Products for Review Draft OUSD A&S SW Acq Docs (July 2019)
-Software Acquisition Pathway Policy
-Business Decision Guidance

#	Product (Selection)	Section Title or Identifier	Category
1	**Policy (Software Acquisition Pathway Policy)**	**Global**	**Technical**
1	**Policy (Software Acquisition Pathway Policy)**	**Global**	**Technical**
2	**Policy (Software Acquisition Pathway Policy)**	**Global**	**Technical**
3	**Policy (Software Acquisition Pathway Policy)**	**Global**	**Technical**
3	**Policy (Software Acquisition Pathway Policy)**	**Global**	**Technical**
4	**Policy (Software Acquisition Pathway Policy)**	**Policy, (c) MVP, MVCR; Fig 1 SW Pathway**	**General**
4	**Guidance (Business Decision Guidance)**	**6. Metrics Plan**	**Technical**
5	**Policy (Software Acquisition Pathway Policy)**	**Applicability (c)**	**Technical**
1	Guidance (Business Decision Guidance)	Global	General
2	Guidance (Business Decision Guidance)	Global	Editorial
3	Guidance (Business Decision Guidance)	Pg 1	General
4	Guidance (Business Decision Guidance)	Global	General
5	Guidance (Business Decision Guidance)	Global	General
6	Guidance (Business Decision Guidance)	Global (e.g., line 403)	Technical
7	Guidance (Business Decision Guidance)	2, User Agreement, line 93, 95	Editorial

8	Guidance (Business Decision Guidance)	2, User Agreement, line 54, "cooperative"	Editorial
9	Guidance (Business Decision Guidance)	2, Establishing Roles and Responsibilities, line 117	General
10	Guidance (Business Decision Guidance)	2, Establishing Roles and Responsibilities, line 64	General
11	Guidance (Business Decision Guidance)	Global	General
12	Guidance (Business Decision Guidance)	3	Technical
13	Guidance (Business Decision Guidance)	3, Acquisition Strategy, Agile Framework, line 91	Technical
14	Guidance (Business Decision Guidance)	3, Acquisition Strategy, line 110, DevSecOps	Technical
15	Guidance (Business Decision Guidance)	3, Acquisition Strategy, line 110-113, "should"	Technical
16	Guidance (Business Decision Guidance)	3, Acquisition Strategy, pg 6, line 121 (access to source code)	Technical
17	Guidance (Business Decision Guidance)	4, Cost Estimates, Realignment Considerations (line 172, "shall"?)	Technical
18	Guidance (Business Decision Guidance)	5, Enterprise Services and DevOps, figure	General
19	Guidance (Business Decision Guidance)	5, Use of DevSecOps determination, DevSecOps SLA, line 187	Editorial
20	Guidance (Business Decision Guidance)	5, DevSecOps Enterprise SLA (line 193)	Editorial
21	Guidance (Business Decision Guidance)	6, Metrics Plan, Realignment Considerations, line 382	Editorial
22	Guidance (Business Decision Guidance)	6, Metrics Plan, Realignment Considerations, line 394	General
23	Guidance (Business Decision Guidance)	7, MVP, 3rd para, main purpose (line 411)	General
24	Guidance (Business Decision Guidance)	8, cATO, Guiding Principles, NIST SP 800-53, line 511)	Technical
25	Policy (Software Acquisition Pathway Policy)	Global	General
26	Policy (Software Acquisition Pathway Policy)	Applicability	General

27	Policy (Software Acquisition Pathway Policy)	Global	Technical
28	Policy (Software Acquisition Pathway Policy)	Global	General
29	Policy (Software Acquisition Pathway Policy)	Global	General
30	Policy (Software Acquisition Pathway Policy)	Pg 2, (e)	Technical
31	Policy (Software Acquisition Pathway Policy)	Pg 2, (e)	Technical
32	Policy (Software Acquisition Pathway Policy)	Pg4, User Agreement	General
33	Policy (Software Acquisition Pathway Policy)	Pg 2, (d)	Technical
34	Policy (Software Acquisition Pathway Policy)	Pg 2, (c)	Technical
35	Policy (Software Acquisition Pathway Policy)	Pg 5,Execution Phase, Para 4, Line 194-208	Technical

36	Policy (Software Acquisition Pathway Policy)	Global	Technical
37	Policy (Software Acquisition Pathway Policy)	Pg 4, Planning, Cost Estimates	Technical
38	Policy (Software Acquisition Pathway Policy)	Policy, Line 39, bullet a	Technical
39	Policy (Software Acquisition Pathway Policy)	Policy, Line 47, bullet b	Technical
40	Policy (Software Acquisition Pathway Policy)	Policy, Line, Line 57	Technical
41	Policy (Software Acquisition Pathway Policy)	Policy, Line 60	Technical
42	Policy (Software Acquisition Pathway Policy)	Policy, Line 65	Technical

43	Policy (Software Acquisition Pathway Policy)	Policy, Line 71	General
44	Policy (Software Acquisition Pathway Policy)	Policy, Line 79	Technical
45	Policy (Software Acquisition Pathway Policy)	Policy, Line 83	Technical
46	Policy (Software Acquisition Pathway Policy)	Policy, Line 88	Technical
47	Policy (Software Acquisition Pathway Policy)	Policy, Line 94	General
48	Policy (Software Acquisition Pathway Policy)	Policy, Line 119	Technical
49	Policy (Software Acquisition Pathway Policy)	Policy, Line 135	Technical
50	Policy (Software Acquisition Pathway Policy)	Policy, Line 138	Technical
51	Policy (Software Acquisition Pathway Policy)	Policy, Line 144	Technical
52	Policy (Software Acquisition Pathway Policy)	Policy, Line 155	Technical
53	Policy (Software Acquisition Pathway Policy)	Policy, Line 202	Technical
54	Policy (Software Acquisition Pathway Policy)	Policy, Line 244	Technical

55	Policy (Software Acquisition Pathway Policy)	Policy, Line 250	Technical
56	Guidance (Business Decision Guidance)	Section 1, Capability Needs Statememnt	Technical
57	Guidance (Business Decision Guidance)	Operational Context	Technical
58	Guidance (Business Decision Guidance)	Threat Summary	Technical
59	Guidance (Business Decision Guidance)	2. User Agreement	Technical
60	Guidance (Business Decision Guidance)	Roles aned Responsibilities	Technical
61	Guidance (Business Decision Guidance)	Activities Covered	Technical
62	Guidance (Business Decision Guidance)	Acquisition Strategy	Technical
63	Guidance (Business Decision Guidance)	Costing based on Work	Technical
64	Guidance (Business Decision Guidance)	Cost estimates	Technical
65	Guidance (Business Decision Guidance)	5. Enterprise Services	Technical
66	Guidance (Business Decision Guidance)	Security and Testing	Technical
67	Guidance (Business Decision Guidance)	Continous ATO	Technical

68	Policy (Software Acquisition Pathway Policy)	6 Metrics Plan DevSecOps	Technical
69	Policy (Software Acquisition Pathway Policy)	5 Enterprise Services DevSecOps (Lines 220-236)	Technical
70	Policy (Software Acquisition Pathway Policy)	Planning Phase, Cost Estimates, line 161	Technical
72	Policy (Software Acquisition Pathway Policy)	Global	General
73	Guidance (Business Decision Guidance)	6. Metrics Plan	Technical
74	Policy (Software Acquisition Pathway Policy)	Global	Technical
75	Guidance (Business Decision Guidance)	Section 8, Continuous ATO	General

76	Policy (Software Acquisition Pathway Policy)	Roles and Responsibilities	Technical
77			
78			
79			
80			
81			
82			
83			
84			
85			
86			
87			
88			
89			
90			
91			
92			
93			
94			
95			
96			
97			
98			
99			
100			

END

Impact	Comment Provided By (Individual or Org)
VH	NDIA (multiple inputs)
VH	NDIA (multiple inputs)
VH	NDIA System Security Engineering Committee
H	NDIA System Security Engineering Committee
H	NDIA System Security Engineering Committee
H	NDIA (multiple inputs)
VH	NDIA (multiple inputs)
H	NDIA (multiple inputs)
L	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
L	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
H	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco

L	Individual - Aleksandra Scalco
L	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
L	Individual - Aleksandra Scalco
H	Individual - Aleksandra Scalco
VH	Individual - Aleksandra Scalco
VH	Individual - Aleksandra Scalco
VH	Individual - Aleksandra Scalco
VH	Individual - Aleksandra Scalco
VH	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
L	Individual - Aleksandra Scalco
M	Individual - Aleksandra Scalco
M	Individual input to NDIA
M	Individual input to NDIA

VH	Individual input to NDIA
M	Individual input to NDIA
H	Individual input to NDIA
H	Individual input to NDIA
M	Individual input to NDIA
M	Individual input to NDIA
M	Individual input to NDIA
M	Individual input to NDIA
M	Individual input to NDIA

M	Individual input to NDIA
H	Individual input to NDIA
H	L3Harris (Security)
VH	L3Harris (Security)
VH	L3Harris (Security)
VH	L3Harris (Security)
H	L3Harris (Security)

H	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
M	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
VH	L3Harris (Security)

H	L3Harris (Security)
H	L3Harris (Security)
M	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
M	L3Harris (Security)
H	L3Harris (Security)
M	L3Harris (Security)
M	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)
H	L3Harris (Security)

M	Boeing
M	Boeing
M	L3Harris
L	Individual - Ron Carson
H	Individual - Ron Carson
M	NDIA System Security Engineering Committee
L	NDIA System Security Engineering Committee

M	NDIA System Security Engineering Committee

Comment and rationale
Generally favorable industry feedback on A&S SW policy and guidance. Support DoD intent and direction. Like the addition of MVCR.
Strong consensus from many sources that the policy and guidance must be part of the overall SE process. Also not clear how (or if) SW integrates with digital engineering intiatives, M&S, MBSE.
Like the objective and direction overall, but this MUST be integrated with Systems Engineering - "the policy and guidance are not usable until integrated with SE."
For a DevSecOps approach to be successful, security concerns must be integrated and addressed as part of the engineering process throughout all activities (concept, roadmap, requirements, design, test, etc.). This is alluded to in some places ((d), buried in the Execution Phase (continuous ATO)) but not sufficient. Need to emphasize the 'Sec' as an integrated and essential element in DevSecOps throughout the pipeline
Continuous ATO is crucial to improving speed of SW delivery, but is not the primary security objective - delivering a secure and resilient system is. The breadth of security objectives, constraints, and application level cybersecurity is not adequately covered.
Generally like the MVCR concept, positive idea. But terms differ from widely used MVP terminology.
Set of 'minimum set of metrics' is far too extensive, and exceeds recommended practice (e.g., DSB, DIB SWAP, PSM, NDIA, 'Accelerate', DORA reports, Kessel Run), with no linkage to business needs, objectives, or how the data will be analyzed and used to drive business decisions. In other areas, the SW policy recommends simplicity, flexibility, and 'tailoring up' but for metrics the recommendations are heavyweight, burdensome, and inconsistent with current industry best practices. Even automated metrics have a cost in collection, analysis, reporting.
Applicability to primarily SW and COTS HW is too limiting and not representative of the majority of DOD systems that align with custom SW and custom HW.
Comprehension
Add subparagraphs for clarity and identification
Clarity
Style consistency - spell out acronyms
Style consistency - formatting, bullets, italics, numbering
Requirement clarity use of "properly" and "sufficient" are too vague (example line 403)
Section 3.1 Roles is it the PM or the Program Office?

Section 3.1 provide definititions
Section 3.1 clarity of roles and responsibilities
Section 3.1 clarify what tailored means
single v double space after sentence period
Section 4. Suitable and appropriate are subjective terms
Section 4. Not clear if this document is about Agile
Section 4. DevSecOps new concept introduction
Section 4 should / shall / acquisition rules clarity
line 211 clarity regarding government access to source code
Line 250 features shall (clarity) also line 411 and in other places
Figure needs caption
Line 269 states DevSecOps not beneficial for all programs and the next bullet states a DevSecOps SLA is formalized
Line 275 provide additonal information about artifact repository
Line 521 states "ensure all members … Agile team are trained"
Line 533 states ensure leadership support on the plan for Agile
Main purposes / overarching (line 553)
Line 652 proposed implementation of control
The policy reads more like guidance than policy. Policy needs to have “shall” statements, not should.
Applicability/Scope is subjective; it does not address what programs/project the policy does not apply to, grandfathering. Not clear the extent of application to weapon and safety critical systems. Not clear the extent this will be applied to existing systems, or whether existing policy will be grandfathered on those systems.

Safety is not addressed in this policy. It is not clear how this applies to safety-critical systems and the implications for safety. Most DOD systems have safety critical components. This is a key factor that must be addressed.
Policy discuses roadmap, capability needs statement, user agreement, acquisition strategy, etc. These are very different than current documents in use, but teams do not have experience with these documents. A few brief summary of a few key points is provided in the business decision guidance, but need more information including the material to be covered and perhaps a good example or two for different types of systems.
The whole Materiel Release process has to be modified to support agile; are these compatible? There are problems/challenges with having a continuous Authority to Operate (ATO) – these need to be addressed.
Policy says that DT/OT shall be streamlined, automated, and integrated. How does that happen? Availability of test facilities and proving grounds is always an issue.
Automated testing is nice, but 100% is not achievable in complex interoperating systems. Cost to automate testing for existing systems is very high. Changes to infrastructure for existing systems may not always be cost effective.
Policy is dependent upon continuous feedback from the warfighter/end-user; we do not always have access to them, they are not always available when needed, or with the right expertise. Some support multiple systems.
Secure cloud not yet available. Would be useful, but can't count on it before it becomes available.
Roadmap does not address architecture and design; will it really evolve? Will it address safety critical applications?
The end users of many DoD systems are in a vast variety of environments – both online and offline. If there is a drive to push continuous delivery through a slow delivery network (electrical and physical), this could result in a significant configuration management risk.

Contractors/vendors may not have the ability to implement the requirements of this policy, such as CI/CT/CD and metrics reporting. The DoD does not currently have the ability to prescribe these development process capabilities. Will the DoD be able to ensure this policy is upheld by contractors/vendors?
During the contractor/vendor initial request and negotiation process, what document from the policy (e.g. CNS?) should be used to properly generate cost and effort estimates? The processes mentioned in the policy do not typically contain a requirements document.
the user shall establish a CNS and UA to capture a commitment between the PM spftware teams and the end user, and are used in lieu of a rigid requirements process, Unfortunately, there is no mention of the Authorizing Authority or the Security organization in this agreement. It assumes the user can articulate the Security Organization's processes and/or requirments.
The Program Manager shall leverage enterprise services by adapting existing services, buying COTS, or creating new services. As written, this statement inserts the PM into the implementation specification and dictates the platform to the contractor or coding organizxation,. At a minimum, this levels the playing field for all competing entities in that there is no room for creativity. Each competitor would be provided the same enterprise services as GFE, or a specification of the expected environment would be available as part of the CNS,.
The MVP is an early iteration of a software product with just enough features to meet the basic minimum functional capabilities…. To quickly get basic capabiities into the user's hands for evaluation, feedback, and improvemen ts. It should be noted that a Minimum Essential Set of Security Requirements shsould be incorporated into the MVP to ensure a secure baseline that the Approval Authority can authorize for use is delivered.
The MVCR is a small set of features that provides value and capability…. The PM and the Warfighter will determine when the MVCR and subsequent releases will be released operationally. Again, the Security Organization/Approval Authority of the security organixation is left out of the equation. As the Approval Authority determines if the MVCR would pose a risk to the user/warfighter, this entity needs to be part of the operational releaase decision.
The Product Roadmap discussion also needs to incorporate security requirements.

Adding one sentence about security being a life cycle requirement is not enough,. It needs to be a discrete capability and th Approving Authority must be involved from creation of the CNS and the UA.
No mention of Security Testing is included in the test phases..
No mention of security Metrics or Vulnerabilies Detected/Prevented.
Conducting value assessments annually to measure the operational impact of the software should also include the impact of the systems's security posture (or lack thereof)
Services/PEOs shall formally tailor… again, no mention of integration of security functions or deiverables consistent with cost, schedule, and delivery objectives.,
Active engagement with the users is required to understand their conops, environment, threats, capabiities and needs. Unfortunately, most users have zero knowledge of their threat enviromment, or over-specify their security requirements because they do not understand the concept of risk acceptance and are afraid to ask the Security Organization for assistance
See comment 11 -- the end user does not understand the security threat environment and should be encouraged to seek guidance from the Approval Authority
User agreement calls for commitment to continuous involvemenet. This also needs the continuous involvement of the security organization if the PEO expects to receive ana Authorization to Operate.
The goal of the acquisition strategy is to document a feasible approach to obtaining the capabilities and aligning to agile principles to develop quality software. No mention of security or said software or the system. How does this play into the Program Protection Plan and the Program Protection Implementation Plan? Again, security involvement needs to be explilcit.
Cost Elements need to include security as well. If we expect to build security into the system, it needs to be accounted for.
This section focuses on "active user engagement", yet barely mentions engagement of security personnel to ensure delivered caspabilities match the risk appetite of the Approval Authority
Secure Software Development and Continuous ATO is called out separately from the other artififacts as if this plan and its process are unique and separate from the other documents. This cannot be the case if a true continuous integration model is expected.

No discussion of how continuous delivery will address the operational environment of deployment. Not all systems that are deployed can be updated at the same time, accommodation of different versions, etc.
CNS captures the operational capabilities to accomplish the mission and combat threats from adversaries. Most users do not understand the cyber threats from adversaries, yet we expect them to articulate the needs for protection.
The section explicitly calls out capability gaps and risks to accomplish the mission -- should it also discuss acceptable risk relative to authorization to operate?
The user organization needs to know where to go to collect an accurate threat summary and to determine effectivce countermeasures.
The User agreement needs to include expectations of the Approval Authority and the cadence and interactions that are expected.
None of the roles and responsibilities have security as a component.
In the discussion of feature identification, there is no mention of security features/requirements, which must be in place at various phases in the roadmap to achieve an ATO.,
Again, the acquisition strategy talks in very general terms and constraints w3ith no mention of security requirements or controls
"Cost estimates are based on the total cost of all of the features implemented in a given release." Please note, that also includes the cost of security features and/or the cost of security assurance.
Need to incorporate just the cost of Enterprise Software and Computing costs, but also the cost of Security Tools such as HBSS
Not everything benefits from DevSecOps -- document the decision. There is no discussion of how the decision is made or who concurs on the document.
Note the first line "security should be everywhere" But instead of incorporating it throughout this document, it gets less than a half page paragraph that says "put it everywhere."
A good section, but it comes too late to have a significant impact on the reader. It needs to be sprinkled throughout the phases and the document, not buried in "Section 8" -- was that really a coincidence?

While a min set of metrics is a good practical start, there is a body of knowledge of a greater set and it is not provided in the guidance. That BOK should be provided for expanding the metrics for each project as required
Missing a few key security activities
"The cost estimate must account for the long term value of the software…." Cost estimates and long term value should consider sustainment costs.
My overall impression is that this new policy seems to be a vehicle for avoiding DODI 5000.02. And without clear "measures of success" I think we're going back to "spiral development" (DODI 5000.2, circa 2003) with no objective end point.
I also think the long list of metrics without connection to stakeholder information needs will make these programs more expensive than is necessary.
Approach for supplier software is not clear. Large acquisitions typically have large supply chains.
Continuous ATO is a good concept, but may not be realistic

Concerns with the Policy not defining the ownership of the ATO; Program Office or User Community such as Air Combat Command.

		For Editor Only
Recommendation	**Keyword**	**Disposition**
None - positive feedback overall, with a few areas of concern summarized separately.	**General**	
Add Systems Engineering as a critical required element of the SW DevSecOps process, and for coordination of cross-functional stakeholders (requirements, security, SW, …)	**SE**	
Add Systems Engineering as an explicit function required for implementation of the SW policy and guidance, and integrate throughout as needed.	**SE**	
Emphasize and integrate Security considerations across all engineering activities (planning, roadmap, design, development, test, operations) not just ATO. Put the 'Sec' throughout the DevSecOps pipeline. Failure to do so can put not only ATO but the system security posture at risk.	**Security**	
Add emphasis on primary security objectives and how to achieve them in an approach integrated with design, development, and test across the software life cycle.	**Security**	
Review MVP terminology and consider impacts and confusion that may result from adoptiong non-standard definitions.	**Terminology**	
Simplify and reduce metrics set. Leverage industry practice and studies. Conduct a single subject meeting with industry to evaluate what metrics are used in practice effectively. Emphasize a framework (PSM) based on information needs with a small set of measures, supplemented with additional measures based on program-specific needs.	**Metrics**	
Apply the SW policy concepts across other domains including custom HW. Realizing the benefits of the SW approach cannot be obtained without including SE and custom HW.	**Scope**	
Add Table of Contents	Editorial	
See markup for suggestions	Editorial	
Add an Overview of the purpose of the document	Editorial	
1st reference of abbreviation spell out, subsequent abbreviate	Editorial	
Consistent formatting (use of bullets, italics, bold and numbering)	Editorial	
Provide detailed definition of what "proper" is	Clarity	
Consistency	Editorial	

what is a "cooperative" s/w development program	Definitions	
clarify PM/Program Office and Acquisiton role	Definitions	
provide definitions	Definitions	
consistency throughout document	Editorial	
provide clarity of what makes s/w suitable or appropriate	Clarity	
Define Agile and clarify if this is a shall requirement or a best practice approach. If this document is proposing following Agile then say so in an overview up front.	Clarity	
Define newly introduced concepts/methods	Definitions	
provide reference to DoD acquisition rules (link to Dau website regarding commercial v. government purchase rules).	Acquisition	
add more information here about the need for govt. access to source code and how that is managed	Acquisition	
throughout document clarity of shall v should	Clarity	
add caption	Editorial	
Clarify if DevSec Ops is an option then it is just a SLA (not necessarily DevSecOps SLA)	Clarity	
add references to existing guidance	Definitions	
If this is a requirement state so, if it is guidance same, to what level and where provide references	Clarity	
state this up front in the document if this is proposing to follow Agile	Editorial	
reference in summary up front	Editorial	
add DoDCAR information	Definitions	
Change “should” to “shall” where appropriate to identify mandatory obligations	Clarity	
Clearly address Applicability/Scope.	Scope	

Address safety and safety-critical systems in the policy, notably MIL-STD-882E and Joint Software Systems Safety Engineering Handbook.	Safety	
Provide information on documents to be developed including the material to be covered and perhaps a good example or two for different types of systems.	Transition	
Address material release process and continuous ATO.	Security	
Much work and authority has to occur to make this happen. Needs high-level involvement and coordination.	Test	
Address realities that not all systems will be 100% automated. Address older systems and infrastructure – any changes required? What are the decision factors in those cases?	Test	
Address user/SME availability in policy.	Users	
Options to secure cloud?	Security	
Address how architecture and design evolves over time. Address how safety critical factors are designed into the system from the beginning in an iterative development.	Architecture	
Review current delivery and deployment capabilities. Determine effort and changes required to meet continuous delivery capability and impact on policy.	Environment	

Review development capabilities requirements and DoD role in enforcement.	Acquisition	
Determine the method by which the DoD can approach prospective contractors/vendors with data suitable to make an informed estimated proposal.	Acquisition	
Explicitly add the Approval Authority or representative of the security organization to the creation of the UA and CNS. Otherwise, there is likely to be a miscommunication of the security requirements for the system that will result in program cost and schedule delays later.	Security	
Kindly define "Enterprise Services" in the context of this policy. If the intent is to use platforms, clouds, or containers that are already available via IDIQ or schedule contracts, so state. If the intent is to use common, standard platforms for the User Organization,so state. As written, the term "enterprise services" is ambiguous and confusing.	Clarity	
Add words into the MVP definition to include a minimum set of security requirements that will be delivered with the MVP.	Security	
Add text to include the Authorizing Authority in the release of the MVCR for operational use.	Security	
Ensure the Approval Authority Security Organization is involved in the Product Roadmap process to maintain a continous authorization to operate over the life of the system.	Security	

If security participation is added into bullets A-D, and not addressed as a single sentence in D, and participation of the Security Organization is incorporated, it would suffice. Note also that Secure Development, Secure Capabiilties, and Secure Life Cycle are not mentioned previously in this document. an may have to be defined,.	Security	
Explictly call out Authorization and Approval testing in this discussion of streamlined, automated, and intgrated test activities.	Security	
Add security metrics into metrics collectio process. As written, it appears to be a list that justifies rapid, iterative development	Security	
Include security in the continual engagement process and value assessments to accurately reflect the security posture of the operational system at all times.	Security	
Need to incorpate security into this tailoring process and to the overall process. It is sorely missing from these descriptions, which will put the Program at risk of not achieving an authorization to operate.	Security	
Explicity incorporate the security organization's participation in the Planning Phase.	Security	
Incorporate the Security Organization into the formulation of the CNS.	Security	
Incorporate involvement of the Security Organization into the User Agreement.	Security	
Iincocproate the security organization as a stakeholder in this proccss,.	Security	
Add a cost element for security, especially over the system life system to address the long term value of secure platforms and secure software,.	Security	
Incorporate the Security Organization into the Execution Phae as a stakeholder.	Security	
Instead of calling out a one paragraph security reference, integrate participation of security personnel in the plans aned phases covered throughout the document.	Security	

In the discussion of continuous operational delivery there also needs to be a discussion of how security will be addressed when all systems cannot be upgraded This is the question of addressing multiple versions and maintenance of these "obsolete" capabilities.	Security	
Suggest explicit discussion of cyber threats and/.or integrationj of appropraite sescurity organizations into the CNS process.	Security	
Add words about "acceptable security risk" within the operational context. For example, an early delivery cycle may have an unacceptable security posture that is corrected within N iterations or that depended on capabiities that were delivered late	Security	
Add words about threats and how the developed system will counter them.	Security	
Add the security organization as a stakeholder in the user agreement.	Security	
Either add a security sponsor role, or designate it as the responsibility of one of the existing roles.	Security	
Explicity add security activities or functions into the feature identification and prioritization discussion as well as the testing and deployment/rollout decisions.	Security	
Incorporate security activities/milestones, such as defining the objective security state at various phases of the program.	Security	
Make the incorporation of security features explicit.	Security	
Elaborate on licensing costs and determination of items that are provided as GFE. For example, what happens if GFE mission functionality does not work in the target security environment..	Security	
Examples of systems that do not benefit would be useful.	Scope	
Again, security needs to be integrated, and the only way for that to happen will be to decompose this section and put it in all of the sections that talk about requirements, metrics, etc.	Security	
Again, capturing security in one section is asking for it to be ignored. It needs to be integrated to be useful.	Security	

provided the following metrics. Availability: Amount of uptime/downtime in a given time period, in accordance with the SLA. Change Failure: Percentage of production deployments that failed. Change Lead Time: Time between a code commit and production deployment of that code. Change Volume: Number of user stories deployed in a given time frame. Customer Issue Resolution Time: Mean time to resolve a customer-reported issue. Customer Issue Volume: Number of issues reported by customers in a given time period. Defect Burn Rate: Amount of time to fix vulnerabilities in an application. Defect Density: The number of bugs identified divided by the codebase of an application. Deployment Frequency; Number of deployments to production in a given time frame. Logging Availability: Amount of uptime/downtime of the logging pipeline in a given time period. Mean Time Between Failures (MTBF): The amount of time that elapses between one failure and the next. Mathematically, this is the sum of MTTF and MTTR, the total time required for a device to fail and that failure to be repaired. Mean Time to Failure (MTTF): Time that a system is online between outages or failures. Mean Time to Recovery (MTTR): Time between a failed production deployment to full restoration	Metrics	
Add threat analysis of the sw architecture and code to determine weaknesses and attack surface (MS STRIDE for example). Include secure coding standards… Acceptance/standards of third party code into the project	Security	
Add "…and sustainment" to cost estimate description.	Estimation	
None	General	
Align metrics set with stakeholder information needs. Clarify linkage of metrics to objectives and actions.	Metrics	
Clarify approach for suppliers and supply chain.	Supply Chain	
Consider additional potential sources supporting continuous, such as NIST Continuous Software Framework.	Security	

	Security	

Notes