to the SP for acceptance that do not meet the acceptance criteria shall be rejected.

4.6.7. Take Action as Appropriate. Based on the results of accepting product, the SP takes one or more of the following actions when applicable:

4.6.7.1. If a contractual non-compliance or failure on the part of the supplier is observed as a result the accepting product effort, the SP shall issue a CAR (see paragraph 5.1.).

4.6.7.2. If a process improvement opportunity is observed as a result of the accepting product effort, the SP should issue a CIO (see paragraph 5.2.).

4.6.7.3. If a trend is observed as a result of the accepting product effort that could affect technical, cost, or schedule performance, the SP shall report the observations to the customer (see paragraph 5.3.).

4.6.8. Document Results. Whenever a task/activity related to accepting product is executed, the SP shall enter a line item record for it into the SSR Log, and create a standalone document in user format (e.g., email, formal/informal report, journal record) containing the detailed results of the formal review/audit that includes at minimum:

- Supplier name (and link to applicable SSP (e.g., control number, project name))
- Name of task/activity performed
- Date task/activity performed
- SPs assessment of the formal review/audit
- Name of the individual who performed the formal review/audit
- How long it took to perform the formal review/audit (Task/Activity Actual Hours)
- If the task/activity satisfies an applicable audit standard
- Surveillance technique(s)/method(s) performed (e.g., Process Review, Formal Review/Audit, Product Examination, Data Collection and Analysis, Accept Product)
- As applicable: The number of attributes reviewed, number of observations made, number of defects found, type of defects, action taken (CAR, CIO, report to customer, other), control number for CAR/CIO (if applicable)
- Any supporting artifacts/documentation

4.6.9. Determine SSP Impact. The SP shall determine if results of the data collection and analysis effort indicate that the Contract, Program, Lite, or Facility SSP should be updated. If so, the SP shall revisit the appropriate section of the SSP to make any needed adjustments (see chapter 3).

## CHAPTER 5

### TAKE ACTION AS APPROPRIATE

#### 5.1. TAKE ACTION AS APPROPRIATE OVERVIEW.

5.1.1. Overarching Process Description. This chapter describes the basic SAM toolset the SP implements to:

- Remedy a contract noncompliance, nonconformance, or deficiency (herein referred to as noncompliance)
- Make continuous process improvement recommendations to the supplier
- Keep the customer informed of issues/concerns that may impact technical, cost, or schedule performance

5.1.2. Overarching Process Flowchart. The overarching process flowchart for “Take Action as Appropriate” can be found at Appendix G.

#### 5.2. CORRECTIVE ACTION REQUEST (CAR).

5.2.1. Sub-process Description. The purpose of a CAR is to ensure protection of government interests in products/services being acquired by requesting the supplier to address and resolve a contract noncompliance identified by the SP.

5.2.2. Sub-process Flowchart. The sub-process flowchart for “Corrective Action Request (CAR)” can be found in Appendix G.

5.2.3. Contractual Noncompliance Identified. When a contract noncompliance is identified by the SP, a CAR shall be documented, issued, and tracked through closure as described in DCMA-INST 1201, “Corrective Action Process” (Reference (aa)).

5.2.3.1. Electronic copies of Level III and IV CARs issued to the supplier shall be provided to the SEAM Center.

5.2.3.2. Electronic copies of Level III and IV CARs to include the suppliers resolution when closed out, shall be provided to the SEAM Center.

5.2.4. Document Results. Whenever a task/activity is executed by the SP that identifies a contract nonconformance, the SP shall enter a line item record for it into the SSR Log. In this case, the minimum documentation requirements are maintained by the SP within the enterprise CAR eTOOL (Reference (ab)).

5.2.5. Determine SSP Impact. The SP shall determine if issuance of the CAR indicates that the Contract, Program, Lite, or Facility SSP should be updated. If so, the SP shall revisit the appropriate section of the SSP to make any needed adjustments (see chapter 3).

### **5.3. CONTINUOUS IMPROVEMENT OPPORTUNITY (CIO).**

5.3.1. Sub-process Description. Documenting and issuing a CIO is the SAM method for formally notifying a supplier that during the software surveillance the SP has observed that a particular supplier process or product (that was not subject to a contractual noncompliance) can be improved. This paragraph describes how to document and issue the CIO to a supplier.

5.3.2. Sub-process Flowchart. The sub-process flowchart for “Continuous Improvement Opportunity (CIO)” can be found in Appendix G.

5.3.3. Continuous Improvement Opportunity Identified. When engaging in a software surveillance task/activity, the SP may discover that an opportunity exists to improve a supplier product or process. When such an opportunity is identified the SP should bring it to the attention of the supplier by issuing a CIO.

5.3.4. Generate CIO and Document Actions Taken. When generating a CIO, the SP shall ensure the supplier understands that any action on the part of the supplier is voluntary and does not result in a constructive change to the contract.

5.3.4.2. The CIO shall be documented and issued using the CIO feature available in the enterprise CAR eTOOL (Reference (ab)).

5.3.4.1. The CIO shall contain the statement: “This CIO is not a directive from the government and does not authorize any constructive changes to the contract.”

5.3.4.3. If the supplier agrees to act on the CIO recommendation, the SP shall track through closure and verify implementation of the suppliers’ solution within the CIO feature of the enterprise CAR eTOOL (Reference (ab)).

5.3.4.4. If the supplier does **not** agree to act on the CIO recommendation, the SP shall close it out in within the CIO feature of the enterprise CAR eTOOL (Reference (ab)).

5.3.5. Document Results. Whenever a task/activity is executed by the SP that results in the SP issuing a CIO, the SP shall enter a line item record for it into the SSR Log. In this case, the minimum documentation requirements are maintained by the SP within the CIO feature of the enterprise CAR eTOOL (Reference (ab)).

5.3.6. Determine SSP Impact. The SP shall determine if issuance of the CIO indicates that the Contract, Program, Lite, or Facility SSP should be updated. If so, the SP shall revisit the appropriate section of the SSP to make any needed adjustments (see chapter 3).

### **5.4. REPORT TO CUSTOMER.**

5.4.1. Sub-process Description. This paragraph describes the procedure to be followed by the SP to keep the customer informed of issues/concerns. It should be understood by the SP that timeliness is of the essence, holding off until the end of a month report is created to inform the

customer of a concern/issue that may impact technical, cost, or schedule performance regarding a service or product being provided by the supplier to the customer is not considered timely reporting.

5.4.2. Timely Reporting of Actual/Potential Impacts. Unless otherwise instructed by the customer, whenever the SP has identified an issue/concern that represents an actual (or indicates a potential) impact to technical, cost, or schedule performance, the SP shall immediately report it to the customer and provide sufficient details that will allow the customer to take action as necessary.

5.4.3. Routine Reporting to Customer. At minimum on a monthly basis, or as otherwise instructed by the customer, the SP shall report the following (but not limited to):

- Status of known program performance-related issues or concerns
- The SPs independent assessments of any supplier risk mitigation efforts
- Results of the SPs data collection and analysis
- Provide recommendations when appropriate

5.4.3.1. As may be applicable, the SP shall report to the customer via pre-established methods as defined in the MOA/MOU, LOD, or other form of agreement/customer instruction.

5.4.3.2. If CMO management approval is required, the SP shall follow the established local protocol to obtain approval.

5.4.3.3. If the SP is assigned to a contract/program involving a major program acquisition having an assigned Program Integrator/Supporting Program Integrator, the SP shall also adhere to the additional reporting requirements that are described in DCMA-INST 205 (Reference (h)).

5.4.4. Document Results. Whenever a task/activity related to customer reporting is executed, the SP shall enter a line item record for it into the SSR Log, and create a standalone document in user format (e.g., email, formal/informal report, journal record) containing the detailed results of the formal review/audit that includes at minimum:

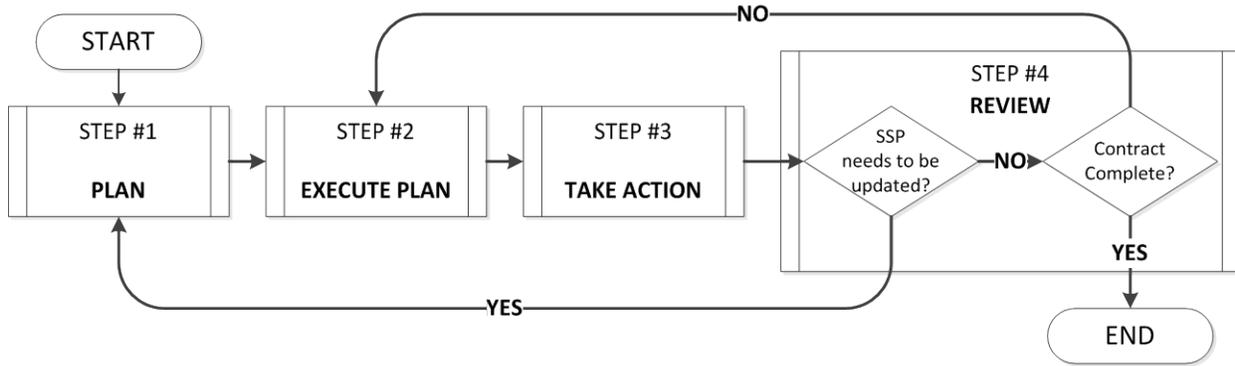
- Supplier name (and link to applicable SSP (e.g., control number, project name))
- Name of task/activity performed
- Date task/activity performed
- SPs assessment of the formal review/audit
- Name of the individual who performed the formal review/audit
- How long it took to perform the formal review/audit (Task/Activity Actual Hours)
- If the task/activity satisfies an applicable audit standard
- Surveillance technique(s)/method(s) performed (e.g., Process Review, Formal Review/Audit, Product Examination, Data Collection and Analysis, Accept Product)
- As applicable: The number of attributes reviewed, number of observations made, number of defects found, type of defects, action taken (CAR, CIO, report to customer, other), control number for CAR/CIO (if applicable)

- Any supporting artifacts/documentation

5.4.5. Determine SSP Impact. The SP shall determine if results of customer reporting indicate that the Contract, Program, Lite, or Facility SSP should be updated. If so, the SP shall revisit the appropriate section of the SSP to make any needed adjustments (see chapter 3).

**APPENDIX A**

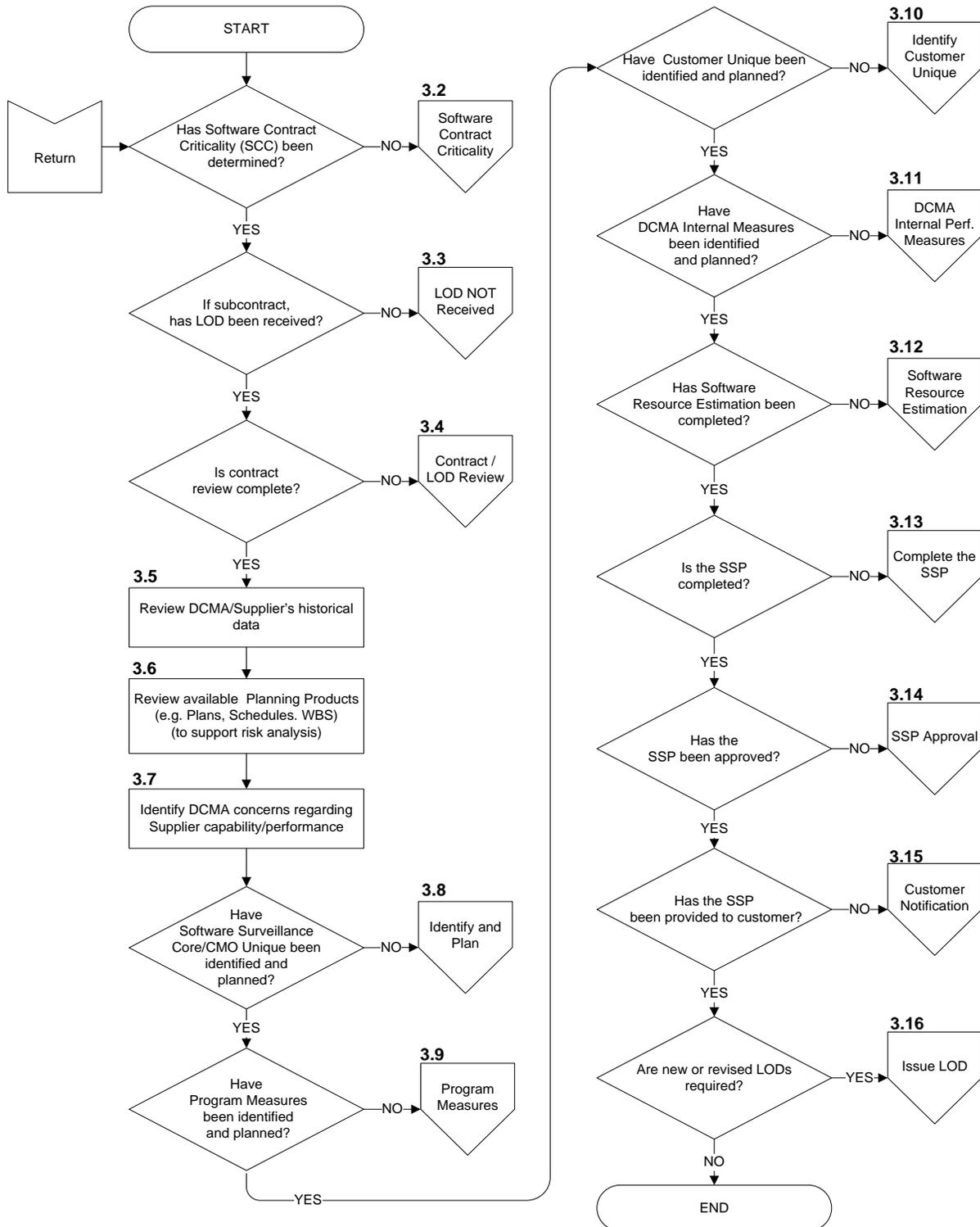
**SOFTWARE ACQUISITION MANAGEMENT (SAM) MISSION  
PROCESS FLOWCHART**



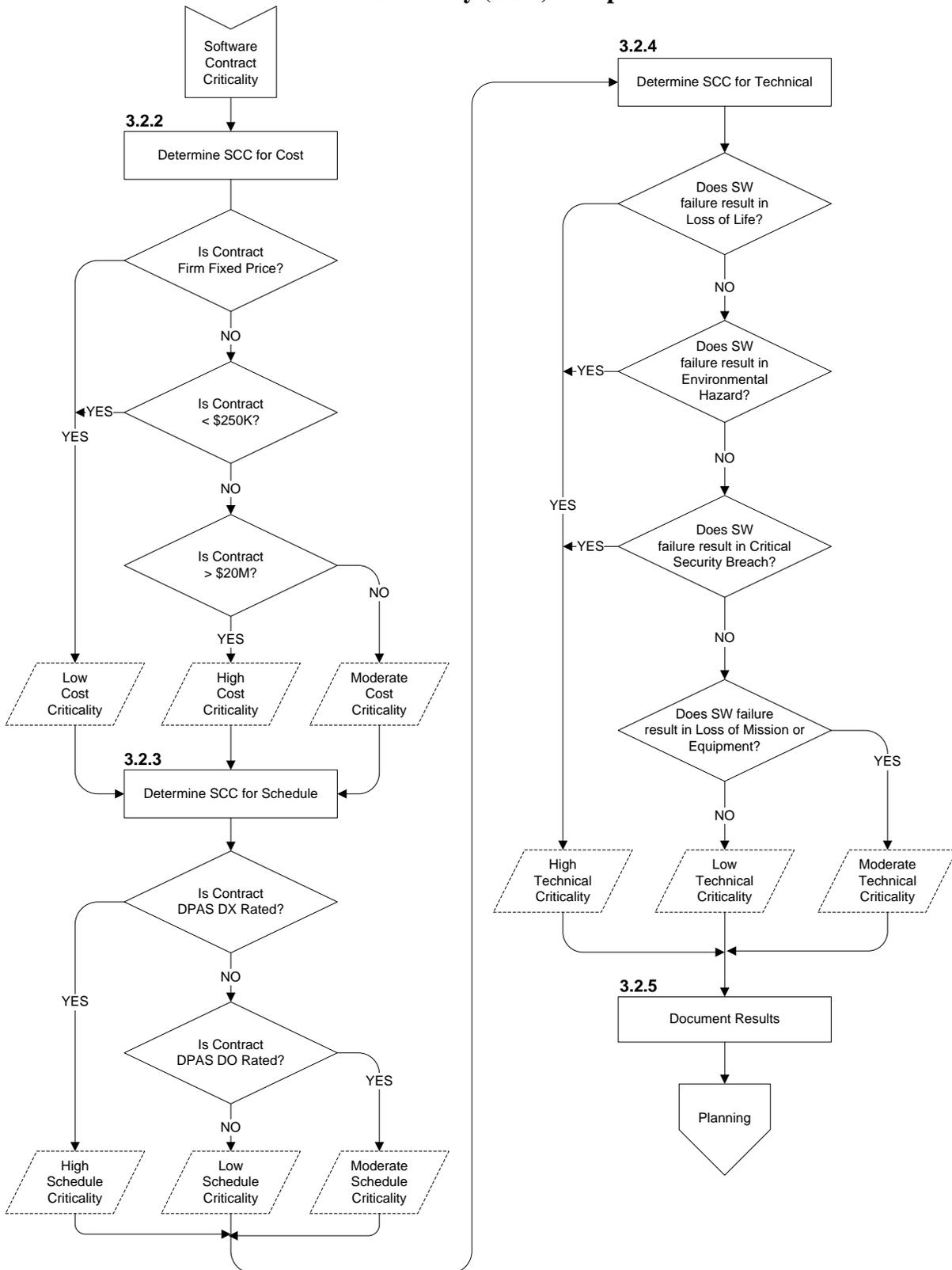
**APPENDIX B**

**SOFTWARE SURVEILLANCE PLANNING PROCESS FLOWCHARTS**

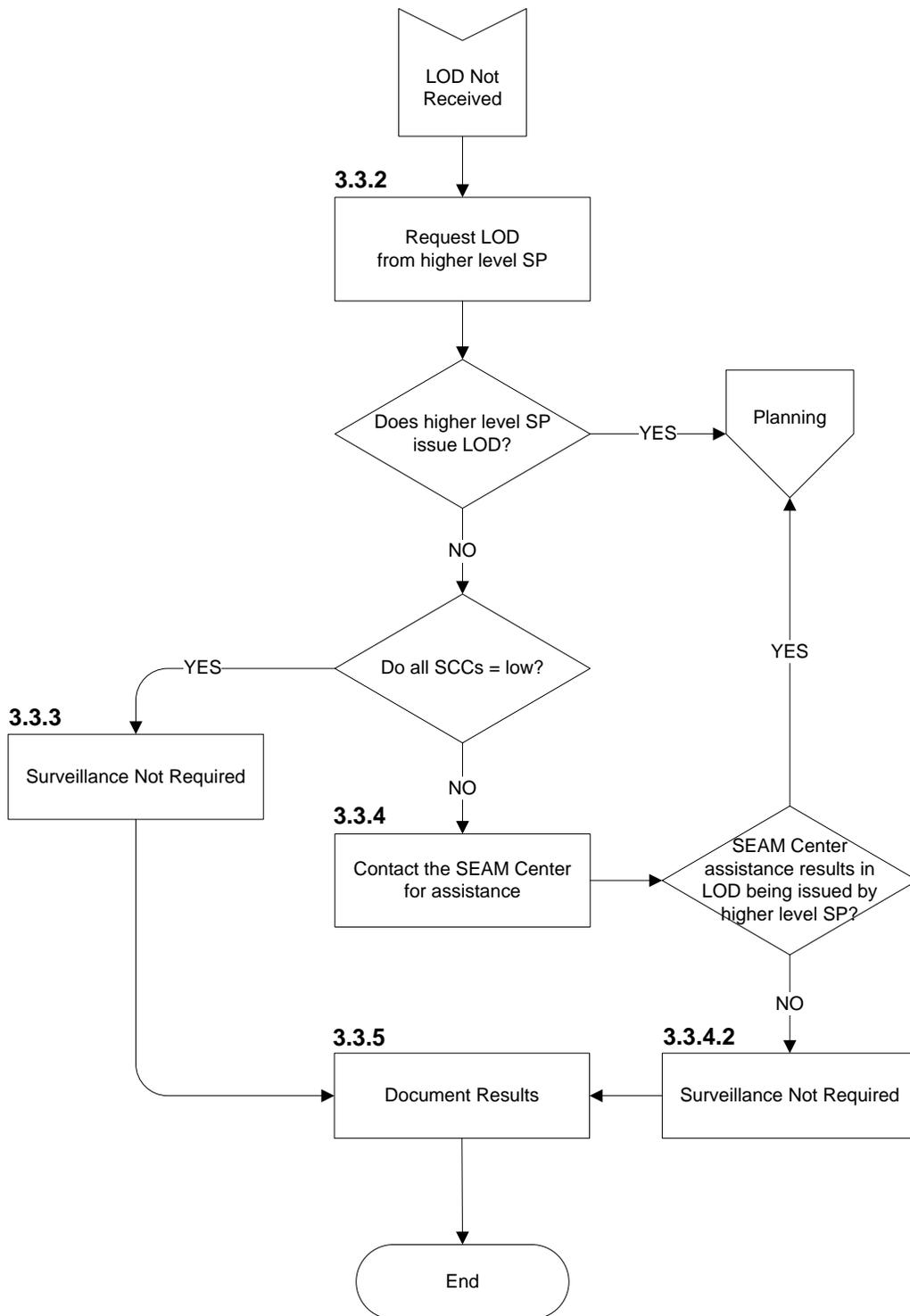
**Overarching Process**



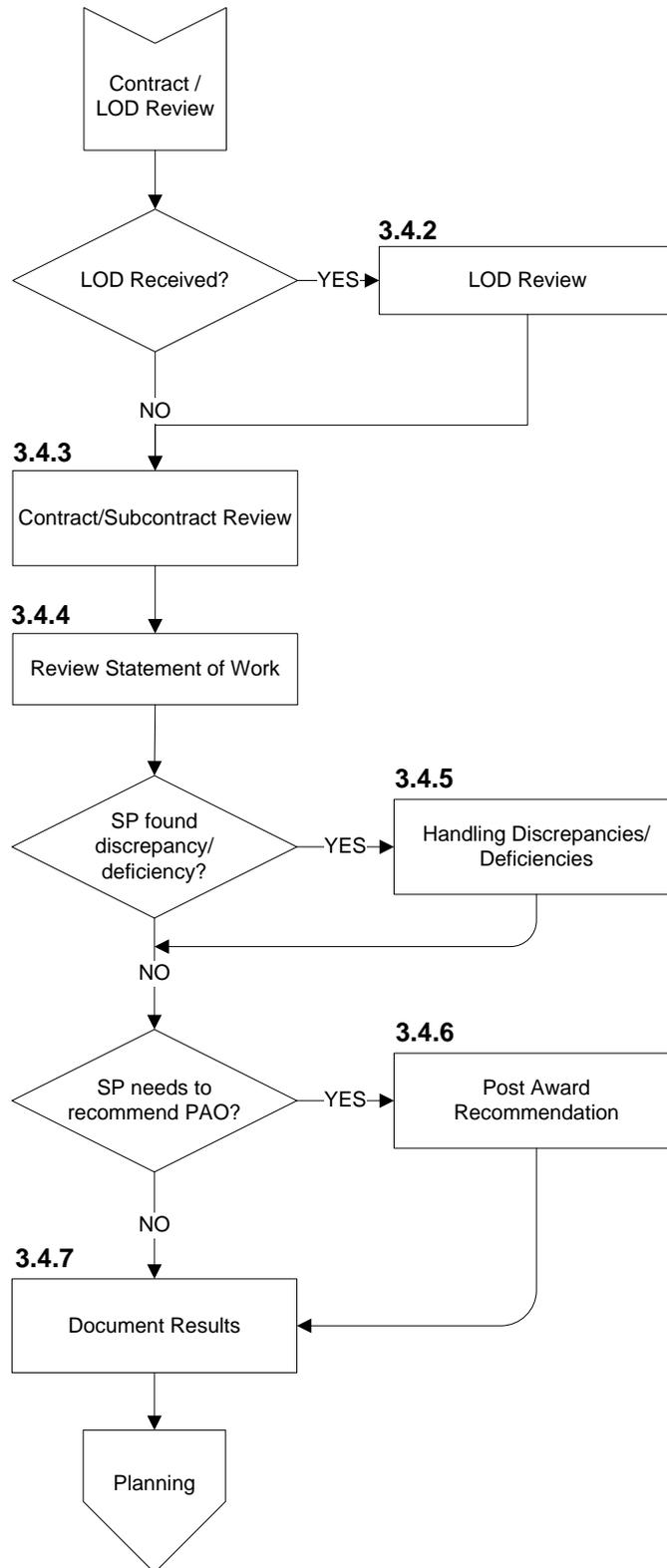
### Software Contract Criticality (SCC) Sub-process Flowchart



### Letter of Delegation (LOD) Not Received Sub-process Flowchart

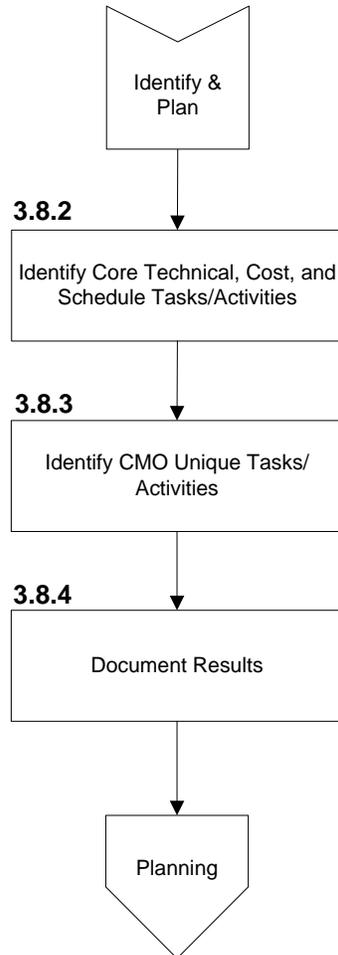


### Contract/LOD Review Sub-process Flowchart

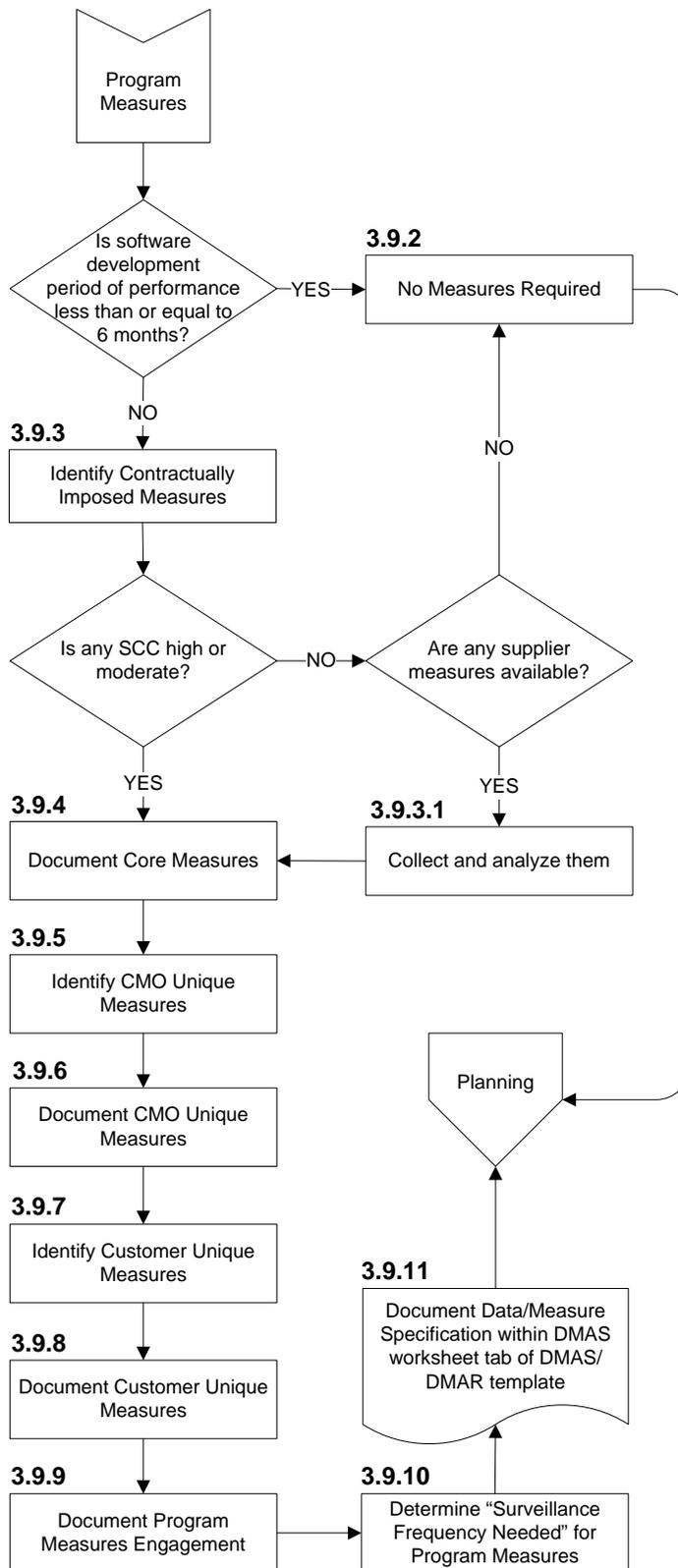




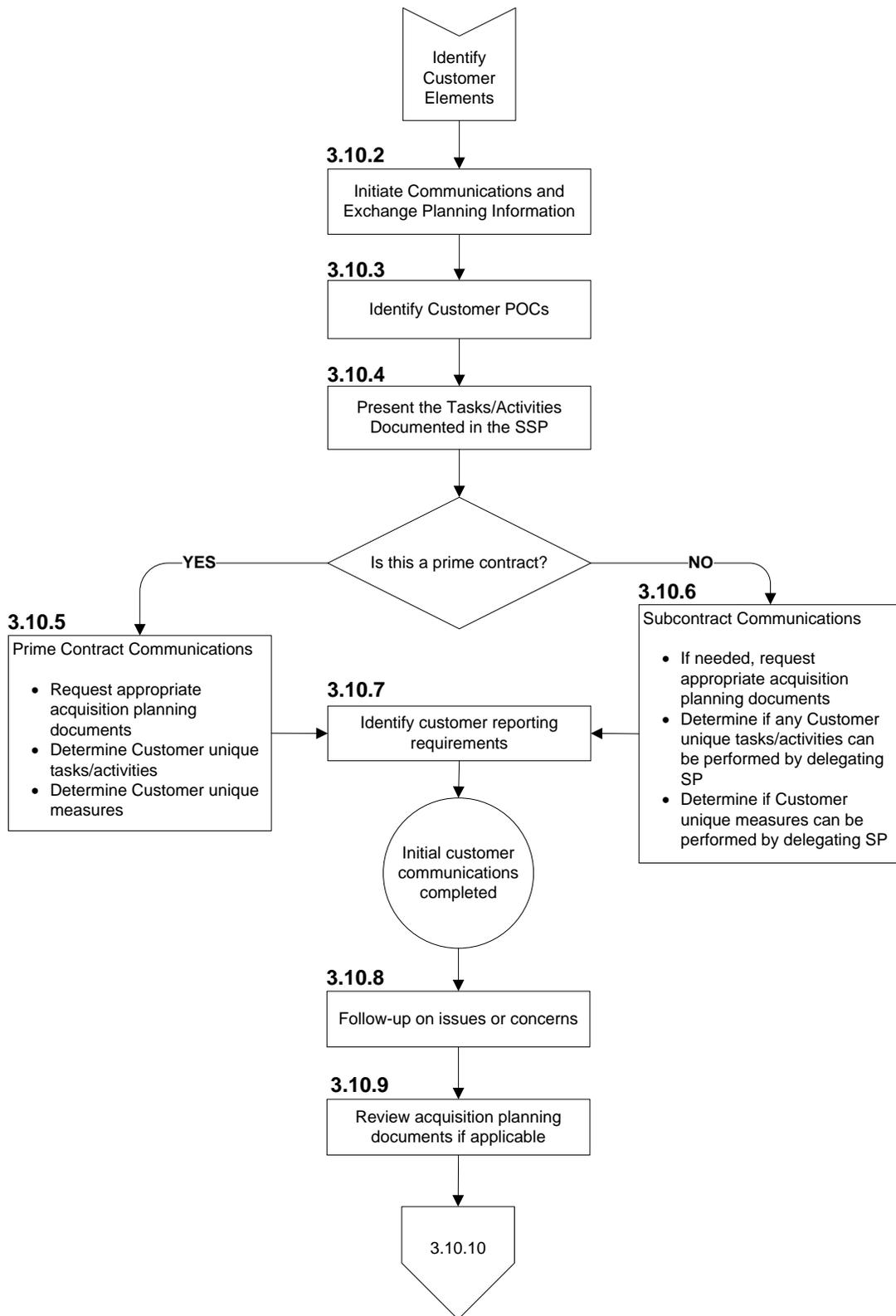
### Identify and Plan Sub-process Flowchart



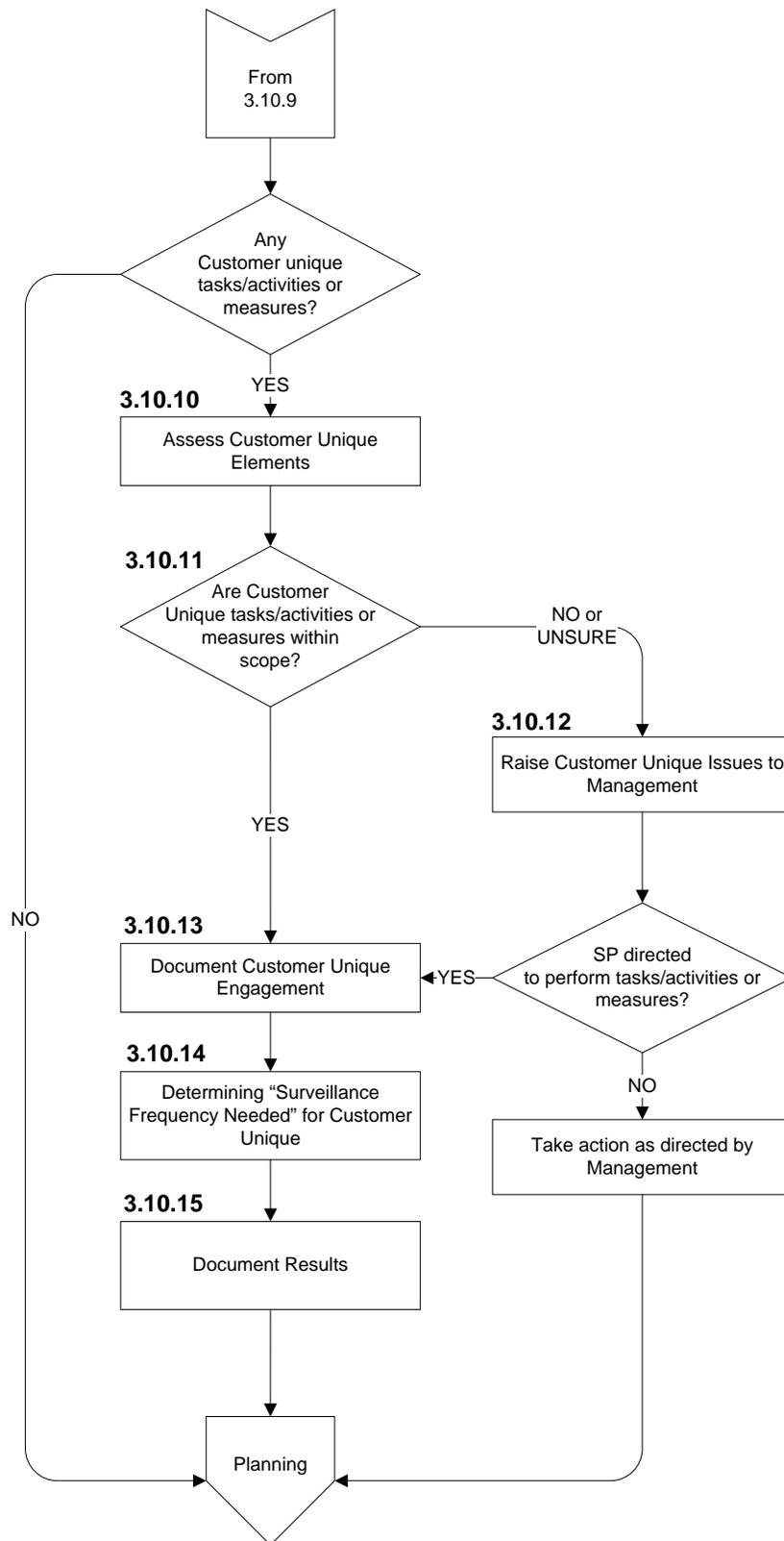
### Program Measures Sub-process Flowchart



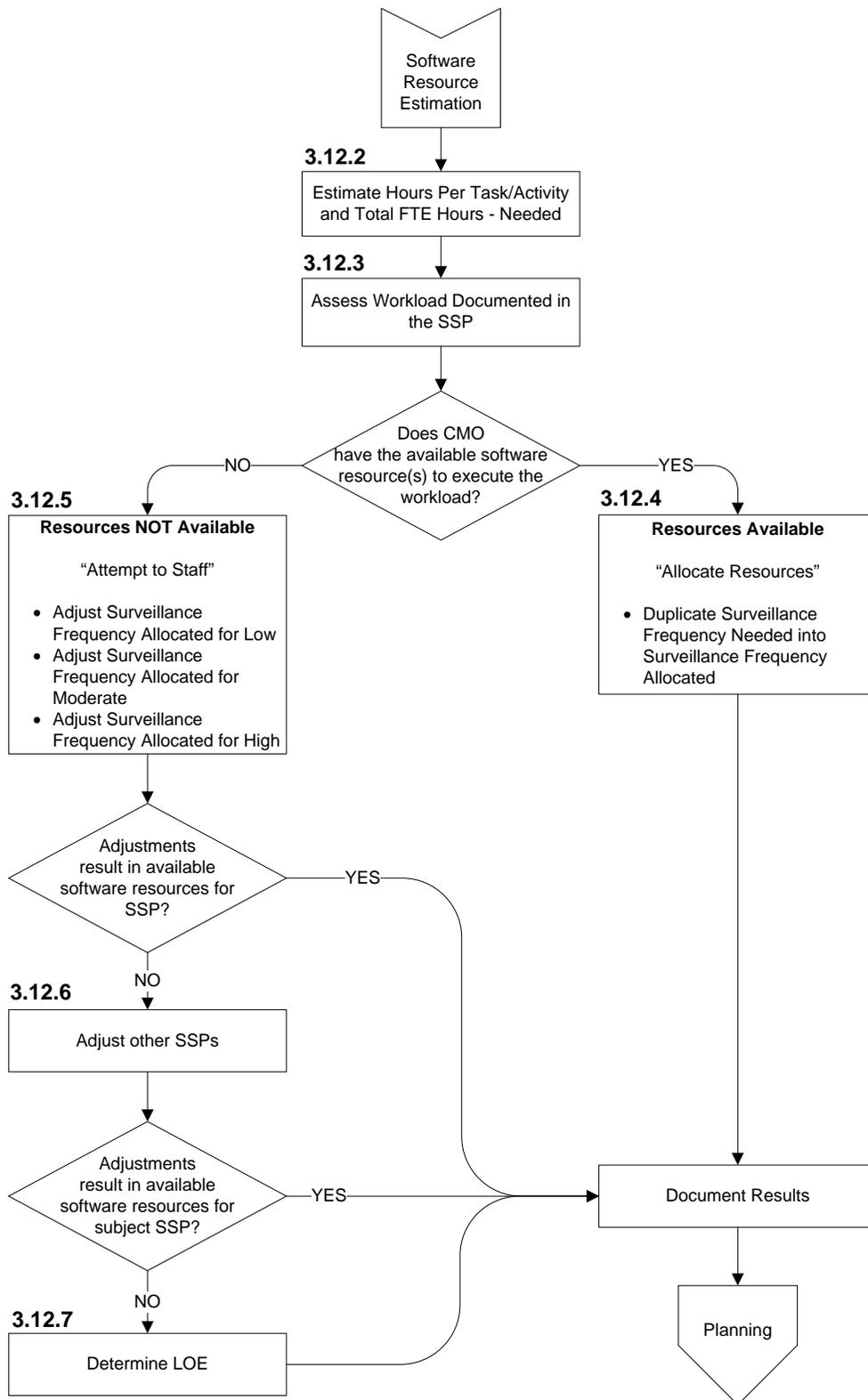
### Identify Customer Elements Sub-process Flowchart – Part 1



### Identify Customer Elements Sub-process Flowchart – Part 2

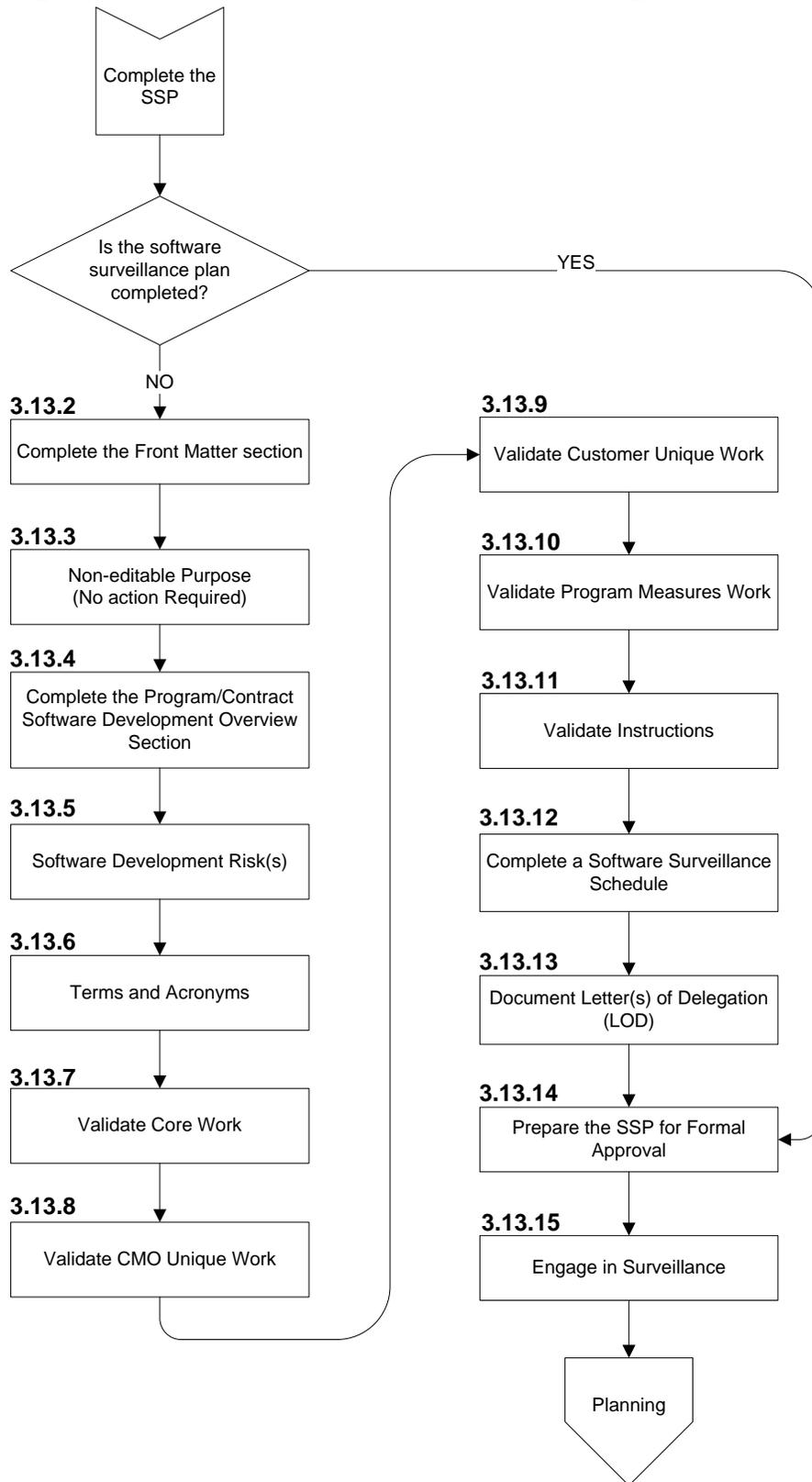


### Software Resource Estimation Sub-process Flowchart

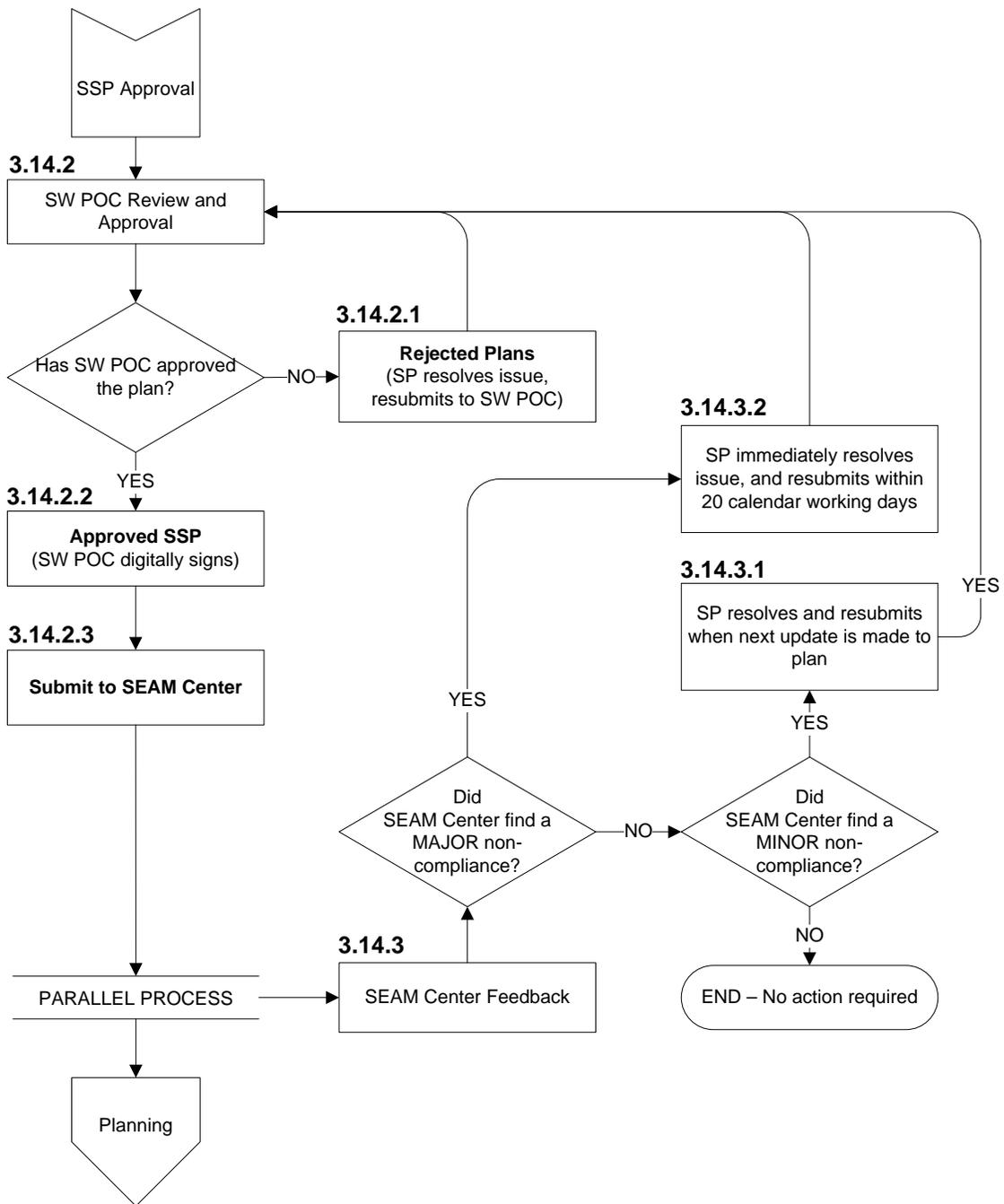




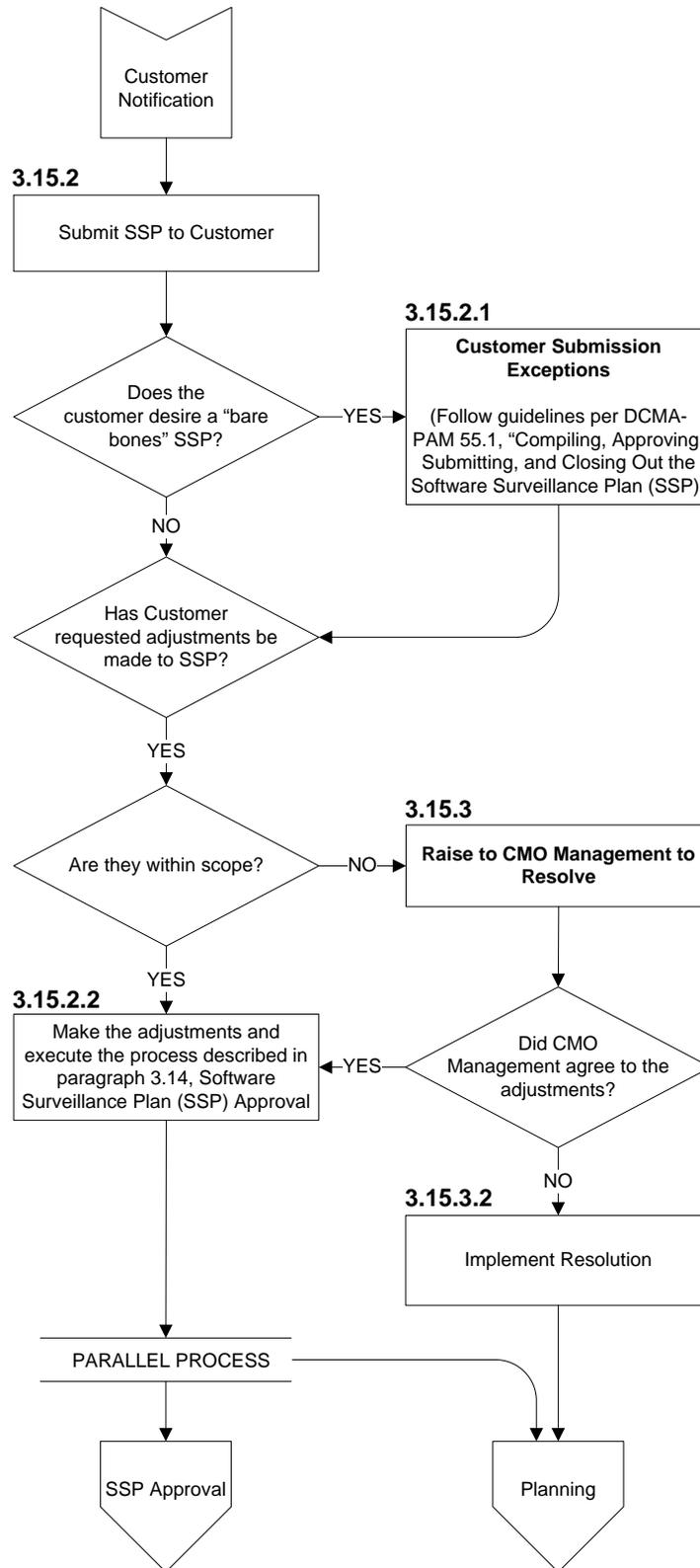
### Complete the Software Surveillance Plan (SSP) Sub-process Flowchart



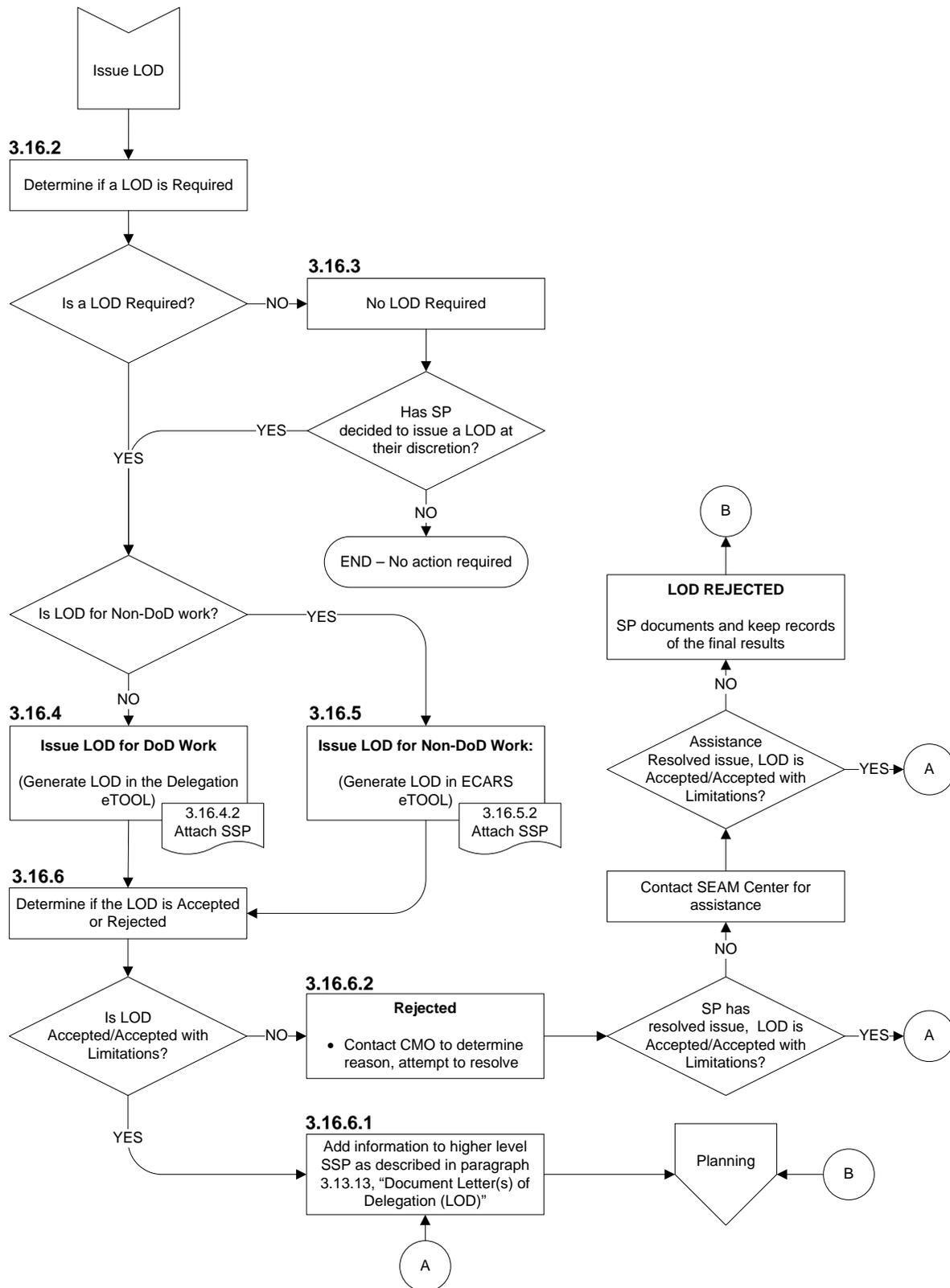
### Software Surveillance Plan (SSP) Approval Sub-process Flowchart



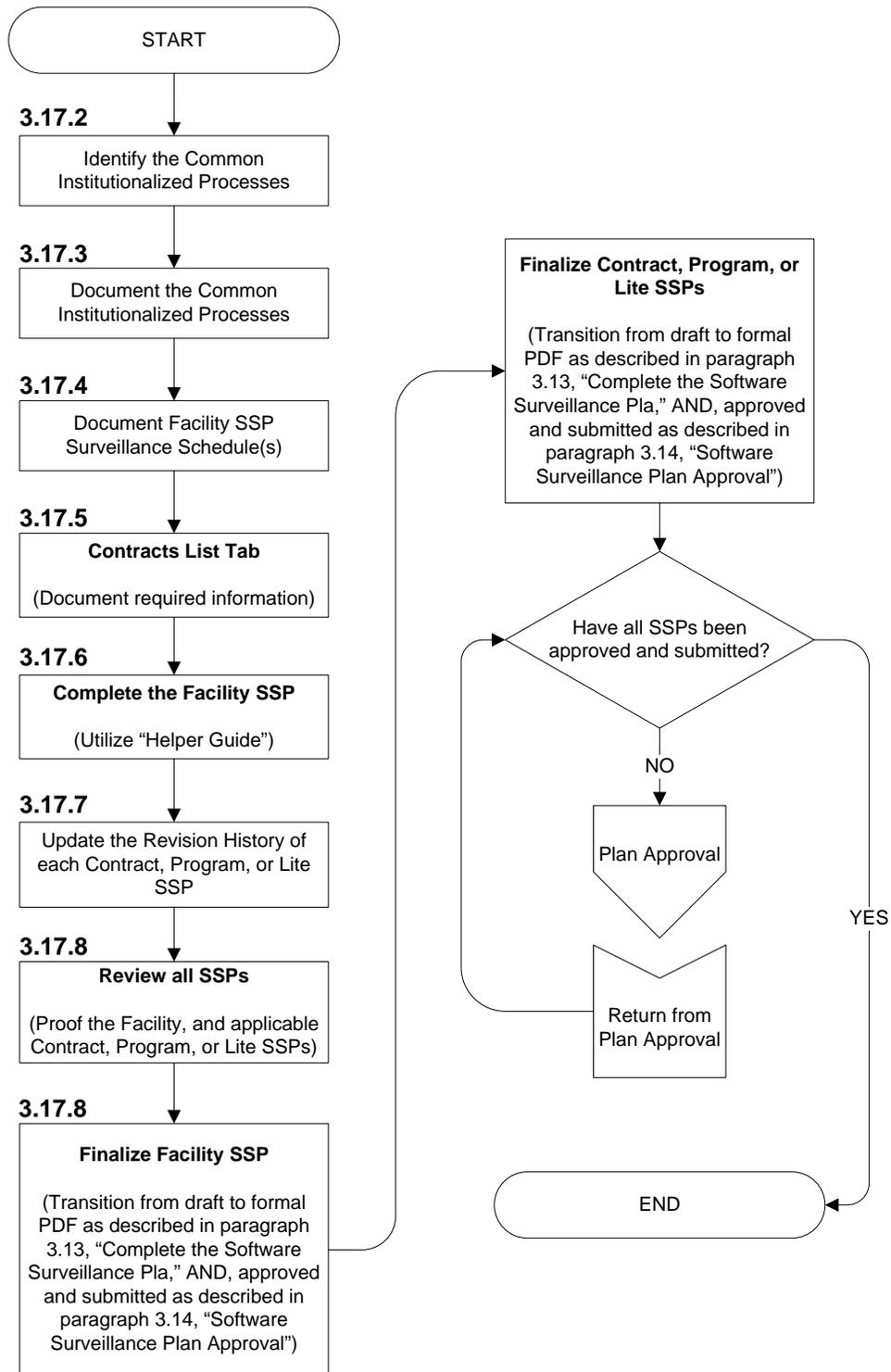
### Customer Notification Sub-process Flowchart



### Issue Letter of Delegation (LOD) Sub-process Flowchart



### Creating a Facility Software Surveillance Plan (Facility SSP) Process Flowchart



## APPENDIX C

### SOFTWARE RISK ASSESSMENT

**C.1. PERFORM SOFTWARE RISK ASSESSMENT.** This software risk assessment process is used by the SP to assess the core technical, cost, and schedule elements. The base process for software risk assessment is derived from standard risk assessment methods as discussed in the “Risk Management Guide for DoD Acquisition,” (Reference (ac)), but it is tailored to accommodate the SAM software surveillance planning process by including a WRR which the SP uses for determining the “Surveillance Frequency Needed” for engagement in the tasks/activities associated with the core technical, cost, and schedule elements.

C.1.1. Select an Core technical, Cost, or Schedule Element to Assess. Every core technical, cost, and schedule element within the SSP is assessed for risk.

**Step 1:** Select a core technical, cost, or schedule element.

**Example:** Technical - Software Quality Assurance (SQA) Element.

C.1.2. Allocate Software Risk Assessment Input Criteria.

**Step 2:** Determine the data that will be used as input information to assess the risk.

**Example:** Continuing with the Technical - SQA element for assessment, and using the following information as an input:

“Historical data shows the suppliers’ SQA has systemic issues of not following up on corrective actions issued to insure they are resolved and closed out. This systemic problem is likely to be realized on this project.”

C.1.3. Perform The Software Risk Assessment. The SP determines the “Likelihood” and “Consequence” levels.

C.1.3.1. Determine the “Likelihood” of Failure. The SP determines the “Likelihood” that the element being assessed will experience a failure that impacts performance, and uses its numerical “Level.” Additional guidance for selecting the appropriate Likelihood Level can be obtained by reading the “Risk Management Guide for DoD Acquisition,” (Reference (ac)).

**Step 3:** Using the information from Table 1 below, identify the numerical “Level” for Likelihood the “risk event will happen” based on professional judgment.

**Example:** Based on the input data allocated to the Technical - SQA Element (see Step 2), it is determined that the probability the supplier will experience a risk event caused by systemic failure to follow-up on corrective actions is: Level 4 (“Highly Likely ~70 percent”).

<b>Table 1. Likelihood</b>		
What is the “LIKELIHOOD” the risk event will happen?		
<b>Likelihood</b>	<b>Probability of Occurrence</b>	<b>LEVEL</b>
Near Certainty	~90%	<b>5</b>
Highly Likely	~70%	<b>4</b>
Likely	~50%	<b>3</b>
Low Likelihood	~30%	<b>2</b>
Not Likely	~10%	<b>1</b>

C.1.3.2. Determine the “Consequence” of Failure. The SP determines the what the “Consequence” of the failure is if the element that is being assessed fails, and uses its numerical “Level”. Additional guidance for selecting the appropriate Consequence Level can be obtained by reading the “Risk Management Guide for DoD Acquisition,” (Reference (ac)).

**Step 4:** Using the information in Table 2 below, identify the numerical “Level” for Consequence of the failure if the “risk event” occurs that is deemed to be most accurate.

**Example:** Based on the input data for this program, it is determined that if the Technical - SQA Element fails, there would be a significant negative impact, jeopardizing the program’s success. Therefore the severity of the Consequence for the Technical - SQA Element is: Level **3** (“Moderate reduction in technical performance or supportability with limited impact on program objectives”).

<b>Table 2. Consequence</b>					
<b>TECHNICAL - What is the “CONSEQUENCE” if the risk event happens?</b>					
<b>LEVEL</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Technical Performance</b>	C1 = Minimal or No consequence to technical performance	C2 = Minor reduction in technical performance or supportability, can be tolerated with little or no impact on program	C3 = Moderate reduction in technical performance or supportability with limited impact on program objectives	C4 = Significant degradation in technical performance or major shortfall in supportability; may jeopardize program success	C5 = Severe degradation in technical performance; Cannot meet KPP or key technical/ supportability threshold; will jeopardize program success
<b>SCHEDULE - What is the “CONSEQUENCE” if the risk event happens?</b>					
<b>LEVEL</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Schedule Performance</b>	C1 = Minimal or no impact	C2 = Able to meet key dates  <b>Slip is &lt; 3* month(s)</b>	C3 = Minor schedule slip. Able to meet key milestones with no schedule float  <b>Slip is &gt; 3 month(s) &lt; 6* month(s)</b>	C4 = Program critical path affected  <b>Slip is &gt; 6 month(s) and &lt; 9* month(s)</b>	C5 = Cannot meet key program milestones.  <b>Slip &gt; 9* months</b>
* For <b>Schedule</b> , the number of months used for the criteria must be identified by the SP prior to performing the risk assessment.					
<b>COST - What is the CONSEQUENCE if the risk event happens?</b>					
<b>LEVEL</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Cost Performance</b>	C1 = Minimal or no impact	C2 = Would exceed APB threshold by  < <b>1%**</b> of Budget	C3 = Would realize budget increase or unit production cost increases <b>&gt; 1% and &lt; 5%**</b> of Budget	C4 = Would realize budget increase or unit production cost increases <b>&gt; 5% and &lt; 10%**</b> of Budget	C5 = Would exceed APB threshold.  <b>&gt; 10%**</b> of Budget
** For <b>Cost</b> , the percentage of budget used for the criteria must be identified by the SP prior to performing the risk assessment. The numbers depicted inside the parentheses (e.g. 1, 5, and 10) are the recommended numbers and correspond to Earned Value criteria.					

C.1.3.3. Determine The WRR. Once the SP enters the “Likelihood” and “Consequence” Levels into the appropriate fields within the “SSP Worksheet” tab of the implemented SSP template for the Technical – SQA Element, the worksheet will automatically index the matrix in Table 3 below to determine the WRR.

**Step 5:** Using the information in Table 3 below, identify the numerical WRR for the Likelihood and Consequence combination (automatically done by the worksheet).

**Example:** Based on a Likelihood Level of 4 (Output of Step 3), and a Consequence Level of 3 (Output of Step 4), the WRR is: 17.

<b>Table 3. 5 x 5 Risk Matrix</b>						
<b>KEY PROCESS/SYSTEM RISK RATING (and Weighted Risk Rating (WRR))</b>						
<b>L I K E L I H O O D</b>	<b>5</b>	<b>L</b> WRR = <b>11(L5C1)L</b>	<b>M</b> WRR = <b>16(L5C2)M</b>	<b>H</b> WRR = <b>20(L5C3)H</b>	<b>H</b> WRR = <b>23(L5C4)H</b>	<b>H</b> WRR = <b>25(L5C5)H</b>
	<b>4</b>	<b>L</b> WRR = <b>07(L4C1)L</b>	<b>M</b> WRR = <b>12(L4C2)M</b>	<b>M</b> WRR = <b>17(L4C3)M</b>	<b>H</b> WRR = <b>21(L4C4)H</b>	<b>H</b> WRR = <b>24(L4C5)H</b>
	<b>3</b>	<b>L</b> WRR = <b>04(L3C1)L</b>	<b>L</b> WRR = <b>08(L3C2)L</b>	<b>M</b> WRR = <b>13(L3C3)M</b>	<b>M</b> WRR = <b>18(L3C4)M</b>	<b>H</b> WRR = <b>22(L3C5)H</b>
	<b>2</b>	<b>L</b> WRR = <b>02(L2C1)L</b>	<b>L</b> WRR = <b>05(L2C2)L</b>	<b>L</b> WRR = <b>09(L2C3)L</b>	<b>M</b> WRR = <b>14(L2C4)M</b>	<b>M</b> WRR = <b>19(L2C5)M</b>
	<b>1</b>	<b>L</b> WRR = <b>01(L1C1)L</b>	<b>L</b> WRR = <b>03(L1C2)L</b>	<b>L</b> WRR = <b>06(L1C3)L</b>	<b>L</b> WRR = <b>10(L1C4)L</b>	<b>M</b> WRR = <b>15(L1C5)M</b>
		<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
		<b>CONSEQUENCE</b>				

C.1.3.4. Document Rationale. The SP documents their Rationale, adding it to the appropriate cell for the Technical – SQA Element.

**Step 6:** Using the criteria that was associated with the selected element in Step 2, and any other information deemed appropriate, formulate a Summary that supports the rationale for the assessment of the selected element.

**Example:**

Consequence = 3: The Technical – SQA Element has an indirect effect on the deliverable software which is flight safety critical.

Likelihood = 4: In the past there have been numerous instances of SQA not following up on corrective actions issued.

**Example Rationale Statement:** “SQA has an indirect effect on the deliverable software which is flight safety critical. In the past, there have been numerous instances of the Contractor’s SQA organization not following up on corrective actions issued. As a result, product was shipped which was later found to be defective, and key functions rendered the system incapable of performance its mission without implementation of a work-around.”

**C.2. REPEAT SOFTWARE RISK ASSESSMENT PROCESS.** The SP repeats the software risk assessment process until all applicable core technical, cost, and schedule elements have been assessed.

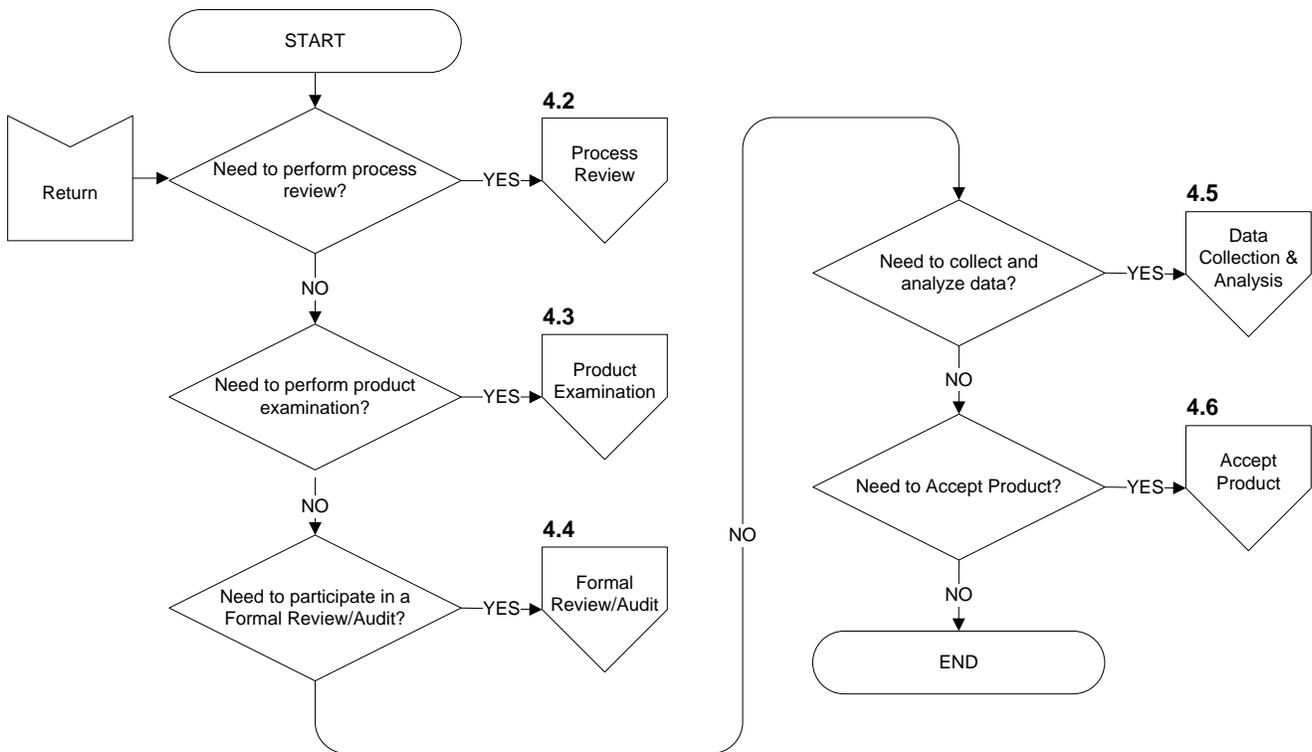
APPENDIX D

Table 4. Data/Measures Life-Cycle											
MEASURE	Applicable Performance Area			System Level		Software Phase					
	Technical	Cost	Schedule	System/Segment Requirements Analysis	System Design	SR	SD		C&UT	I&T	FQT
						Software Requirements Analysis	Preliminary Design	Detailed Design	Coding & CSU Testing	CSC Integration & Testing	CSCI Testing
Software Size	X										
Staffing	X										
Requirements Stability	X										
Technical Progress (Planned/Actual):	X		X								
Requirements	X										
Design	X										
Software Coding & Unit Testing	X										
Software Integration & Testing	X										
Formal Qualification Testing (FQT)	X										
Defects	X										
Earned Value	X	X	X								
Schedule	X		X								

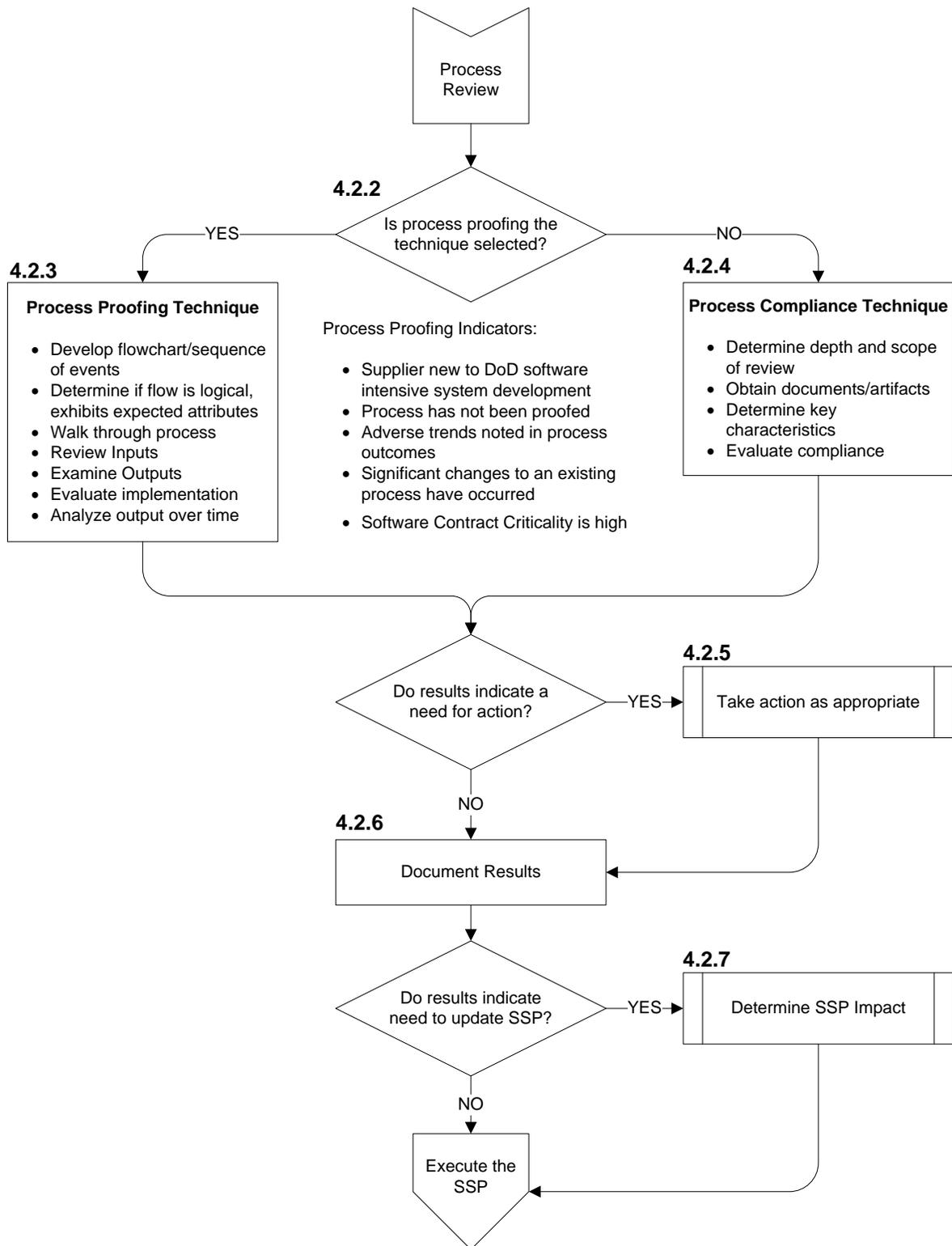
## APPENDIX E

### EXECUTE THE SOFTWARE SURVEILLANCE PLAN PROCESS FLOWCHARTS

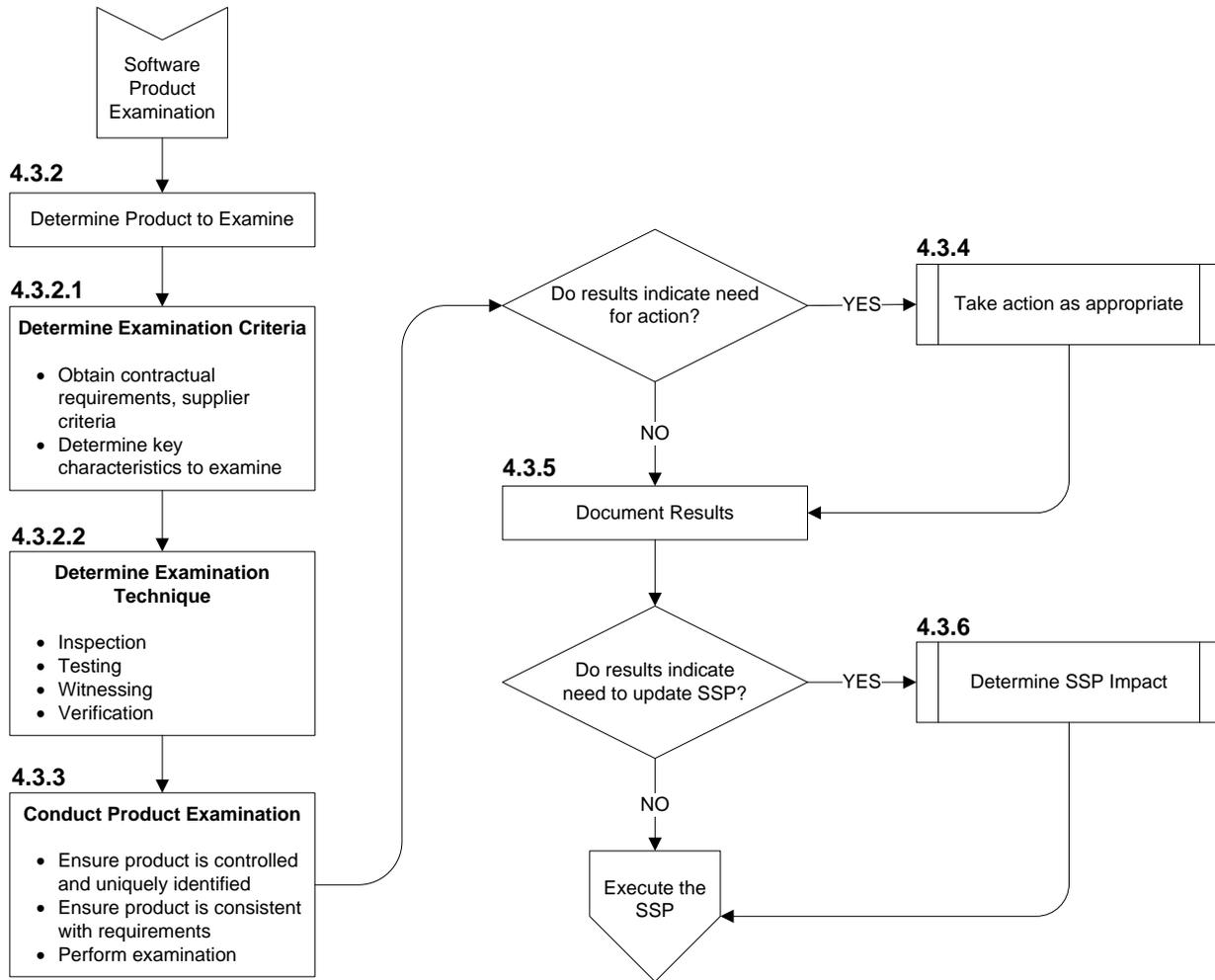
#### Overarching Process



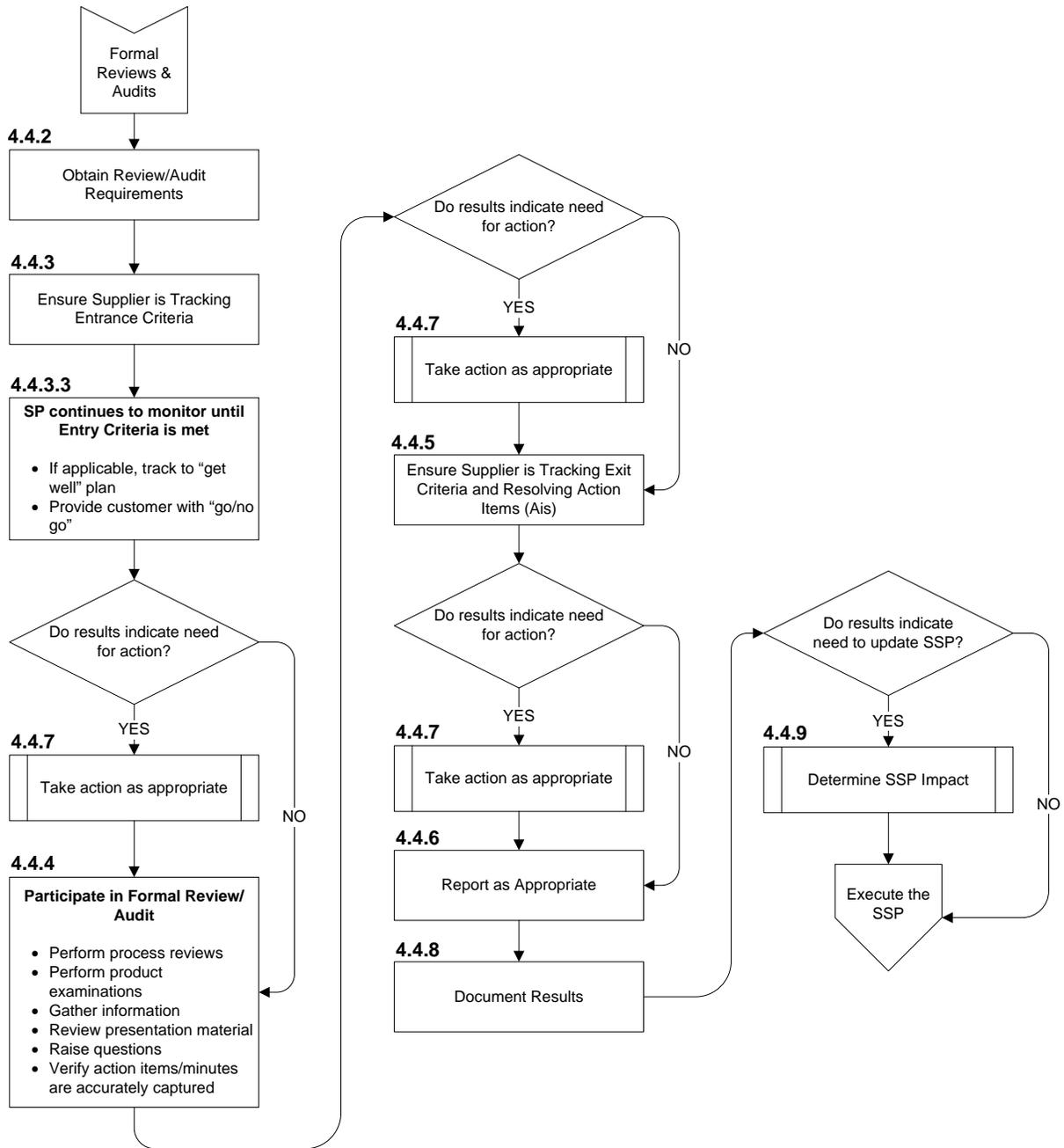
### Process Review Sub-process Flowchart



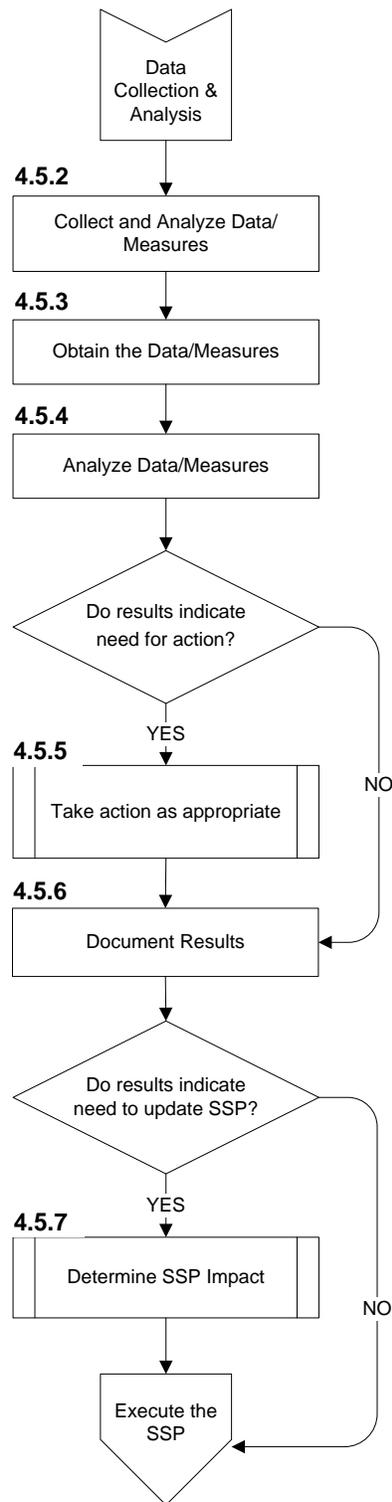
### Software Product Examination Sub-process Flowchart



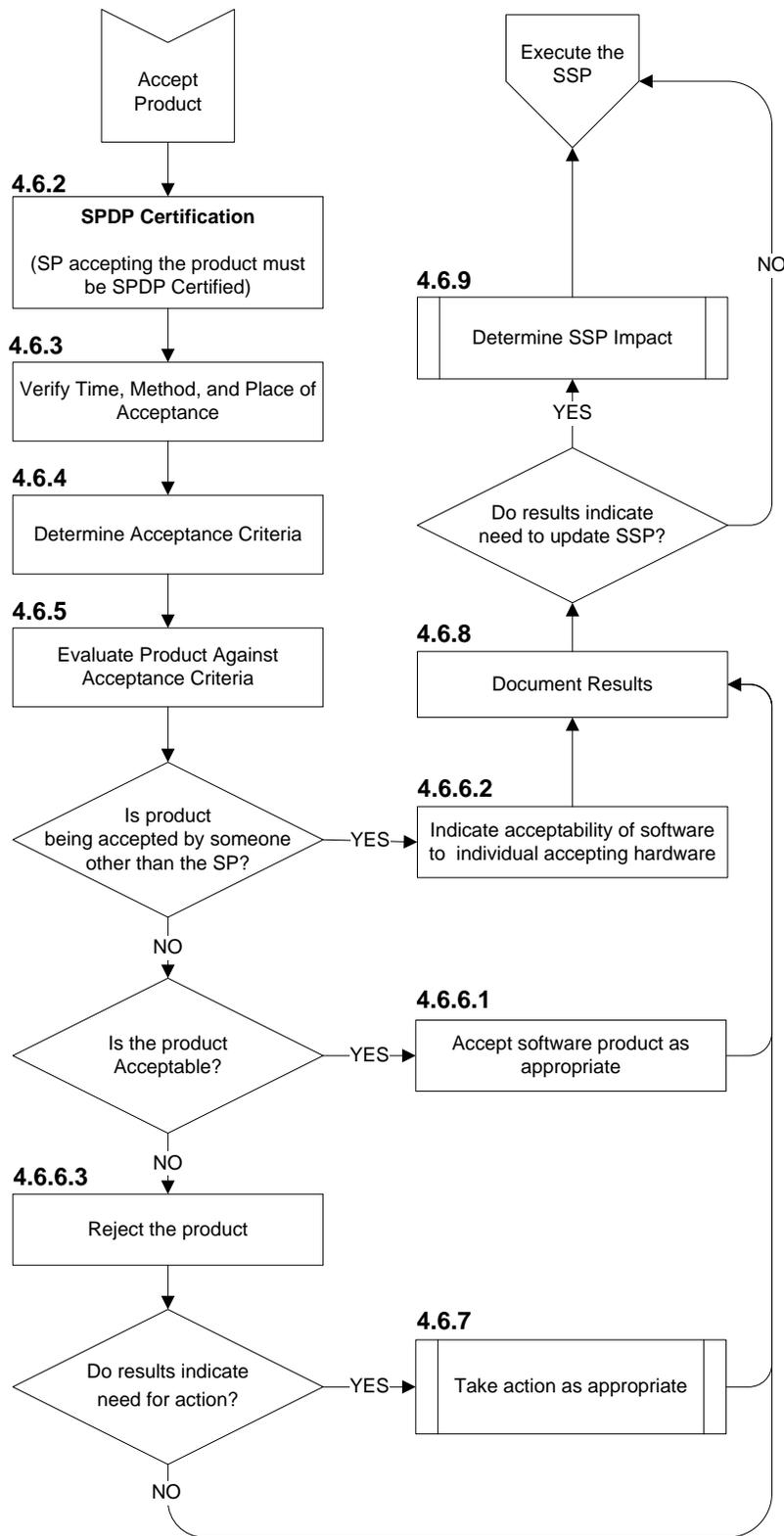
### Formal Reviews and Audits Sub-process Flowchart



### Data Collection and Analysis Sub-process Flowchart



### Accept Product Sub-process Flowchart





**APPENDIX F**

**PROCESS REVIEW AND PRODUCT EXAMINATION GOALS**

<b>Table 5. Process Review Goals</b>	
<b>Process Area</b>	<b>Goal(s)</b>
Code and Unit Test	To ensure the Supplier process results in a coding solution that effectively implements the design.
Corrective Action	To ensure the Supplier process results in identification, analysis, correction and disposition of defects and problems. To ensure the Supplier process accounts for analysis and reduced likelihood of reoccurrence.
Design	To ensure the Supplier process results in a design that effectively supports the software requirements.
Formal Test	To ensure the Supplier process results in compliant and Customer acceptable software.
Informal Test	To ensure the Supplier process adequately tests the software and allows for the capture and disposition of defects (prevents defect escapes) before formal test.
Measurement and Analysis	To ensure the Supplier collects and analyzes data so management can make informed decisions regarding program performance. (Note: this may be embedded in other process areas and not be a stand-alone process.)
Peer Reviews	To ensure the Supplier process identifies and removes defects as early as possible.
Product Integration	To ensure the Supplier process identifies and removes defects as early as possible.

Project Monitoring and Control	To ensure the Supplier process provides for monitoring and analyzing progress so appropriate actions can be taken when cost, schedule or performance deviates from the plan.
Project Planning	To ensure the Supplier process provides for establishing and maintaining plans which define the project activities.
Requirements	To ensure the Supplier process effectively identifies, develops, manages, and controls software requirements and satisfactorily addresses safety and security requirements that meet Customer needs.
Risk Management	To ensure the Supplier process provides for identifying, developing and implementing a risk mitigation strategy.
Software Configuration Management (SCM)	To ensure the Supplier process establishes and maintains the integrity of software work products.
Software Quality Assurance (SQA)	To ensure the Supplier process objectively evaluates software products and processes, and non-compliances are identified, documented and resolved.
Subcontractor Management	To ensure the Supplier process provides for controlling and managing the acquisition of products or services.

<b>Table 6. Product Examination Goals</b>	
<b>Product Area</b>	<b>Goal(s)</b>
Software Product Examination	To ensure the Supplier is producing software products that meet specification, format and documentation, and performance requirements. (Deliverable products and non-deliverable supporting artifacts are developed and documented in a timely manner and meet requirements.)
Software Development Plan (SDP)	To ensure SDP is accurate, complete, correct and suitable for the project. <ul style="list-style-type: none"> <li>• Scope of SDP accurately reflects project</li> <li>• Contains correct reference documents</li> <li>• Overview of required work included (e.g., requirements and constraints, acquisition strategy)</li> <li>• Plans for software development activities (e.g., development methods, standards for products)</li> <li>• Project planning and oversight</li> <li>• Software engineering environment (e.g., lab, tools)</li> <li>• Schedules reflect work to be accomplished</li> <li>• Project organization and resources are assigned</li> </ul>
Software Development Folders/Files (SDF)	To ensure SDF is accurate, complete, and correct. <ul style="list-style-type: none"> <li>• Requirements for each software component</li> <li>• Design</li> <li>• Test planning, cases, procedures at each level</li> <li>• Deficiency/problem reports and actions taken</li> </ul>
System/Segment Specification (S/SS)	To ensure SSS is produced using the supplier standard and is complete. <ul style="list-style-type: none"> <li>• Correct reference documents</li> <li>• Software requirements</li> <li>• Qualification methods</li> <li>• Requirements traceability (required capabilities are clear and realistic)</li> </ul>

System/Subsystem Design Document (S/SDD)	<p>To ensure S/SDD is accurate, complete, and correct.</p> <ul style="list-style-type: none"> <li>• Correct reference documents</li> <li>• Subsystem and System-wide design decisions</li> <li>• System architectural design</li> <li>• Requirements traceability</li> </ul>
Software Test Plan (STP)	<p>To ensure STP is accurate, complete, and correct.</p> <ul style="list-style-type: none"> <li>• Scope of test coverage (including dependencies on GFE if applicable) is described</li> <li>• Correct reference documents</li> <li>• Software test environment</li> <li>• Test definition</li> <li>• Tests to be performed</li> <li>• Test schedule</li> <li>• Requirements traceability</li> </ul>
Software Test Descriptions (STD)	<p>To ensure STD is accurate, complete, and correct.</p> <ul style="list-style-type: none"> <li>• Correct reference documents</li> <li>• Test preparation</li> <li>• Test descriptions</li> <li>• Requirements traceability</li> </ul>
Software Test Report (STR)	<p>To ensure STR is accurate, complete, and correct.</p> <ul style="list-style-type: none"> <li>• Correct reference documents</li> <li>• Overview of test results</li> <li>• Detailed test results (e.g., problems encountered, deviations from cases/procedures)</li> <li>• Test log</li> </ul>
Software Requirements Specification (SRS)	<p>To ensure SRS is produced using the supplier standard and is complete.</p> <ul style="list-style-type: none"> <li>• Correct reference documents</li> <li>• Software requirements</li> <li>• Qualification methods</li> <li>• Requirements traceability</li> </ul>

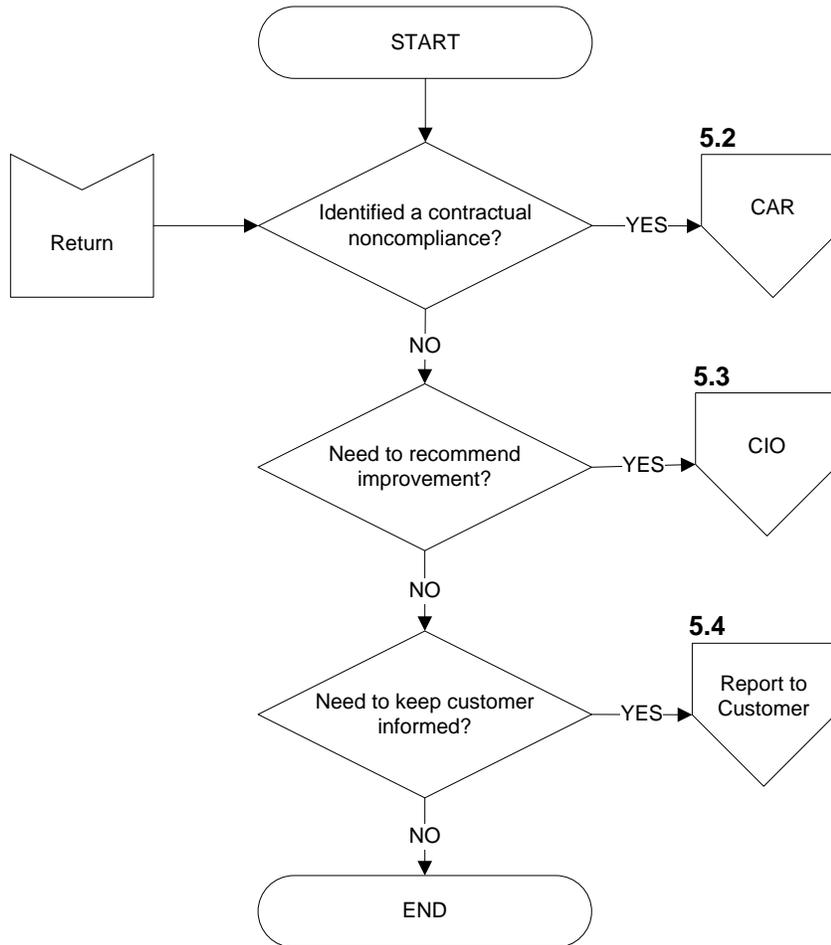
Interface Requirements Specification (IRS)	<p>To ensure IRS is produced using the supplier standard.</p> <ul style="list-style-type: none"> <li>• Correct reference documents</li> <li>• Interface requirements</li> <li>• Qualification methods</li> <li>• Requirements traceability</li> </ul>
Software Design Document (SDD)	<p>To ensure SDD is accurate, complete, and correct.</p> <ul style="list-style-type: none"> <li>• Correct reference documents</li> <li>• Software design</li> <li>• Requirements traceability</li> <li>• Is understandable</li> </ul>
Interface Design Document (IDD)	<p>To ensure IDD is accurate, complete, and correct.</p> <ul style="list-style-type: none"> <li>• Correct reference documents</li> <li>• Software Interface design</li> <li>• Requirements traceability</li> <li>• Is understandable</li> </ul>
Source Code	<p>To ensure source code is accurate, complete, and correct.</p> <ul style="list-style-type: none"> <li>• Code conforms to documentation requirements and coding standards/conventions</li> <li>• Unit tests are developed for target code</li> <li>• Evaluate CSU test results/test procedures/test descriptions</li> <li>• Peer review/walkthrough follow-up have occurred</li> <li>• Test procedures for conducting integration and testing of the module in development</li> <li>• SDFs reflect unit of code status</li> <li>• CM of unit IAW supplier Standards</li> <li>• Traceability</li> </ul>
Software Version Description (SVD)	<p>To ensure SVD is accurate, complete, and correct.</p> <ul style="list-style-type: none"> <li>• Correct reference documents</li> <li>• Version description (e.g., changes installed, installation instructions, possible problems and known errors)</li> </ul>

<p>Software Product Specification (SPS)</p>	<p>To ensure SPS is produced using the sSupplier standard and is complete.</p> <ul style="list-style-type: none"><li>• Correct reference documents</li><li>• Software requirements</li><li>• Required deliverable references:<ul style="list-style-type: none"><li>o Source code</li><li>o Executable source files</li></ul></li><li>• Qualification methods</li><li>• Requirements traceability</li></ul>
<p>Requirements Verification Traceability Matrix</p>	<p>To ensure requirements are traceable and matrix is accurate, complete, and correct.</p> <ul style="list-style-type: none"><li>• Requirements traceability (specified/derived requirements)</li><li>• Test traceability</li></ul>

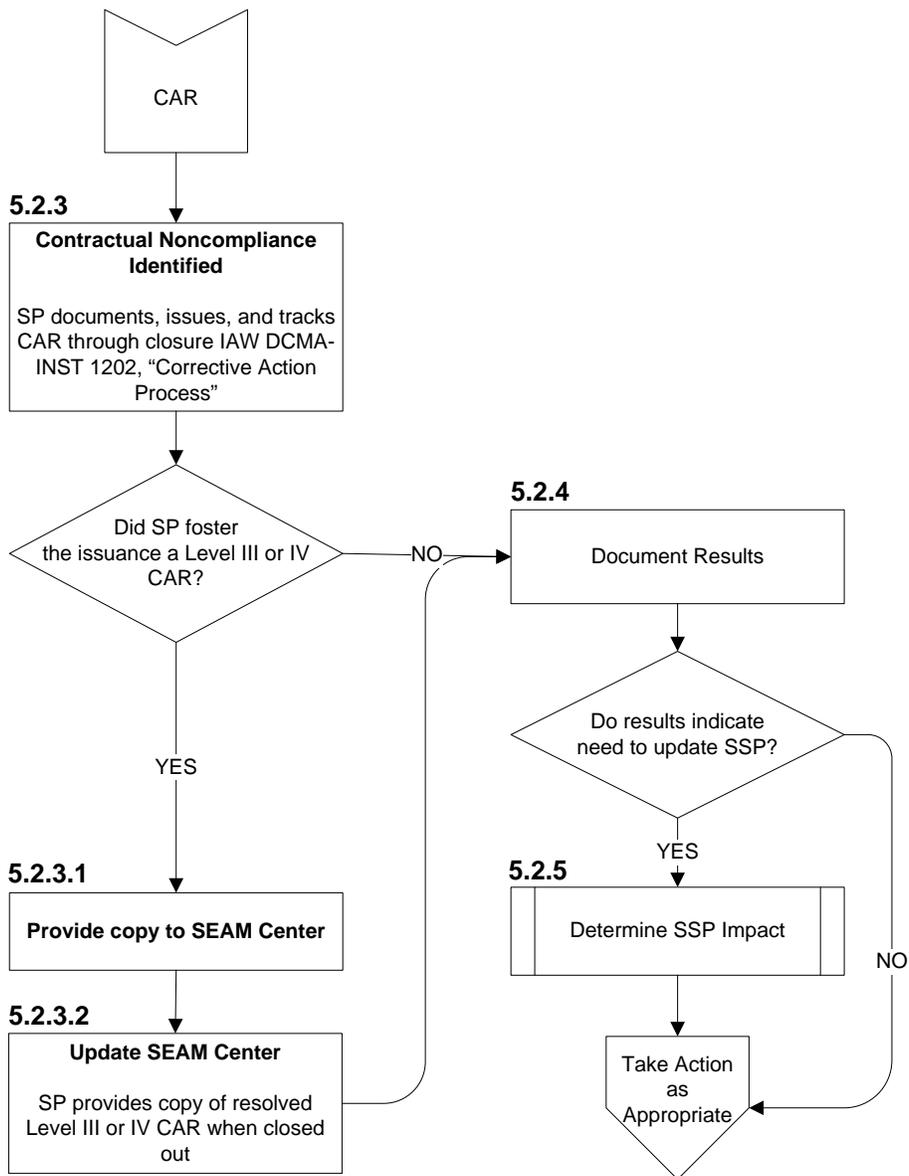
### APPENDIX G

#### TAKE ACTION AS APPROPRIATE PROCESS FLOWCHARTS

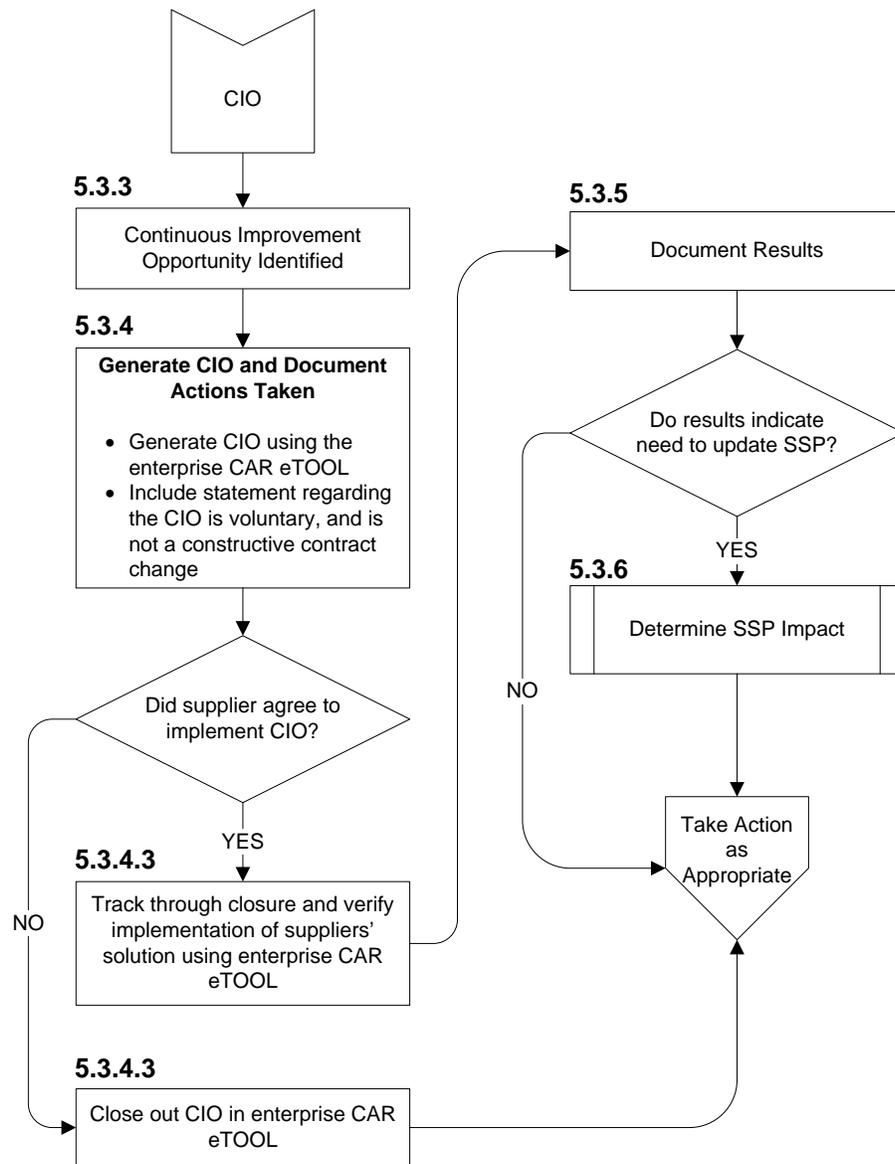
##### Overarching Process



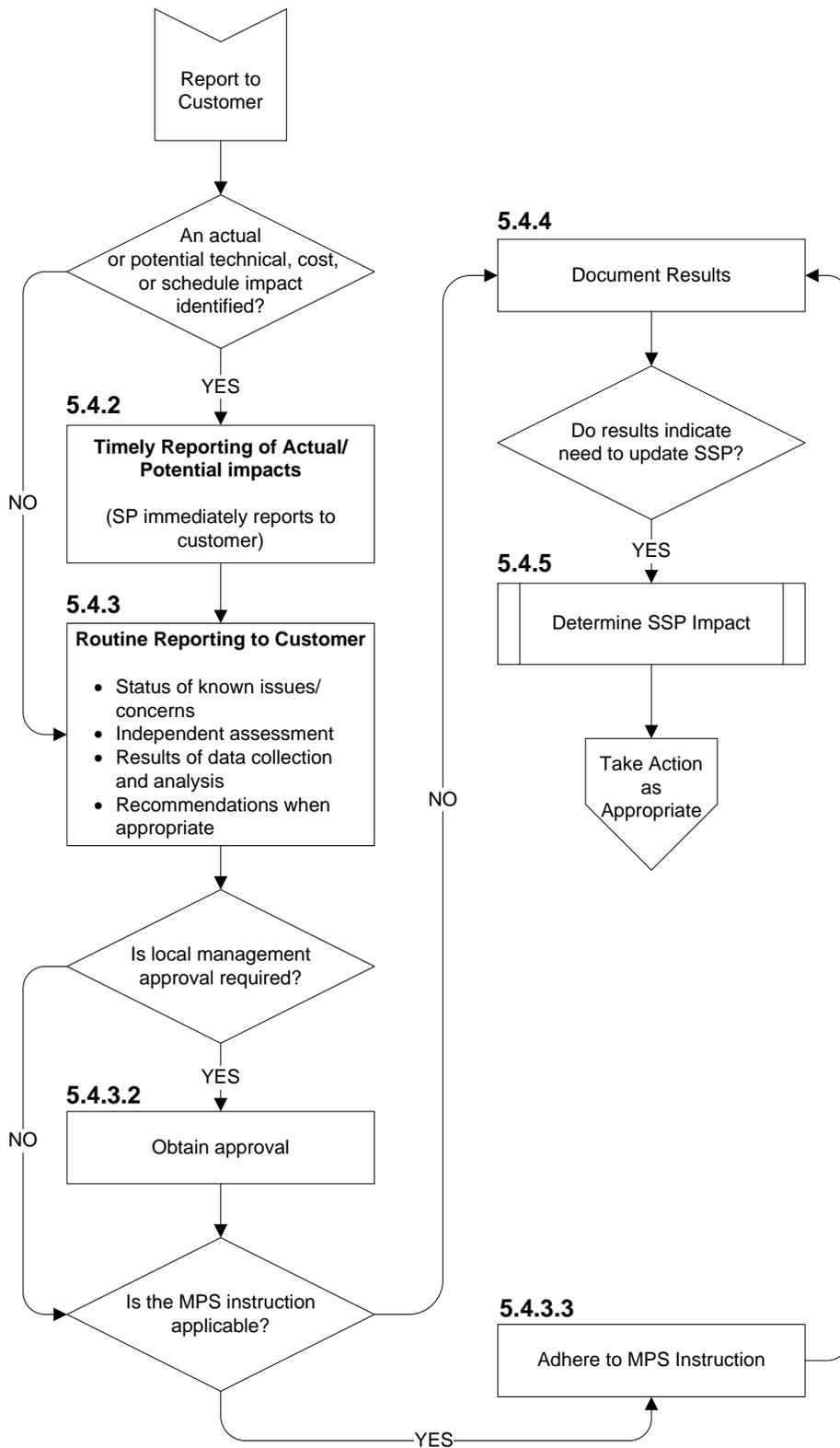
### Continuous Improvement Opportunity (CIO) Sub-process Flowchart



### Continuous Improvement Opportunity (CIO) Sub-process flowchart



### Report to Customer Sub-process Flowchart



## GLOSSARY

### DEFINITIONS

**Accept Product.** The action(s) taken by the Software Professional to verify if a software related product/service satisfies the requirements of the contract – thereby allowing the product/service to be accepted by the Government.

**Acquisition Customer.** The actual contracting officer that issued the contract (also see “Customer”).

**CMO Allocated Hours.** The actual amount of time that has been allocated to perform a task/activity over the duration of the life-cycle for the SSP. It is calculated based on: “Surveillance Frequency Allocated” x “Hours Per Task/Activity.”

**CMO Estimated Hours Per Task/Activity.** The estimated time (in hours and 15 minute increments) it would take to perform a task/activity as determined by the SP/CMO management.

**CMO Unallocated Hours.** The actual amount of time that has not been allocated to perform a task/activity over the duration of the life-cycle for the SSP. It is calculated based on: “Total Hours Needed” - “CMO Allocated Hours.”

**CMO Unique Measures.** Optional measures that are determined by the SP that will be collected, analyzed, and reported.

**CMO Unique Tasks/Activities.** Tasks/activities related to DCMA internal business processes that need to be performed that are not already pre-identified as a core technical, cost, or schedule element sections of the Software Surveillance Plan (SSP).

**Customer.** A DCMA functional specialist or CMO (that is not the Acquisition Customer) which has delegated work to a supporting SP located at a subcontractor facility (also see “Acquisition Customer”).

**Customer Unique Measures.** Any measure the customer requests the SP to collect, analyze, and report on that is not already a pre-defined core, contractually imposed standalone/TPM, or a CMO unique measure.

**Customer Unique Tasks/Activities.** A task/activity requested by the Customer (aka: “Mandatory’s”) that is not already pre-defined as a core technical, cost, schedule, or defined as a CMO unique task/activity.

**Data Collection and Analysis.** The process of obtaining data/measures, performing analysis, determining trends (negative/positive), taking action when necessary, and reporting.

**Data/Measures Analysis Results (DMAR).** Worksheet used to capture and document data/measures analysis results.

**Data/Measures Analysis Specification (DMAS).** The DMAS contains the detailed information about for how a data/measure (e.g., source of data, sample chart/graph, thresholds for analysis) will be collected, analyzed, and reported.

**Hours Per Task/Activity.** The estimated time (in hours and 15 minute increments) it would take to perform a task/activity as automatically calculated by the implemented SSP template.

**Optional Surveillance Notes.** The field within the SSP Worksheet where the SP can record notes for a task/activity.

**Program Measures.** The core measures, contractually imposed standalone and Technical Performance Measures (TPMs), CMO unique (SP defined), and customer unique data/measures that will be collected and analyzed.

**Software Contract Criticality (SCC).** SCC is the overall contract rating determined by the Software Professional for Technical Performance, Cost, and Schedule. The SCC determines the level of DCMA involvement.

**Software Risk Assessment.** The process the SP executes to determine the risk for a process area (e.g., Software Quality Assurance (SQA), Software Configuration Management (SCM), Software Requirements Analysis (SRA) phase of software development).

**Software Resource Estimation.** The process of determining the required DCMA resources needed to perform software acquisition management activities.

**Software Surveillance Plan Worksheet (SSP Worksheet).** The worksheet within the Contract, Program, Lite, or Facility Software Surveillance Plan (SSP) template where the SP documents the tasks/activities to be performed.

**Core Measures.** The default mandatory pre-defined measures the SP is required to collect, analyze, and report.

**Standalone Measure.** A specified measure (excluding a Technical Performance Measure (TPM)) that is imposed on the supplier by the contract that is not a pre-defined core, CMO unique, or customer unique measure.

**Surveillance Frequency Allocated.** The number of times a task/activity will be engaged in based on functional resource availability.

**Surveillance Frequency Needed:** The number of times a task/activity needs to be engaged in based on risk, contractual requirements, customer specification, or as determined by the SP.

**Templates.** The automated tools used by the SP to document surveillance related work (e.g., Contract/Program/Lite/Facility SSP, DMAS/DMAR).

**Total Hours – Needed.** The total number of hours required to perform 100 percent of the software surveillance tasks/activities identified in the Software Surveillance Plan (SSP).

**Weighted Risk Rating (WRR).** A numerical indicator utilized for determining the Frequency of surveillance engagement (a single digit ranging from 1 to 25 derived from the standard DoD 5 x 5 Likelihood/Consequence Risk Matrix).

## GLOSSARY

### ACRONYMS

aka	also known as
ACAT	Acquisition category
AI	action items
CAR	Corrective Action Request
CDR	Contract Deficiency Report
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CDW	Contract data workflow
CIO	Continuous Improvement Opportunity
CLIN	Contract Line Item Number
CMMI	Capability Maturity Model Integrated
CMO	Contract Management Office
COTS	Commercial off-the-shelf
CSCI	Computer Software Configuration Item
DCMA-INST	DCMA Instruction
DFARS	Defense Federal Acquisition Regulation Supplement
DMAR	Data/Measure Analysis Results
DMAS	Data/Measure Analysis Specification
DO	Delivery Order
DPAS	Defense Priorities and Allocation System
ECARS	Electronic Contract Administration Request System
EDA	Electronic Document Access
EDW	Electronic data workflow
EMD	Engineering and Manufacturing Development
EV	Earned Value
FARS	Federal Acquisition Regulation
FCA	Functional Configuration Audit
FFP	Firm Fixed Price
FTE	full-time equivalent
GFE	Government-furnished equipment
GFI	Government-furnished information

GFM	Government-furnished material
GOTS	Government off-the-shelf
GS	general schedule
I&A	Inspection and Acceptance
IAW	In accordance with
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IRS	Interface Requirements Specification
IV&V	Independent Verification and Validation
LOD	Letter of Delegation
LOE	Level of effort
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSA	Material Solution Analysis
NDI	Non-developmental item
O&S	Operations and Support
PAO	Post award orientation
P&D	Production and Deployment
PCA	Physical Configuration Audit
PDF	portable document format
PDR	Preliminary Design Review
PLAS	Performance Labor Accounting System
PMO	Program Management Office
PO	Purchase Order
POC	Point of contact
PST	Program Support Team
QA	Quality Assurance
QALI	Quality Assurance Letter of Instruction
RMP	Risk Management Plan
SAM	Software Acquisition Management
SCAMPI	Standard CMMI Appraisal Method for Process Improvement

SCC	Software Contract Criticality
SDP	Software Development Plan
SEAM	Software Engineering and Acquisition Management
SEP	Systems Engineering Plan
SI	Software Item
SOW	Statement of work
SP	Software Professional
SPDP	Software Professional Development Program
SPR	Software Problem Report
SQA	Software quality assurance
SQAP	Software Quality Assurance Plan
SRA	Software Requirements Analysis
SRR	Software Requirements Report
SRR	System/Software Requirements Review
SRS	Software Requirements Specification
SSP	Software Surveillance Plan
SSR	Software Surveillance Record
SW POC	Software Point of Contact
STP	Software Test Plan
TD	Technology Development
TEMP	Test Evaluation Master Plan
TOC	Table of Content
TPM	Technical Performance Measure
TRR	Test Readiness Review
VTC	Video Teleconference Communications
WBS	Work breakdown structure
WRR	Weighted Risk Rating