DoD Draft Software Acquisition Pathway Policy and Guidance

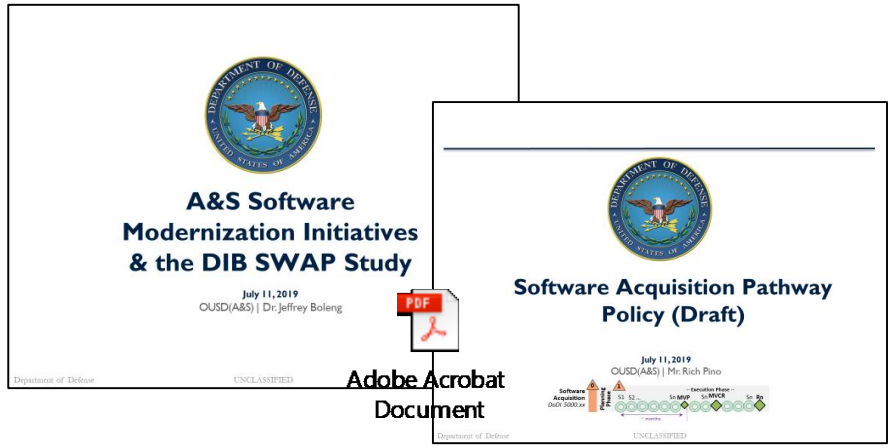
NDIA SE Division

Industry Review Feedback

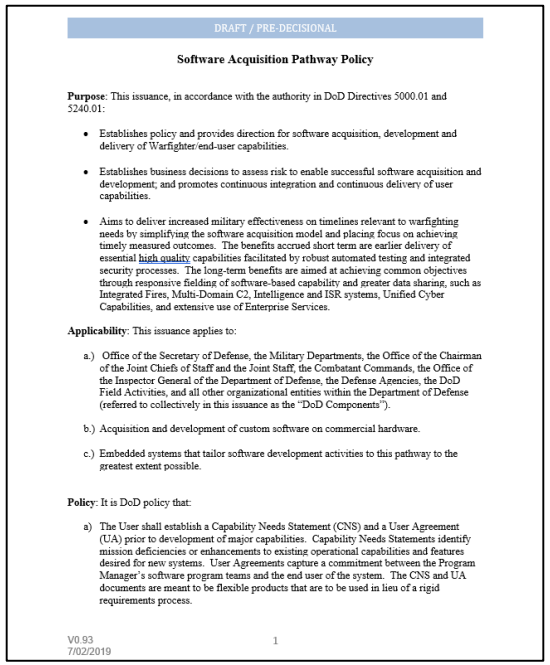
August 8, 2019

DoD Software Acquisition Pathway (Draft)

- **OUSD (A&S) is seeking industry feedback on draft (1) Software Acquisition Pathway Policy and (2) Business Decision Guidance. (aka "Software 5000.02")**
- **Cross-divisional NDIA review kickoff held at NDIA HQ (7/11/19)**
  - Systems Engineering; ADAPT; Integrated Program Management; Cyber
- **Industry comments widely solicited (various means) thru 8/2/19**



Microsoft Word Document



DRAFT / PRE-DECISIONAL

Software Acquisition Pathway Policy

Purpose: This issuance, in accordance with the authority in DoD Directives 5000.01 and 5240.01:

- Establishes policy and provides direction for software acquisition, development and delivery of Warfighter/end-user capabilities.
- Establishes business decisions to assess risk to enable successful software acquisition and development; and promotes continuous integration and continuous delivery of user capabilities.
- Aims to deliver increased military effectiveness on timelines relevant to warfighting needs by simplifying the software acquisition model and placing focus on achieving timely measured outcomes. The benefits accrued short term are earlier delivery of essential high quality capabilities facilitated by robust automated testing and integrated security processes. The long-term benefits are aimed at achieving common objectives through responsive fielding of software-based capability and greater data sharing, such as Integrated Fires, Multi-Domain C2, Intelligence and ISR systems, Unified Cyber Capabilities, and extensive use of Enterprise Services.

Applicability: This issuance applies to:

a.) Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (referred to collectively in this issuance as the "DoD Components").

b.) Acquisition and development of custom software on commercial hardware.

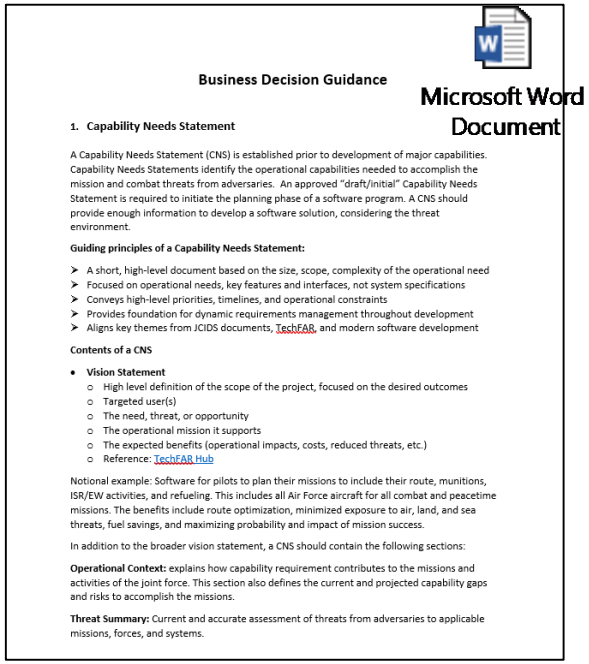
c.) Embedded systems that tailor software development activities to this pathway to the greatest extent possible.

Policy: It is DoD policy that:

a) The User shall establish a Capability Needs Statement (CNS) and a User Agreement (UA) prior to development of major capabilities. Capability Needs Statements identify mission deficiencies or enhancements to existing operational capabilities and features desired for new systems. User Agreements capture a commitment between the Program Manager's software program teams and the end user of the system. The CNS and UA documents are meant to be flexible products that are to be used in lieu of a rigid requirements process.

V0.93
7/02/2019
1

Microsoft Word Document



Business Decision Guidance

1. Capability Needs Statement

A Capability Needs Statement (CNS) is established prior to development of major capabilities. Capability Needs Statements identify the operational capabilities needed to accomplish the mission and combat threats from adversaries. An approved "draft/initial" Capability Needs Statement is required to initiate the planning phase of a software program. A CNS should provide enough information to develop a software solution, considering the threat environment.

Guiding principles of a Capability Needs Statement:

- A short, high-level document based on the size, scope, complexity of the operational need
- Focused on operational needs, key features and interfaces, not system specifications
- Conveys high-level priorities, timelines, and operational constraints
- Provides foundation for dynamic requirements management throughout development
- Aligns key themes from JCIDS documents, TechFAR, and modern software development

Contents of a CNS

- **Vision Statement**
  - High level definition of the scope of the project, focused on the desired outcomes
  - Targeted user(s)
  - The need, threat, or opportunity
  - The operational mission it supports
  - The expected benefits (operational impacts, costs, reduced threats, etc.)
  - Reference: TechFAR Hub

Notional example: Software for pilots to plan their missions to include their route, munitions, ISR/EW activities, and refueling. This includes all Air Force aircraft for all combat and peacetime missions. The benefits include route optimization, minimized exposure to air, land, and sea threats, fuel savings, and maximizing probability and impact of mission success.

In addition to the broader vision statement, a CNS should contain the following sections:

Operational Context: explains how capability requirement contributes to the missions and activities of the joint force. This section also defines the current and projected capability gaps and risks to accomplish the missions.

Threat Summary: Current and accurate assessment of threats from adversaries to applicable missions, forces, and systems.

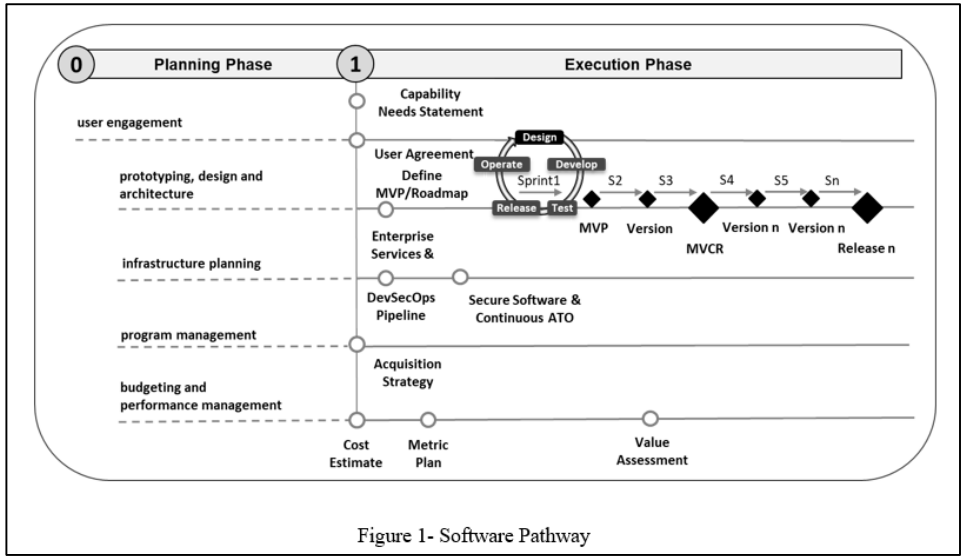


Figure 1- Software Pathway

Broad solicitation for industry inputs
(written comments, informal comments, verbal discussion/feedback)

- **NDIA**
  - Systems Engineering Division
    - Committees
    - Industry steering committee (company reps)
  - ADAPT
  - Cyber Division
  - Integrated Program Management Division
- **Company-internal**
  - Lockheed Martin, Northrop Grumman, Raytheon, L3Harris, …
  - Cross-functional (Engineering, Software, Agile/DevOps SMEs)
- **INCOSE WGs (IS2019)**
  - Agile and SE WG; SSE WG; Measurement WG
- **Inputs from individuals**

Substantial consensus across industry organizations and stakeholder groups led to a consolidated response to A&S review request

Summary Level Industry Feedback

Generally very favorable industry feedback on A&S SW policy and guidance. Support DoD intent and direction.
A few areas of concern: SE; Security; Metrics.

General	Key Inputs
• Positive overall concepts, approach, direction • Like Minimally Viable Capability Release (MVCR) concept • …but some terms differing from common industry usage (e.g., MVP) can be confusing for adoption)	• Very strong industry consensus that integration with Systems Engineering must be included • Scope should also apply to custom SW on custom HW /embedded to the extent practical (leverage benefits broadly; few programs are pure SW/COTS) • Strengthen Security integration with Engineering across all aspects of life cycle (DevSecOps) – concept, roadmap, architecture, design, development, test, delivery, … • Security objective is much broader than continuous ATO ► secure, resilient cyber systems – must be designed in • Over-achieved significantly on SW metrics – well beyond prior input recommendations (DSB, DIB SWAP, PSM, NDIA, …) and industry practice. Lack linkage to information needs, actions.

Substantial consensus on these inputs across industry (companies, stakeholder groups)
Many details provided in consolidated commenting spreadsheet and other attachments.

Summary of written inputs in commenting spreadsheet

(NDIA SE Division - as of 8/2/19)

Category	L	M	H	VH	Grand Total
Editorial	1	5			6
General	7	9	4		20
Technical		16	27	14	57
Grand Total	**8**	**30**	**31**	**14**	**83**

Comment Provided By(Individual or Org)	(All)

Count of Impact		In				
Product (Selection)	**Category**	**L**	**M**	**H**	**VH**	**Grand Total**
Policy (Software Acquisition Pathway Policy)	General	1	4	4		9
	Technical		11	16	8	35
Policy (Software Acquisition Pathway Policy) Total		**1**	**15**	**20**	**8**	**44**
Guidance (Business Decision Guidance)	Editorial	1	5			6
	General	6	5			11
	Technical		5	11	6	22
Guidance (Business Decision Guidance) Total		**7**	**15**	**11**	**6**	**39**
Grand Total		**8**	**30**	**31**	**14**	**83**

Summary of written spreadsheet inputs only.
Does not include comments received from other sources (verbal, informal).

Comment Provided By(Inc	(All)

Count of Impact		Impact				
Product (Selection)	**Keyword**	**L**	**M**	**H**	**VH**	**Grand Total**
Policy (Software Acquis	Acquisition		1	1		2
	Architecture		1			1
	Clarity		1		1	2
	Environment		1			1
	Estimation		1			1
	General	1			1	2
	Metrics		1			1
	Safety				1	1
	Scope		1	1		2
	SE				2	2
	Security		4	16	3	23
	Supply Chain		1			1
	Terminology			1		1
	Test		1	1		2
	Transition		1			1
	Users		1			1
Policy (Software Acquisition Pathway Policy) T		**1**	**15**	**20**	**8**	**44**
Guidance (Business Dec	Acquisition				2	2
	Clarity		2	2	2	6
	Definitions	2	3		1	6
	Editorial	4	6			10
	Metrics			1	1	2
	Scope			1		1
	Security	1	4	7		12
Guidance (Business Decision Guidance) Total		**7**	**15**	**11**	**6**	**39**
Grand Total		**8**	**30**	**31**	**14**	**83**

Keywords assigned by NDIA for affinity grouping of topic areas

Extensive participation, discussion, and feedback from System Security Engineering (SSE) Committee (thank you, Holly and Cory!)

Key Take-aways:

- Security is framed in a way of compliance; to reach Approval to Operate is not to reach a secure system.
- The focus on DevSecOps will contribute significantly to the concept of continuous ATO, but the document omits the need for Application level cybersecurity.
- As many of our products are systems of systems, a holistic appreciation of all security specializations (Cyber, IA, AT, SSE, SwA, SCRM) is necessary; Compliance to RMF Controls only buys a minimum level of assurance and doesn't adequately cover the security specialties in an integrated risk managed trade space.
- Importance of MVCR security requires elevation, fielding a 'minimum' introduces environmental, intended use, and configuration control concerns. A greater definition of a sustainment support community is necessary.
- The push to 'leverage enterprise services' and the level of interaction with the test strategy seems to ignore embedded systems.
- With the shift from monolithic requirements to more agile methodology, cost estimation will be a problem. The top recommendation cited to improve cost estimates is to "define the team size and makeup", which is great for defining how much will be spent but a poor way to determine how much the work should cost. This also assumes a dedicated workforce with the right skills are available. This may work for top priority programs but will be challenging to scale to all programs with the gap in talent.
- While the idea of user testing of an MVP allows for flexibility in terms of capability and design, security is best designed into the architecture from the onset, major revisions may lead to vulnerabilities.
- The flexibility of CNS/UA/MVP is an exciting prospect, but firm high-level requirements are necessary to drive core architecture.
- The document fails to capture the need for systems-level thinking and the involvement of systems engineers and architects.
- Lessons learned include the short story incremental development and review cycles are good but the traditional major reviews are still needed to ensure the big picture isn't lost while focusing on detailed iterative developments.

- **Many additional detailed security-related comments provided in attached notes and commenting spreadsheet**

Microsoft Word Document

Next Steps

- **Integrate written inputs from ADAPT and other NDIA divisions**
- **Review industry inputs with NDIA SE Division for consensus**
- **Submit inputs to OUSD A&S**
- **Request a collaborative meeting with OUSD A&S to discuss industry input**
  - Follow-up from NDIA HQ kickoff and OUSD A&S request