NPS-AM-10-038

EXCERPT FROM THE

PROCEEDINGS

OF THE

SEVENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM WEDNESDAY SESSIONS VOLUME I

Acquisition Research

Creating Synergy for Informed Change

May 12 - 13, 2010

Published: 30 April 2010

Prepared for: Naval Postgraduate School, Monterey, California 93943

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Test and Evaluation at the Speed of Need	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Information Systems Agency,Arlington,VA,22204**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
7th Annual Acquisition Research Symposium to be held May 12-13, 2010 in Monterey, California.

14. ABSTRACT

During this past year, Congress passed the Weapons Systems Acquisition Reform Act, which made several changes to DoD acquisition organizations and processes. More recently, Congress passed, and the President signed, the National Defense Authorization Act for FY2010, becoming Public Law 111-84, directing changes in DoD acquisition of information technologies (IT). The law requires the DoD to base the new acquisition process on recommendations in the March 2009 Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology (hereafter DSB-IT). The report recommends an agile model for acquiring information technologies (IT) similar to successful commercial practices (see http://www.acq.osd.mil/dsb/reports.htm). A second DSB report, also issued in March 2009 the Report of the Defense Science Board Task Force on Achieving Interoperability in a Net Centric Environment (DSB-NC), made recommendations to ensure that IT acquisition delivers information-assured, interoperable capabilities essential to modern warfighting. Together, the reports provide a foundation on which to build the new model for acquisition and testing of IT; this paper attempts to connect them and fill the remaining gaps necessary to truly transform to agile processes that foster rapid acquisition of enhanced IT capabilities for the warfighter

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**31**	

The research presented at the symposium was supported by the Acquisition Chair of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request Defense Acquisition Research or to become a research sponsor, please contact:

NPS Acquisition Research Program
Attn: James B. Greene, RADM, USN, (Ret.)
Acquisition Chair
Graduate School of Business and Public Policy
Naval Postgraduate School
555 Dyer Road, Room 332
Monterey, CA 93943-5103
Tel: (831) 656-2092
Fax: (831) 656-2253
E-mail: jbgreene@nps.edu

Copies of the Acquisition Sponsored Research Reports may be printed from our website www.acquisitionresearch.net

Test and Evaluation at the Speed of Need

Steven J. Hutchison—Dr. Steven J. Hutchison assumed duties as Test and Evaluation Executive, Defense Information Systems Agency in August 2005. Dr. Hutchison supervises the Joint Interoperability Test Command, T&E Management Center, and the IT testbed in the Major Range and Test Facility Base.

Dr. Hutchison previously served with the Director, Operational Test and Evaluation and Army Test and Evaluation Command. Dr. Hutchison retired from the US Army in 2002.

Dr. Hutchison earned a PhD in Industrial Engineering at Purdue University, an MS in Operations Research at the Naval Postgraduate School, and is a 1982 graduate of the United States Military Academy.

Abstract

During this past year, Congress passed the *Weapons Systems Acquisition Reform Act*, which made several changes to DoD acquisition organizations and processes. More recently, Congress passed, and the President signed, the *National Defense Authorization Act for FY2010*, becoming Public Law 111-84, directing changes in DoD acquisition of *information technologies* (IT). The law requires the DoD to base the new acquisition process on recommendations in the March 2009 *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology* (hereafter *DSB-IT*). The report recommends an agile model for acquiring information technologies (IT) similar to successful commercial practices (see http://www.acq.osd.mil/dsb/reports.htm). A second *DSB* report, also issued in March 2009, the *Report of the Defense Science Board Task Force on Achieving Interoperability in a Net Centric Environment* (*DSB-NC*), made recommendations to ensure that IT acquisition delivers information-assured, interoperable capabilities essential to modern warfighting. Together, the reports provide a foundation on which to build the new model for acquisition and testing of IT; this paper attempts to connect them and fill the remaining gaps necessary to truly transform to agile processes that foster rapid acquisition of enhanced IT capabilities for the warfighter.

Test and Evaluation at the Speed of Need

Department of Defense acquisition is always under the watchful eye of the Congress. During this past year, Congress passed the *Weapons Systems Acquisition Reform Act*, which made several changes to DoD acquisition organizations and processes. More recently, Congress passed, and the President signed, the *National Defense Authorization Act for FY2010*, becoming Public Law 111-84, directing long overdue changes in DoD acquisition of *information technologies* (IT). According to section 804, "The Secretary of Defense shall develop and implement a new acquisition process for information technology systems." The law requires the DoD to base the new acquisition process on recommendations in the March 2009 *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology* (hereafter *DSB-IT*). The report recommends an agile model for acquiring information technologies (IT) similar to successful commercial practices (see http://www.acq.osd.mil/dsb/reports.htm). Interestingly, a second *DSB* report, also issued in March 2009, the *Report of the Defense Science Board Task Force on Achieving*

Interoperability in a Net Centric Environment (DSB-NC), made recommendations to ensure that IT acquisition delivers information-assured, interoperable capabilities essential to modern warfighting. Together, the two reports should be used as the foundation on which to build the new model for acquisition and testing of IT; this paper attempts to connect them and fill the remaining gaps necessary to truly transform to agile processes that foster rapid acquisition of enhanced IT capabilities for the warfighter.

Acquisition and Testing of Information Technologies in the DoD

The DoD acquires IT using the same acquisition model as tanks and ships and planes. Figure 1 is the familiar Defense Acquisition Management System taken from *DoD Instruction 5000.02*. This system essentially makes no distinction between major defense acquisition programs (MDAP) and major automated information systems (MAIS); program managers for IT capabilities manage the same set of milestones and decision points and are subject to the same governance processes and oversight. Make no mistake; this system has produced the best military equipment in the world, but in recognizing this fact, it is important to realize that the process works well when there is a looooooooooong time between user need definition (far left of chart) and declaration of Initial Operational Capability (IOC) (subsequent to the final decision point on the chart). Therein lies the problem for IT: the fundamental reason this model does not work well for IT capabilities is that we typically want a very short time between user need definition and IOC.

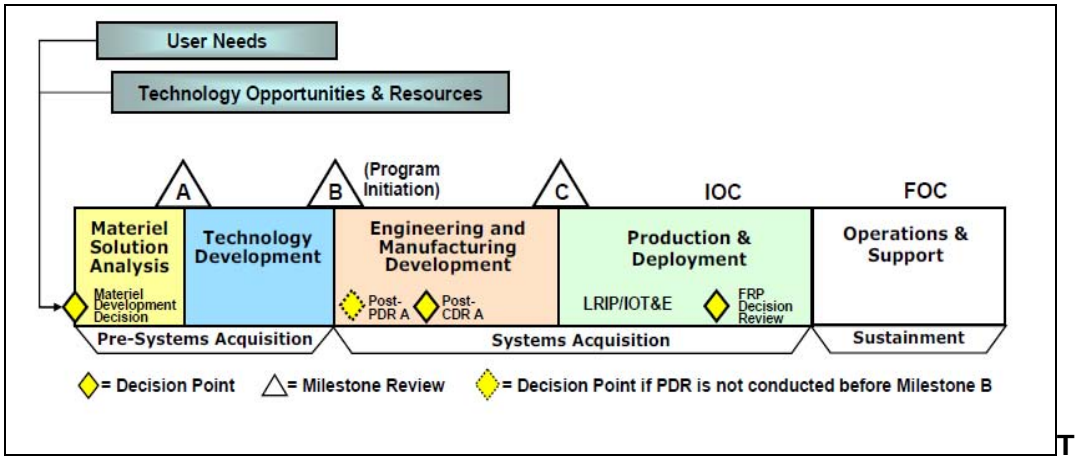


Figure 1. The Defense Acquisition Management System

The *DSB-IT* describes the current DoD IT acquisition process as a "big bang approach," meaning we try to get everything in the first increment. The report describes the approach as one that "begins with an analysis phase followed by an equally long development phase that culminates in a single test and evaluation event." The *DSB-IT* cited an analysis conducted by the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) of 32 major automated information systems, which showed that the average time to deliver an initial capability is 91 months! Figure 2, taken from the *DSB-IT* report, summarizes the length of time spent in each phase of the acquisition system, according to the ASD(NII) analysis. The *DSB-IT* concludes, "The conventional DoD acquisition process is too long and cumbersome to fit the needs of the many systems that require continuous changes and upgrades."

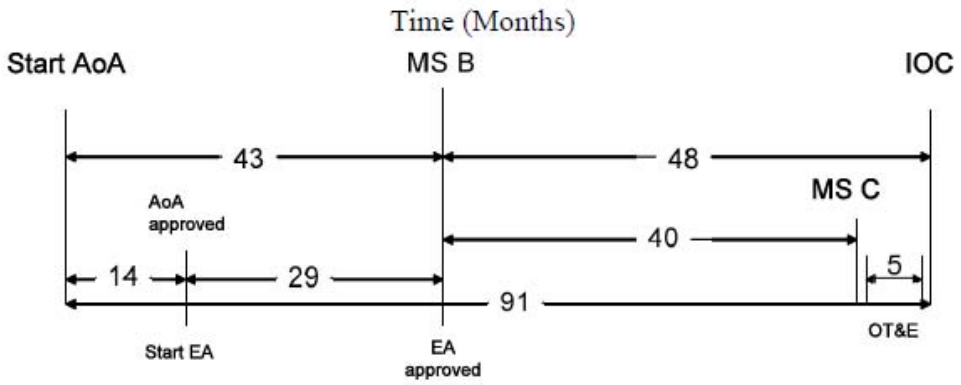


Figure 2. DoD IT Acquisition Timeline
(OUSD(AT&L), 2009a)

The *DSB-IT* reached the conclusion that current acquisition policies and processes (as defined in the DoD 5000 series directive and instruction) "do not address the fundamental challenges of acquiring information technology for its range of uses in DoD. Instead, a new acquisition approach is needed that is consistent with rapid IT development cycles and software-dominated acquisitions." The *DSB-IT* proposed a new model for acquisition of IT, depicted in Figure 3. The proposed model is agile, based on successful commercial practices, and intended to deliver capability in "release" cycles of approximately 18 months or less. Releases are divided into "iterations" (nominally three iterations per release). Lastly, the model highlights integrated developmental test (DT) and operational test (OT).

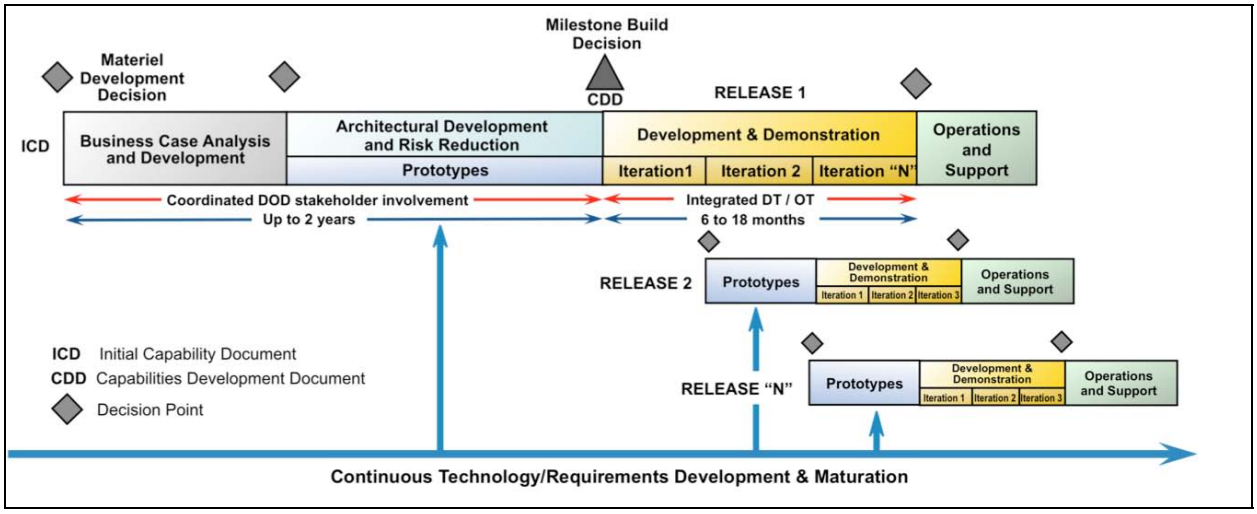


Figure 3. Proposed IT Acquisition Process
(OUSD(AT&L), 2009a)

Test and evaluation (T&E) is an essential part of the DoD acquisition system. Test and evaluation typically begins with early prototypes, and then becomes increasingly complex, as testing progresses from individual components to systems, then the "system of systems." Likewise, test conditions generally evolve from benign, low stress, lab environments through early operational assessments with a limited user base, to full scale, formal OT&E on production representative systems with trained users. Figure 4 depicts the flow of test events, all of which are found on the right side of the "systems engineering V" diagram, as shown in the Integrated Defense Acquisition, Technology and Logistics Life Cycle Management System chart (DAU, 2009). Despite the increased emphasis on "integrated testing" today, test, evaluation, and certification (TE&C) activities still concentrate at the end of development. Moreover, the DoD version of the V, as depicted in the figure, does not connect the early test activities to the IOT&E or interoperability testing. In an acquisition model designed for IT, we have to transform the traditional "one way" V into an iterative process; likewise, testing should be early and often (parallel versus integrated) and always with a mission focus.

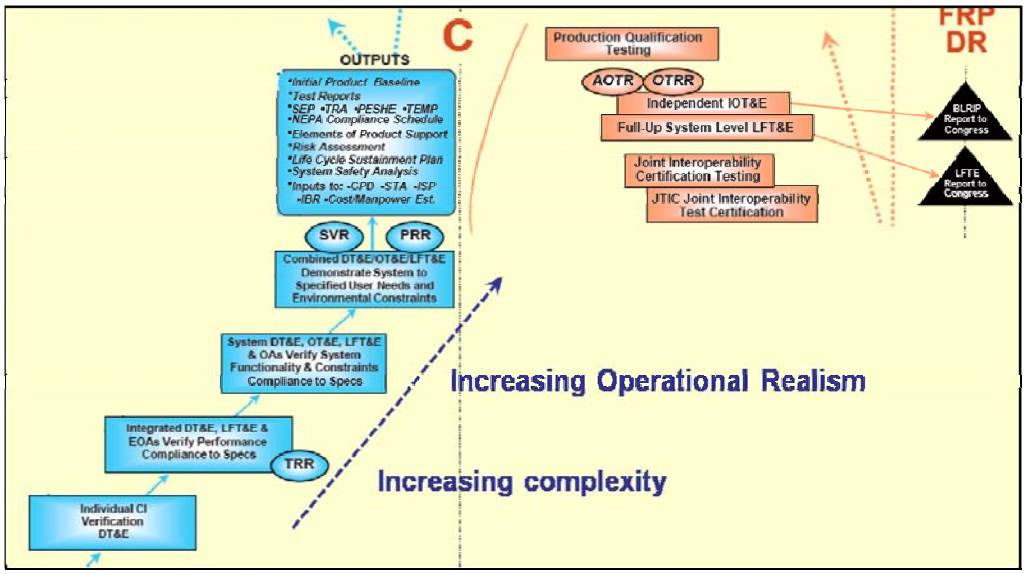


Figure 4. T&E in the Systems Engineering "V"

One of the concerns with the process depicted in Figure 4 is that programs engage different test organizations at different times, or change them mid-stream. This is particularly evident in the transition from the developmental tester to the independent operational test agent and may explain the disconnect noted above. For IT capabilities, the interoperability tester and the security (information assurance) tester conduct assessments and report results for separate decision-making (certification) purposes. This separation of test organizations and activities may have the effect of parsing information to different decision-makers as opposed to fusing results into a comprehensive evaluation. As we develop a new IT acquisition model, we should consider a TE&C model that synchronizes the efforts of all test organizations towards improving capability and providing comprehensive information to decision-makers.

Test and evaluation has its own "big bang" in the DoD acquisition system. The Initial Operational Test and Evaluation (IOT&E), shown in Figure 1, is the culminating event in a T&E strategy and is necessary to achieve a fielding decision. Title 10 USC, §139, mandates

IOT&E for MDAPs for "the purpose of determining the effectiveness and suitability of the weapons, equipment, or munitions for use in combat by typical military users"; the *DoD 5000* applies this requirement to MAIS. The IOT&E is a complex endeavor; it takes a long time to plan, requires a test unit (sometimes hard to come by in a Department at war), time to train the test unit and the testers, a support system, extensive data collection and analysis, and time to prepare reports for decision-makers. The National Research Council observed, the "DoD is fast approaching a period in which a single all-encompassing large-scale operational test, as currently practiced, will cease to be feasible" (NRC, 2006). For warfighting platforms that have long developmental timelines, an IOT&E is likely to be a small proportion of the total program cost and short relative to the total program schedule. This is another factor to consider in development of an IT acquisition model. For IT capabilities following agile development, the current approach to IOT&E could have significant cost and schedule impact. The question is, therefore, how to reduce the impact without loss in rigor and objectivity.

Test, Evaluation, and Certification of DoD IT

Test, evaluation, and certification for IT has several facets. Figure 5 portrays a high-level view of the IOT&E "test execution window" for IT capabilities. Depicted in the figure are the various TE&C and supporting activities to satisfy the three decision-making processes necessary to field new IT capabilities:

- joint interoperability certification from the Joint Staff J6 (JS J6),
- information assurance certification and accreditation (IA C&A) from the Designated Accrediting Authority (DAA), and
- the acquisition decision from the Milestone Decision Authority (MDA).

There are likely to be several DT activities, such as integration and acceptance testing, which may occur prior to or within the window. Time must be allocated to train users and testers, and the programs have to implement support systems, such as the help desk, as intended to support the fielded system. The IA C&A typically precedes OT to obtain an authority to test, while interoperability testing may be a separate activity or in conjunction with the OT. All of these events set the stage for OT to confirm that the capability is ready for fielding.

The timeline in Figure 5 depicts a mix of both policy and practice. For example, policy requires a test concept brief 120 days prior to OT, and test plan approval 60 days prior, for programs on the T&E oversight list. In practice, OT duration varies by system; some tests can exceed what is shown by months. Likewise, final evaluation report preparation varies; the 60 days shown is probably conservative. Hence, the IOT&E test execution window can exceed 6 months. Figure 5 is not intended to imply that either interoperability or information assurance certification occurs within the time blocks shown, merely that these activities form an essential part of the IT T&E strategy and must be planned and resourced accordingly.

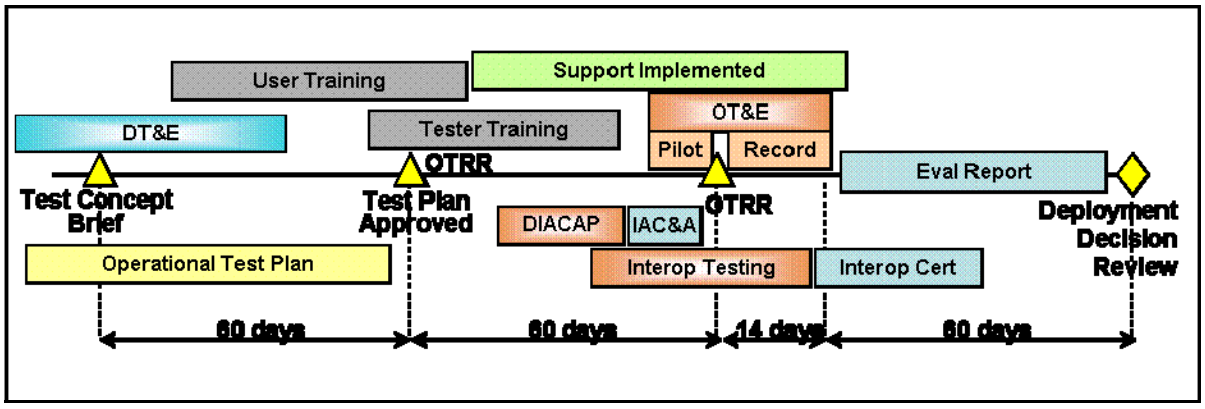


Figure 5. Test Execution Window

As stated above, effectiveness and suitability are not the only considerations for IT capabilities; information systems must also be interoperable and secure. Interoperability certification and the DoD Information Assurance Certification and Accreditation Process (DIACAP) are governed separately from the DoD acquisition system through various DoD and Chairman, Joint Chiefs of Staff directives and instructions. Separate governance processes can be disadvantageous in an acquisition system for IT; for example, it is possible today for the milestone decision authority to make a decision to buy the new capability for the department, while the DAA may deny operation on their network. In a new IT acquisition system, interoperability and information assurance processes should be integrated, not separate elements, and the testing activities associated with these certification processes should form an integral part of the IT T&E strategy.

Interoperability

One of the major complaints from the field today is lack of interoperability among the countless information systems at the strategic, operational, and tactical levels. In any new IT acquisition system, it seems clear that we are going to have to treat interoperability differently—elevate its place in the decision-making process and establish meaningful accountability. The *DoDI 5000.02* is weak in describing interoperability considerations and offers very little guidance on interoperability testing. Rather than being overseen by the milestone decision authority, interoperability is managed through a separate decision-making process governed by the *DoD 4630* directive and instruction and the *Chairman of the Joint Chiefs of Staff Instruction 6212*. As a result, joint interoperability testing is not well integrated into the overall T&E strategy of a system; for example, is the PM responsible for interoperability testing or is the operational test agent (OTA)? ... Who approves the interoperability test plan? ... Should the JS J6 sign the T&E Master Plan (TEMP)?

Interoperability is a key performance parameter (KPP), referred to today as the Net-Ready KPP (NR-KPP). The *Glossary of Defense Acquisition Terms* defines a KPP as a system characteristic "considered critical or essential to the development of an effective military capability." The interoperability KPP has not been a stable element of the requirements system, however, and the final report of the Defense Acquisition Performance Assessment (DAPA) Project referred to the interoperability KPP as one "for which there is no method of testing." From August 1999 to the present, the interoperability KPP has been defined and redefined four times.

The Interoperability KPP (I-KPP) was first introduced in the Requirements Generation System (RGS) in the August 1999 issuance of *CJCSI 3170.01A*. The methodology for assessing the I-KPP based on "information exchange requirements" (IERs) followed in the May 2000 *CJCSI 6212.01B*. The Joint Staff canceled the RGS in June 2003 and implemented the Joint Capability Integration and Development System (JCIDS) in *CJCSI 3170.01C*, then in November 2003, the Joint Staff replaced the I-KPP with the NR-KPP in *CJCSI 6212.01C*. The NR-KPP moved away from measurable and testable IERs to technical compliance attributes such as the "Net-Centric Operations and Warfare Reference Model (NCOW-RM)," "key interface profiles," and "integrated architecture products"—none of which were particularly well suited to "hands-on" testing. In the March 2006 *CJCSI 6212.01D*, the NR-KPP statement changed to read in more operationally meaningful terms, but the threshold and objective requirements retained the same technical attributes. In December 2008, the NR-KPP changed again; the *CJCSI 6212.01E* replaced "key interface profiles" with the "Technical Standards/Interfaces" element, deleted the NCOW-RM, and introduced GIG Enterprise Service Profiles (GESPs)—again, not readily "hands-on" testable. Despite the continuous revisions, the NR-KPP remains arguably the least measurable and testable of all the required KPPs. An operationally meaningful, measurable, and testable interoperability KPP will be an essential element of a new IT acquisition system.

Information Assurance

Information assurance (IA) is another critical element in IT acquisition and requires security testing. Like interoperability, the *DoDI 5000.02* is weak in describing IA considerations and offers little guidance on security testing. Instead of being overseen by the milestone decision authority, information assurance is governed through the *DoD 8500* series and the *CJCSI 6510*. The *DoDI 8580.1*, *Information Assurance in the Defense Acquisition System*, does link the two governance processes though. Security T&E is another category of testing for which we do not have a standard approach in developing the overall T&E strategy; for example, who approves the security test plan? ... Should the DAA sign the TEMP?

The DoD implemented IA C&A in December 1997 with the release of the *DoDI 5200.40*, *DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*. In November 2003, as threats to DoD information systems and networks were becoming increasingly apparent, the *CJCSI 6212.01C* included IA as an element of the newly defined NR KPP. In July 2006, the ASD(NII) canceled *DITSCAP*, issued interim guidance, and then, in November 2007, *DIACAP* became the process of record with the release of *DoDI 8510.01*. Completion of the DITSCAP or DIACAP process has essentially equated to satisfying the IA element of the NR KPP. Completing the DITSCAP or DIACAP process, however, has never been completely satisfying in the overall T&E strategy.

In November 1999, the Director, Operational Test and Evaluation (DOT&E) issued the *Policy for Operational Test and Evaluation of Information Assurance*. The policy required the independent OTAs to assess IA as part of the system evaluation, while leveraging to the extent possible other IA testing, such as DITSCAP security T&E, to reduce duplication. In some cases, the policy required "field penetration testing by a Red Team" as part of IOT&E. Inclusion of red teams in IOT&E adds a new level of complexity into the already challenging and resource intensive undertaking discussed earlier.

Unlike joint interoperability certification, which has a single process owner and single tester (although a recent change to the *CJCSI 6212* permits testing within the components

for designated programs), IA has many owners and many testers. In our current IA C&A process, each information system has a DAA appointed by the component head or the mission area Principal Accrediting Authority (PAA). The DAA is responsible for the decision to accredit, and may authorize or deny operation or testing of their assigned information systems. The combined effect of multiple decision authorities and multiple test organizations is likely to contribute more to delay and inconsistency than efficiency and standardization. The *Defense Science Board Task Force on Achieving Interoperability in a Net Centric Environment (DSB-NC)* described the problem in these terms:

> Multiple certification processes and inconsistent retest processes exist, often resulting in the delivery of obsolete products or products that are no longer supported. Current test, evaluation, and certification (TE&C) processes take months and often years. In a wartime environment where information and technical capability is becoming more and more critical to the warfighter, a delay of months or years for redundant testing to deliver a new capability is unacceptable.

The *DSB-NC* observed that one cause of redundant testing is "Testing, evaluation, and certification that are performed by one Service or one agency are most often not accepted by other Services or agencies." The *DSB-NC*, therefore, recommended a new mandate: "test by one, accept by all." Recently, DoD PAAs signed a policy for reciprocity to accept each other's security assessments (DoD, 2009). This policy is a very positive step toward reducing redundancy and streamlining capability delivery to the enterprise.

As stated, the *DSB-IT* recommended a new, agile IT acquisition system. To its credit, the *DSB-IT* described the capability at each iteration as "tested and potentially deployable," and highlighted "integrated DT/OT" (refer back to Figure 3). Unfortunately, the *DSB-IT* retained an essentially status quo T&E approach, writing: "Following the nominal completion of three iterations, an Initial Operational Test and Evaluation (IOT&E) is accomplished prior to operationally fielding a release." This may not be the most efficient model; for example, capability developed and tested in early iterations is likely to be tested again in IOT&E. Moreover, if we conduct the IOT&E as we do it today (six months of TE&C activities), then the desired 18-month release cycle may in reality approach 24 months. More importantly, however, potentially deployable capability may be withheld from fielding until completion of the release and IOT&E. While this approach has the well-intentioned effect of reducing the churn of multiple fieldings on the operational force, it is not agile. Therefore, we might consider a model in which the decision to field, whether at iteration or release, is at the discretion of the gaining commander. Regardless of whether we test iteration or release, we are going to need a new T&E model that is responsive to agile IT programs.

Towards an Agile IT Acquisition and TE&C System

The preceding sections have made the case that acquisition of information technology in the DoD consists of multiple processes that do not necessarily share the goal of rapid delivery of enhanced capabilities to the warfighter. We lack an overarching process specifically designed for fielding IT capabilities to the enterprise. Likewise, we have challenges to overcome to create truly integrated TE&C processes that ensure capabilities are effective, suitable, interoperable, and secure.

From beginning to end—requirements definition, capability development, TE&C, governance, and operations—the department lacks agile processes designed for IT. An agile IT acquisition model must begin with agility in the requirements system; thus, one

consideration (beyond the scope of this article) would be to develop a “JCIDS-light” requirements system for IT. An agile IT requirements system must shift from the current big bang, “everything in the first increment” approach to prioritizing capability needs for delivery in a series of little bangs. Additionally, we need operationally meaningful KPPs for interoperability and security.

An agile IT acquisition model requires agile oversight, so management and governance processes must be redesigned to foster rapid development and fielding cycles. DoD business IT systems have already moved to a “business capability lifecycle” (BCL) management process intended to be more flexible. The BCL “merges three major DoD processes [JCIDS, the DoD 5000 Acquisition System, and the Investment Review Board (IRB)/Defense Business System Management Committee (DBSMC) governance bodies] to provide a single governance and decision support framework to enable faster delivery of business capabilities” (http://www.bta.mil/products/bcl.html). The BCL leverages the Enterprise Risk Assessment Methodology (ERAM) “to reduce systemic risk and support informed decision making” (http://www.bta.mil/products/eram.html). Similar governance approaches could be adopted within the warfighting, intelligence, and enterprise information environment portfolios as well.

As requirements processes become more agile, programs will shift to design-build cycles based on prioritized requirements. Whereas the traditional systems engineering “V” model has the perception of being a one-way path, the agile development lifecycle is more iterative, less sequential. The TE&C community must be ready to engage agile programs through equally agile processes; the six-month test execution window that occurs at the end of an increment today has to be shortened and moved well left in the schedule, to focus on the development iterations. A key element of tester agility will be formation of a capability test team to merge the traditional DT, OT, interoperability, and security test activities into a comprehensive TE&C strategy.

Our objective in T&E should be mission-focused agility: rapidly composable mission-oriented test plans that permit objective assessments of technical and operational capabilities and limitations in each iteration. Likewise, we need agile DIACAP and interoperability certification, where “test by one, accept by all” is the norm. For capabilities developed in six-month iterations, the capability test team should be able to complete the entire test execution window—plan, execute, report—in six-weeks or less. Figure 6 depicts the TE&C paradigm shift. This can be accomplished only through a highly collaborative process that is responsive to changing requirements priorities and developer agility. Essential to this approach will be early and continuous involvement from the user community. In this model, the overarching theme is “build a little, test a little (learn a lot), field a little.” Then, as capabilities are deployed, the fielding paradigm should be “start small, scale rapidly,” while continuously monitoring to ensure the capability performs as desired.

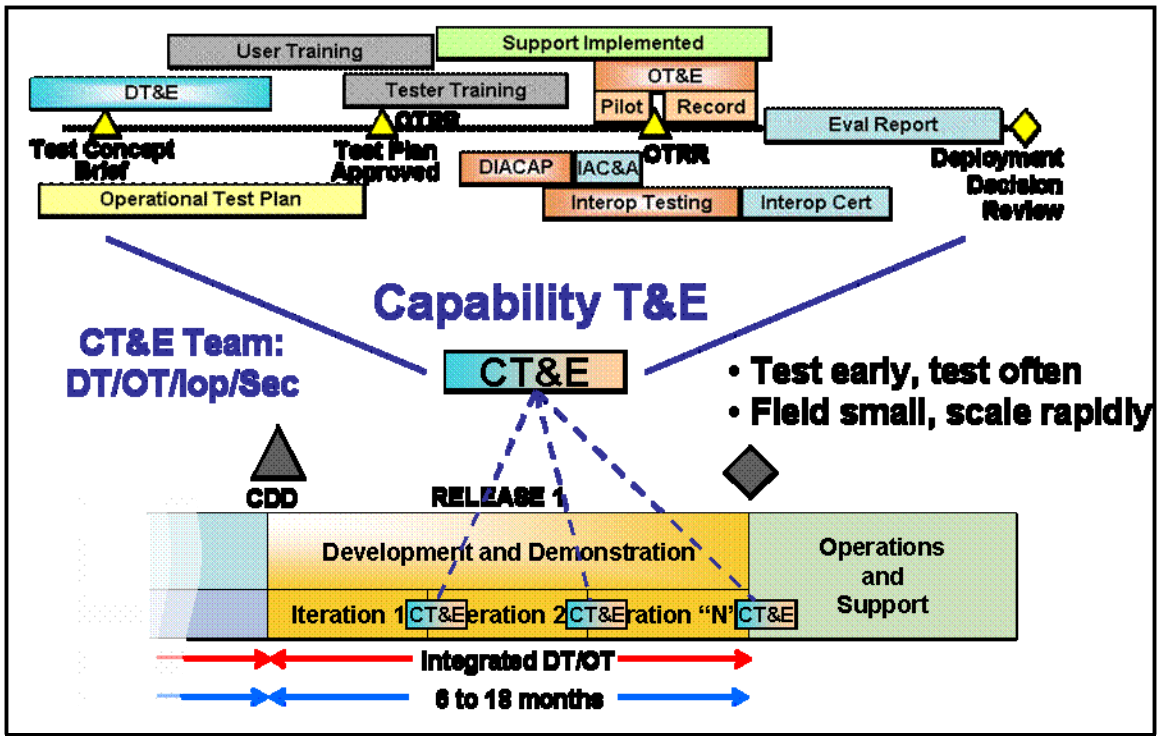


Figure 6. Agile T&E

Summary

Information technologies evolve rapidly, as is abundantly evident in the commercial sector. As the DoD acquires IT to enhance warfighting capabilities, we need to become more agile. Agility cannot just occur in capability development either; all aspects of the IT acquisition system must be redesigned for agility. To be responsive to operational requirements, and to ensure the capabilities work as intended, test, evaluation, and certification must move at the speed of need. The Defense Science Board reports provide a good starting point from which to build a new model for acquisition of IT; now, let's take the next bold step to implement agile processes that deliver enhanced IT capabilities for the warfighter.

References

CJCS. (1999). *Requirements generation system* (CJCSI 3170.01A). Washington, DC: Author.

CJCS. (2000). *Interoperability and supportability of national security systems and information technology systems* (CJCSI 6212.01B). Washington, DC: Author.

CJCS. (2003a). *Interoperability and supportability of national security systems and information technology systems* (CJCSI 6212.01C). Washington, DC: Author.

CJCS. (2003b). *Joint capability integration and development system* (CJCSI 3170.01C). Washington, DC: Author.

CJCS. (2006). *Interoperability and supportability of national security systems and information technology systems* (CJCSI 6212.01D). Washington, DC: Author.

CJCS. (2008). *Interoperability and supportability of national security systems and information technology systems* (CJCSI 6212.01E). Retrieved March 30, 2010, from http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf

DAU. (2009, June 15). *Integrated defense acquisition, technology and logistics life cycle management system chart* (Vers. 5.3.4). Retrieved March 30, 2010, from https://acc.dau.mil/IFC/index.htm

DoD. (1997). *DoD information technology security certification and accreditation process (DITSCAP)* (DoD Instruction 5200.40). Retrieved March 30, 2010, from http://iase.disa.mil/diacap/i520040.pdf

DoD. (2004). *Interoperability and supportability of information technology (IT) and national security systems (NSS)* (DoD Directive 4630.05). Retrieved March 30, 2010, from http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf

DoD. (2007). *DoD information assurance certification and accreditation process (DIACAP)* (DoD Instruction 8510.01). Washington, DC: Author.

DoD. (2008). *Operation of the defense acquisition system* (DoD Instruction 5000.02). Retrieved March 30, 2010, from http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf

DoD. (2009). *DoD information system certification and accreditation reciprocity*. Memorandum. Retrieved March 30, 2010, from http://www.doncio.navy.mil/Download.aspx?AttachID=1055

National Research Council (NRC). (2006). *Testing of defense systems in an evolutionary acquisition environment*.

OUSD(AT&L). (2009a). *Department of Defense policies and procedures for the acquisition of information technology*. Retrieved March 30, 2010, from http://www.acq.osd.mil/dsb/reports.htm

OUSD(AT&L). (2009b). *Report of the Defense Science Board Task Force on achieving interoperability in a net centric environment*. Retrieved March 30, 2010, from http://www.acq.osd.mil/dsb/reports.htm

United States Code. (2009). Title 10, Chapter 4, § 139. Retrieved March 30, 2010, from http://uscode.house.gov/download/pls/10C4.txt

US Congress. (2009). *Weapons acquisition system reform through enhancing technical knowledge and oversight act of 2009*. Retrieved March 30, 2010, from http://thomas.loc.gov/cgi-bin/query/z?c111:S.454:

US Congress. (2010). *National defense authorization act of 2010*. Retrieved March 30, 2010, from http://thomas.loc.gov/cgi-bin/query/z?c111:S.454:

THIS PAGE INTENTIONALLY LEFT BLANK

2003 - 2010 Sponsored Research Topics

Acquisition Management

- Acquiring Combat Capability via Public-Private Partnerships (PPPs)
- BCA: Contractor vs. Organic Growth
- Defense Industry Consolidation
- EU-US Defense Industrial Relationships
- Knowledge Value Added (KVA) + Real Options (RO) Applied to Shipyard Planning Processes
- Managing the Services Supply Chain
- MOSA Contracting Implications
- Portfolio Optimization via KVA + RO
- Private Military Sector
- Software Requirements for OA
- Spiral Development
- Strategy for Defense Acquisition Research
- The Software, Hardware Asset Reuse Enterprise (SHARE) repository

Contract Management

- Commodity Sourcing Strategies
- Contracting Government Procurement Functions
- Contractors in 21st-century Combat Zone
- Joint Contingency Contracting
- Model for Optimizing Contingency Contracting, Planning and Execution
- Navy Contract Writing Guide
- Past Performance in Source Selection
- Strategic Contingency Contracting
- Transforming DoD Contract Closeout
- USAF Energy Savings Performance Contracts
- USAF IT Commodity Council
- USMC Contingency Contracting

Financial Management

- Acquisitions via Leasing: MPS case
- Budget Scoring
- Budgeting for Capabilities-based Planning

- Capital Budgeting for the DoD
- Energy Saving Contracts/DoD Mobile Assets
- Financing DoD Budget via PPPs
- Lessons from Private Sector Capital Budgeting for DoD Acquisition Budgeting Reform
- PPPs and Government Financing
- ROI of Information Warfare Systems
- Special Termination Liability in MDAPs
- Strategic Sourcing
- Transaction Cost Economics (TCE) to Improve Cost Estimates

Human Resources

- Indefinite Reenlistment
- Individual Augmentation
- Learning Management Systems
- Moral Conduct Waivers and First-tem Attrition
- Retention
- The Navy's Selective Reenlistment Bonus (SRB) Management System
- Tuition Assistance

Logistics Management

- Analysis of LAV Depot Maintenance
- Army LOG MOD
- ASDS Product Support Analysis
- Cold-chain Logistics
- Contractors Supporting Military Operations
- Diffusion/Variability on Vendor Performance Evaluation
- Evolutionary Acquisition
- Lean Six Sigma to Reduce Costs and Improve Readiness
- Naval Aviation Maintenance and Process Improvement (2)
- Optimizing CIWS Lifecycle Support (LCS)
- Outsourcing the Pearl Harbor MK-48 Intermediate Maintenance Activity
- Pallet Management System
- PBL (4)
- Privatization-NOSL/NAWCI
- RFID (6)

- Risk Analysis for Performance-based Logistics
- R-TOC AEGIS Microwave Power Tubes
- Sense-and-Respond Logistics Network
- Strategic Sourcing

Program Management

- Building Collaborative Capacity
- Business Process Reengineering (BPR) for LCS Mission Module Acquisition
- Collaborative IT Tools Leveraging Competence
- Contractor vs. Organic Support
- Knowledge, Responsibilities and Decision Rights in MDAPs
- KVA Applied to AEGIS and SSDS
- Managing the Service Supply Chain
- Measuring Uncertainty in Earned Value
- Organizational Modeling and Simulation
- Public-Private Partnership
- Terminating Your Own Program
- Utilizing Collaborative and Three-dimensional Imaging Technology

A complete listing and electronic copies of published research are available on our website: www.acquisitionresearch.org

THIS PAGE INTENTIONALLY LEFT BLANK

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CALIFORNIA 93943

www.acquisitionresearch.org

Defense Information Systems Agency

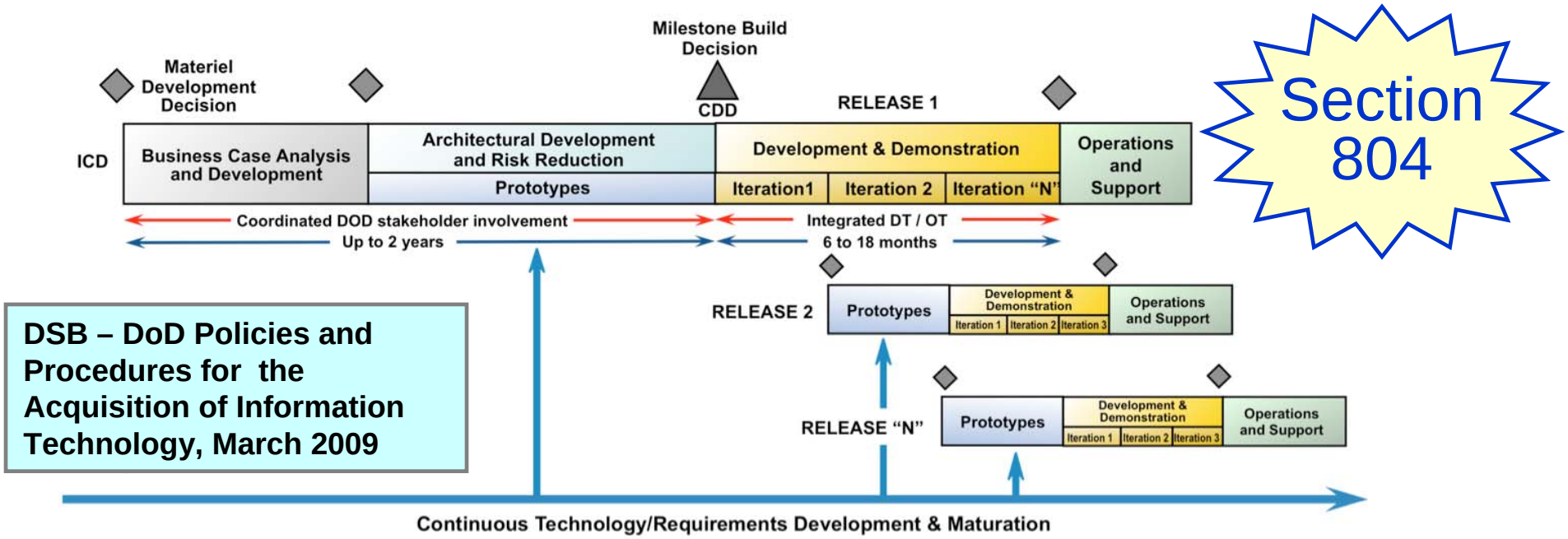
A Combat Support Agency

Test and Evaluation for Agile Information Technologies

Dr. Steven Hutchison
DISA Test & Evaluation Executive
May 12, 2010

New DoD Acquisition Process for IT

A Combat Support Agency



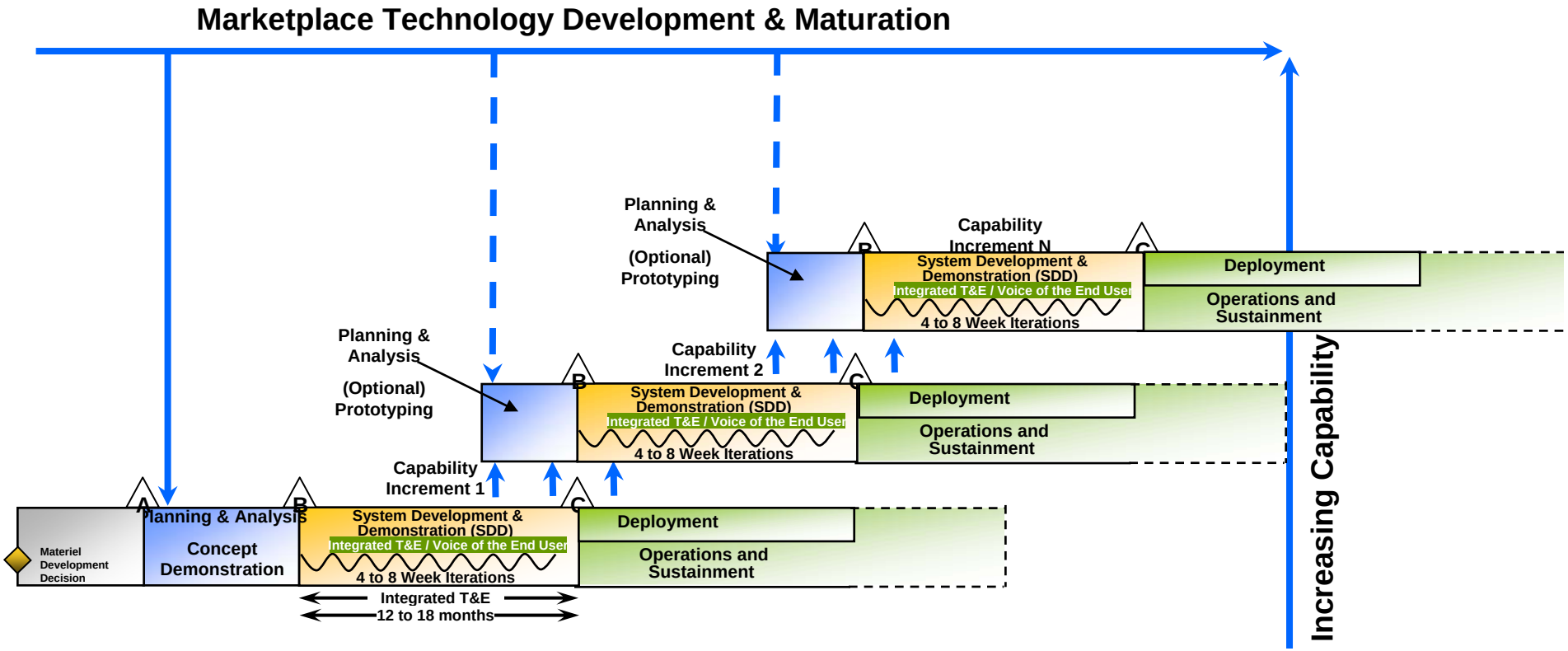
Section 804

DSB – DoD Policies and Procedures for the Acquisition of Information Technology, March 2009

- Modeled on successful commercial practices
  - Agile software Development
- Multiple, rapidly executed increments or releases of capability
  - Releases divided into ~6 month iterations
  - Iterations tested and potentially deployable
- Early and continual involvement of the user
- Integrated testing

National Academies Proposed Model

A Combat Support Agency

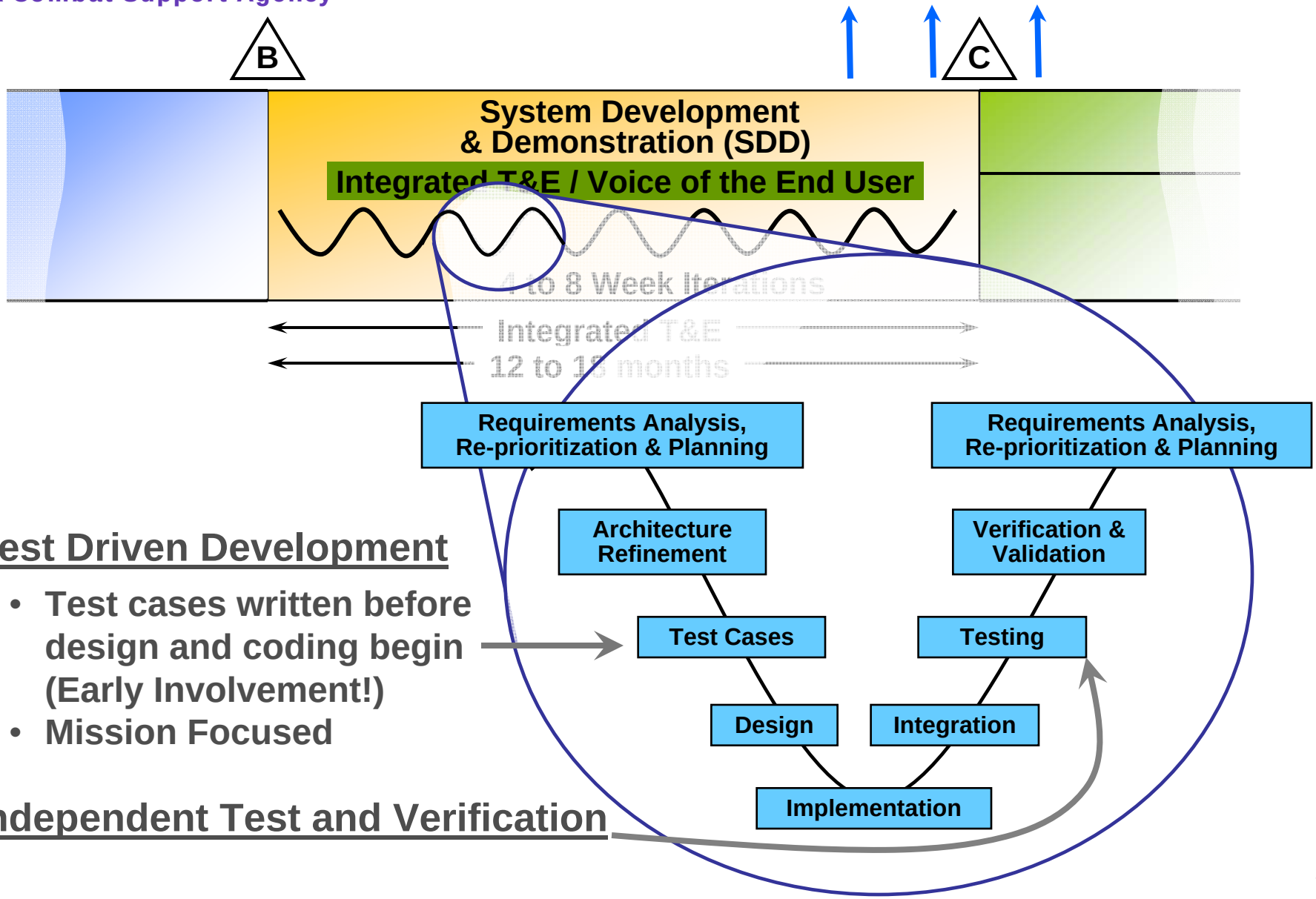


Acquisition Management Approach for Software Development and Commercial off-the-shelf (COTS) software Integration IT programs

National Academy of Sciences: Achieving Effective Acquisition of Information Technology in the Department of Defense, December 2009

DISA
A Combat Support Agency

NAS Model - Details



Test Driven Development

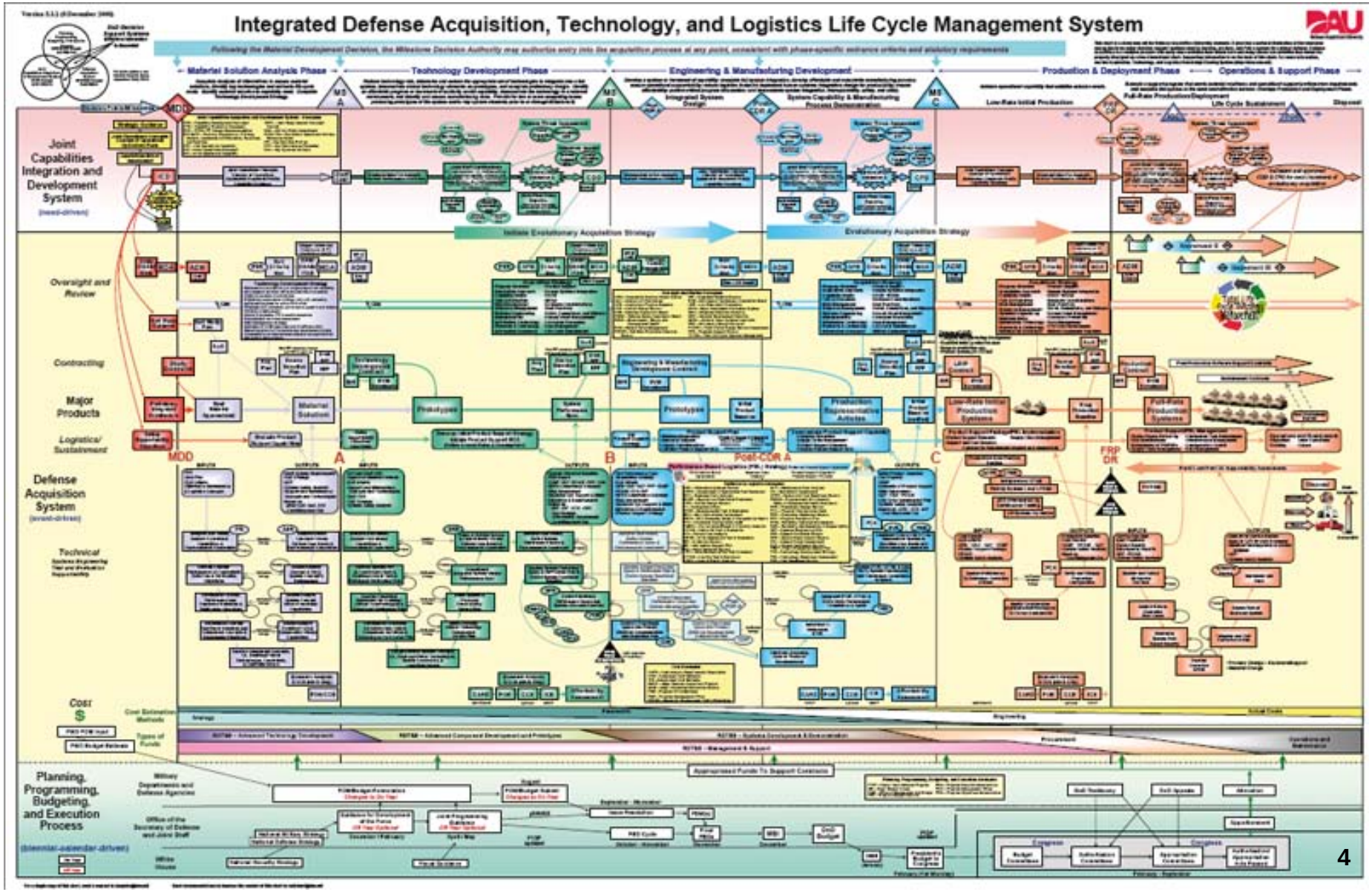
- Test cases written before design and coding begin (Early Involvement!)
- Mission Focused

Independent Test and Verification

DISA

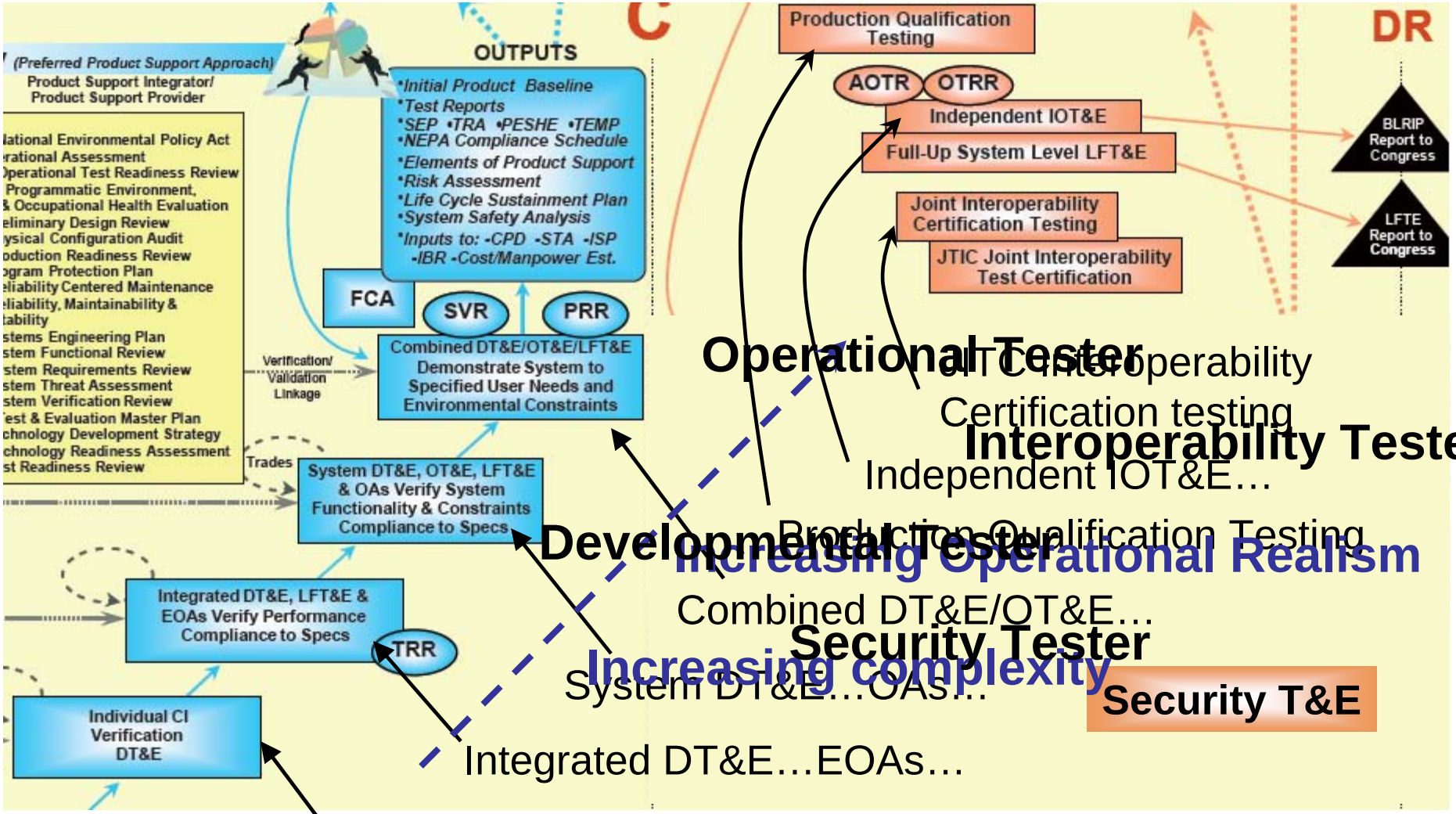
A Combat Support Agency

The DoD Acquisition Model



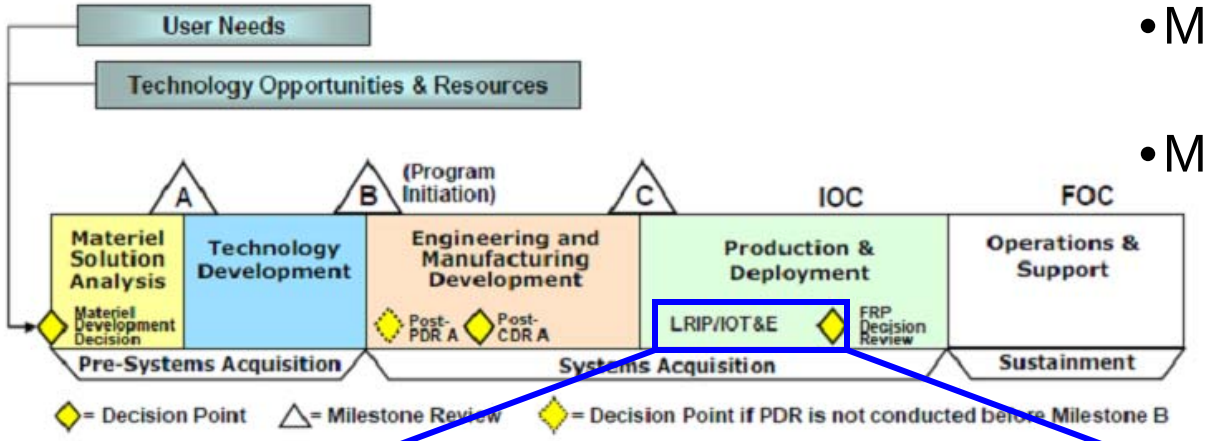
DISA
A Combat Support Agency

T&E in Acquisition Lifecycle

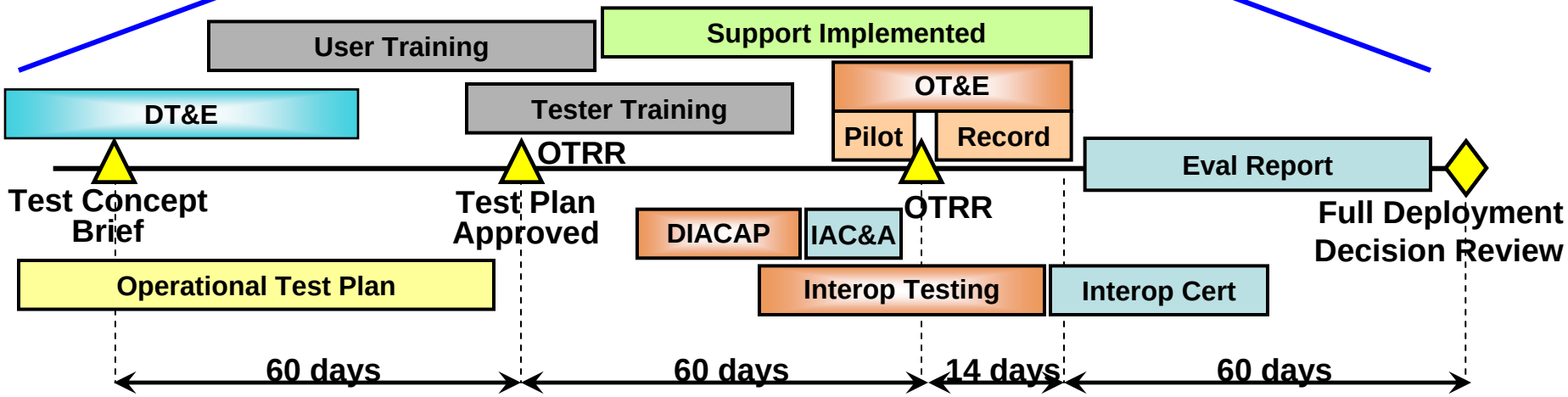


DoD Test, Evaluation & Certification

A Combat Support Agency



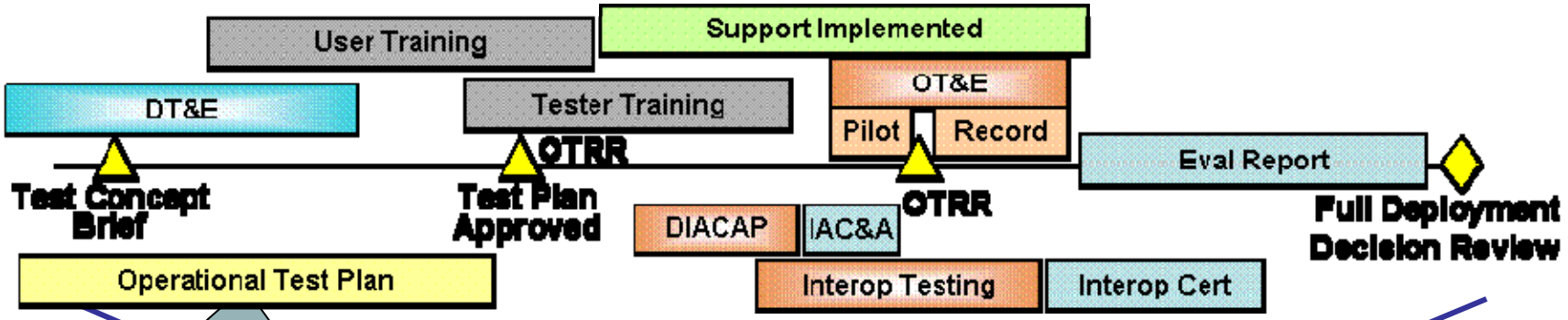
- Multiple Test Orgs
  - DT, OT, Iop, IA
- Multiple Decision Makers
  - MDA, JS J6, DAA



T&E Plan – Test – Report (PTR) cycle can exceed six months!

DISA
A Combat Support Agency

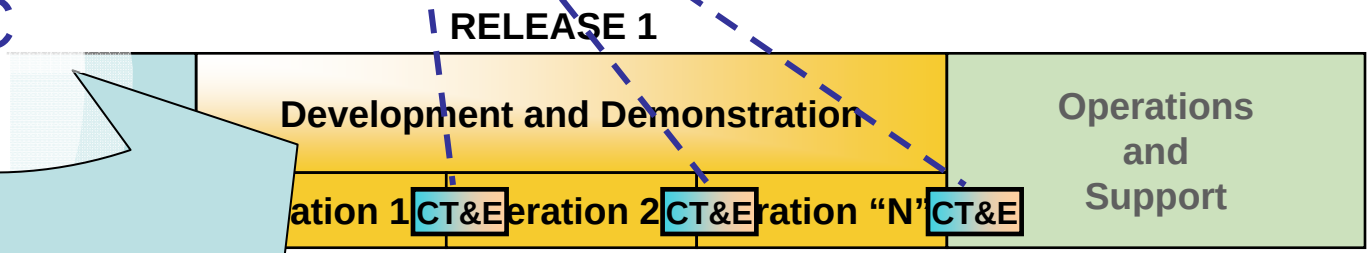
TE&C Paradigm Shift Capability TE&C”



Paradigm Shift: from large scale, sequential TE&C to *Agile* TE&C

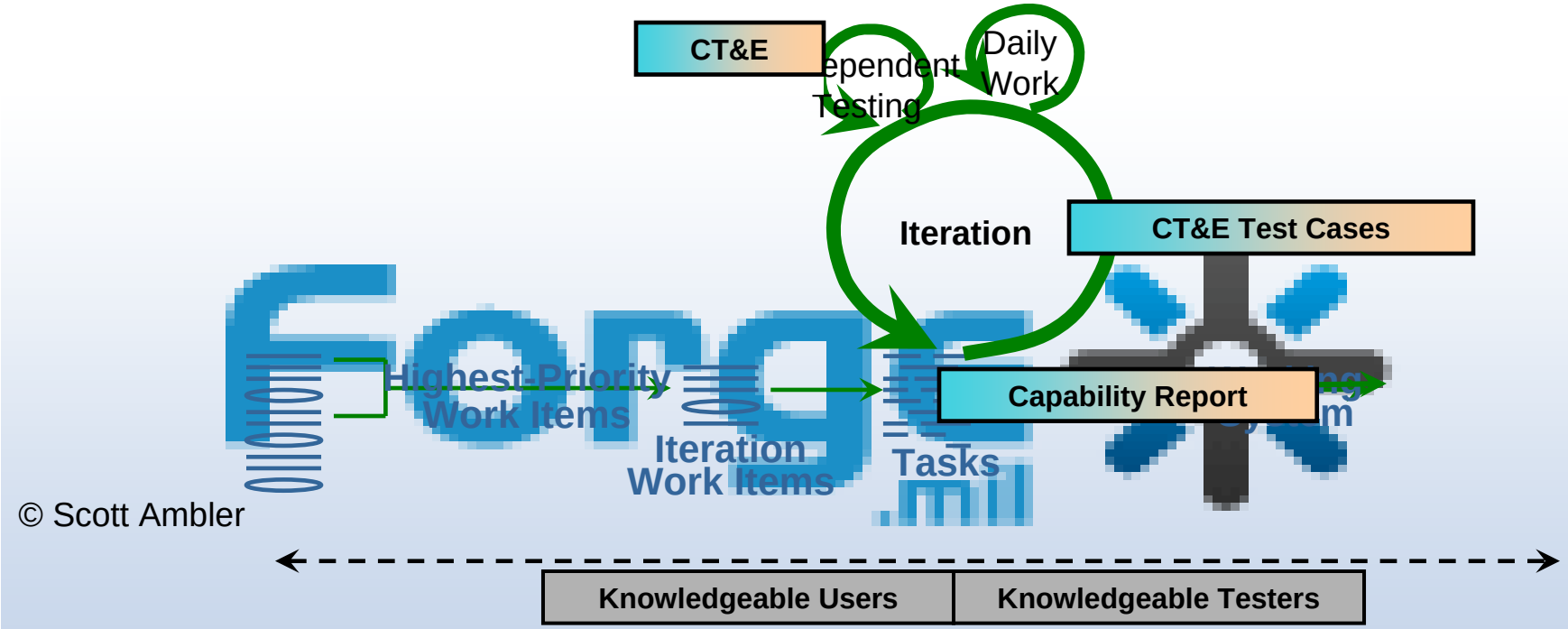
Capability TE&C

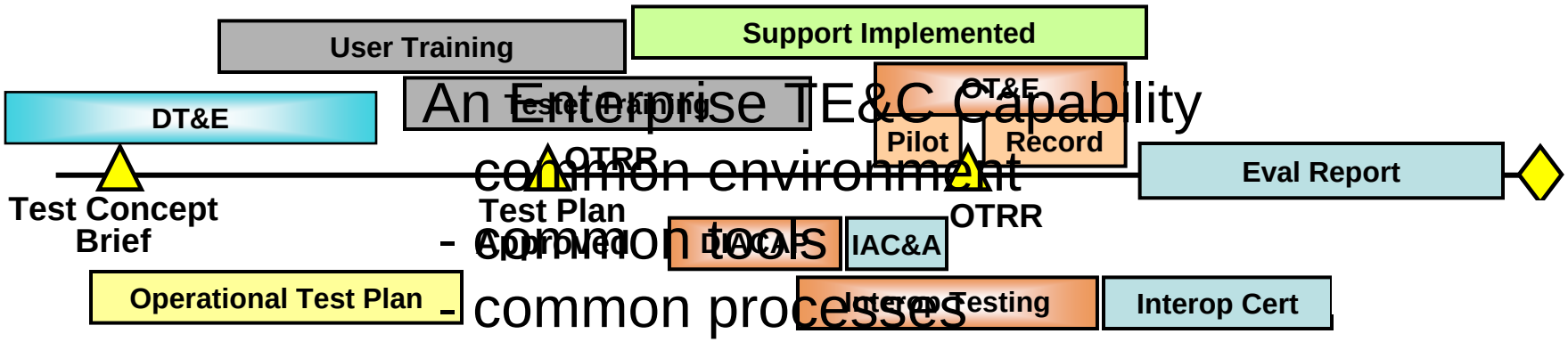
Capability Test Team
Fully integrated DT/OT/Iop/Sec



DISA
A Combat Support Agency

Capability TE&C

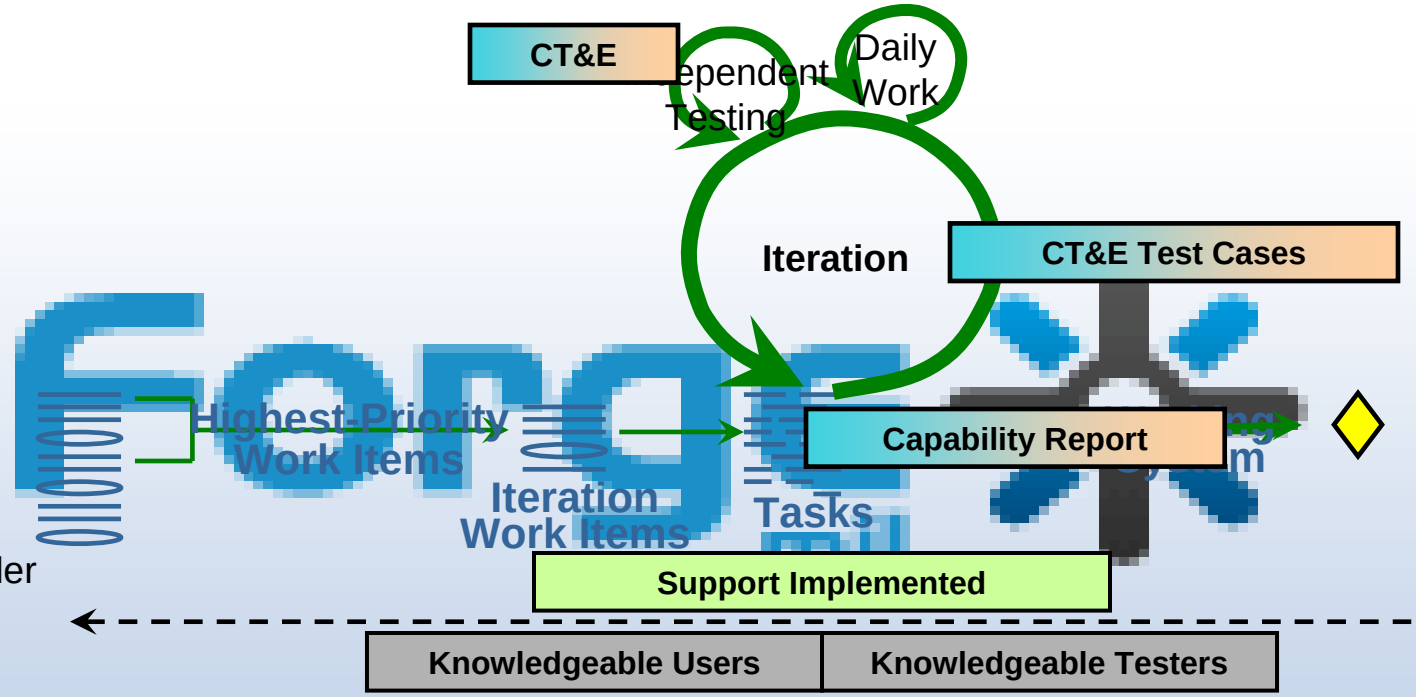




An Enterprise TE&C Capability
- common environment
- common tools
- common processes

DISA
A Combat Support Agency

Capability TE&C



- **Responsible Test Organization**
  - **Coordinates test assets**
- **Empowered Capability Test Team**
  - **Executes testing**
- **Ready access to knowledgeable users**
- **Automation essential!**

- **Rapid Plan –Test – Report Cycle**
  - **Risk based; mission focused**
  - **Relevant critical technical parameters**
  - **Relevant key performance parameters**
  - **Relevant interoperability measures**
  - **Relevant security measures**

DISA
A Combat Support Agency

Summary

- New IT Acquisition model is coming
- TE&C processes must adapt
  - Responsive to iterative, incremental development
  - Responsive to User priorities
  - Lean processes!
  - High optempo
- Dramatically reduced TE&C timelines
- Objective: Rapid fielding of enhanced IT capabilities to the Warfighter


DEFENSE INFORMATION SYSTEMS AGENCY