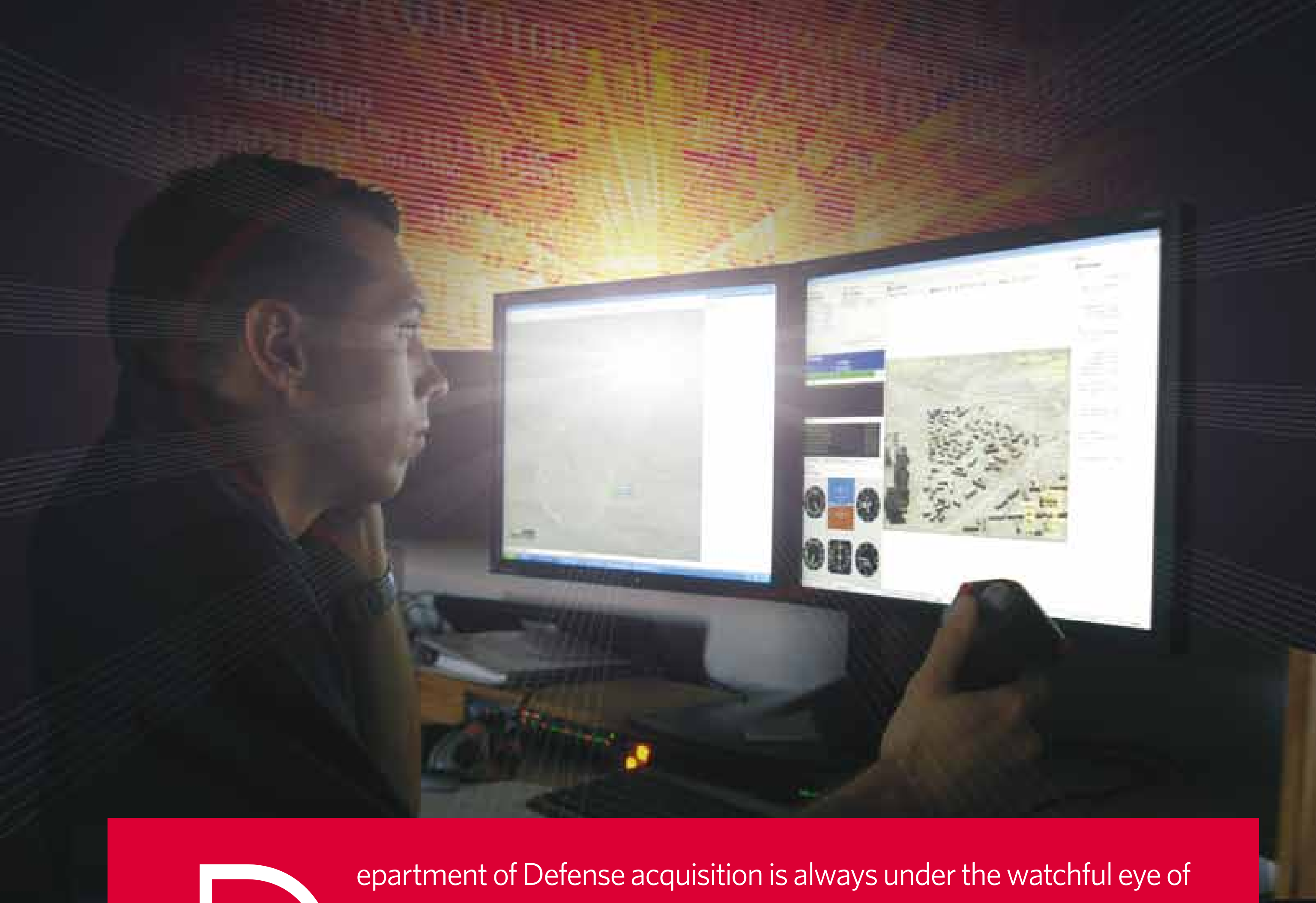
Test and Evaluation at the Speed of Need

Steven Hutchison



Department of Defense acquisition is always under the watchful eye of Congress. In 2009, Congress passed the Weapon 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 fiscal year 2010, becoming Public Law 111-84, directing long overdue changes in DoD acquisition of information technologies. According to section 804 of the law, "The Secretary of Defense shall develop and implement a new acquisition process for information technology systems."

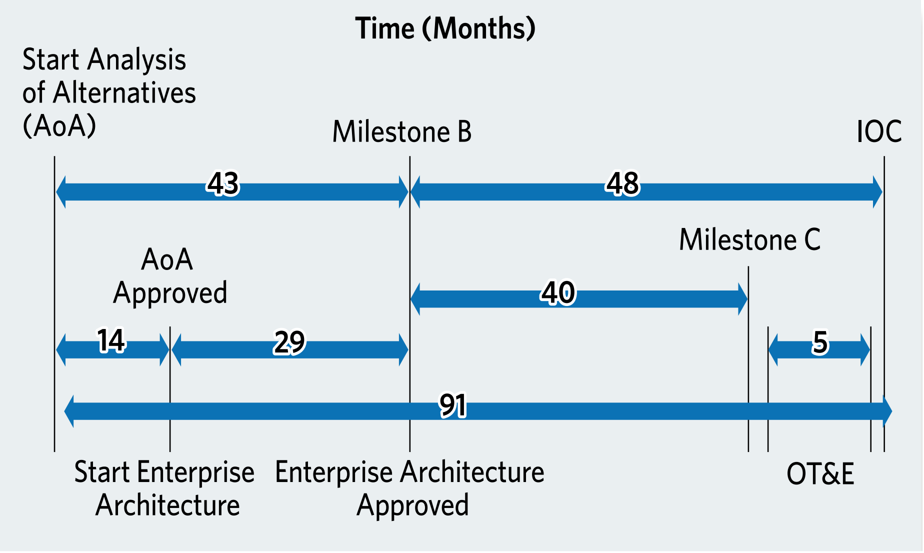
Hutchison *is the test and evaluation executive with the Defense Information Systems Agency.*

The law requires 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 (DSB-IT). The report recommends an agile model for acquiring IT similar to successful commercial practices (see <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 article attempts to connect them and fill the remaining gaps necessary to truly attain agile processes that foster rapid acquisition of enhanced IT capabilities for the warfighter.

Acquisition and Testing of IT

DoD acquires IT using the same acquisition model as for tanks, ships, and planes. A chart of the familiar Defense Acquisition Management System, taken from DoD Instruction 5000.02, can be found at < https://acc.dau.mil/CommunityBrowser.aspx?id=294453>. The system essentially makes no distinction between major defense acquisition programs and major automated information systems, and program managers for IT capabilities manage programs using 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 long time between user need definition (at the beginning of the Defense Acquisition Management System) and declaration of initial operational capability (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 initial operational capability.

Figure 1. **DoD IT Acquisition Timeline**

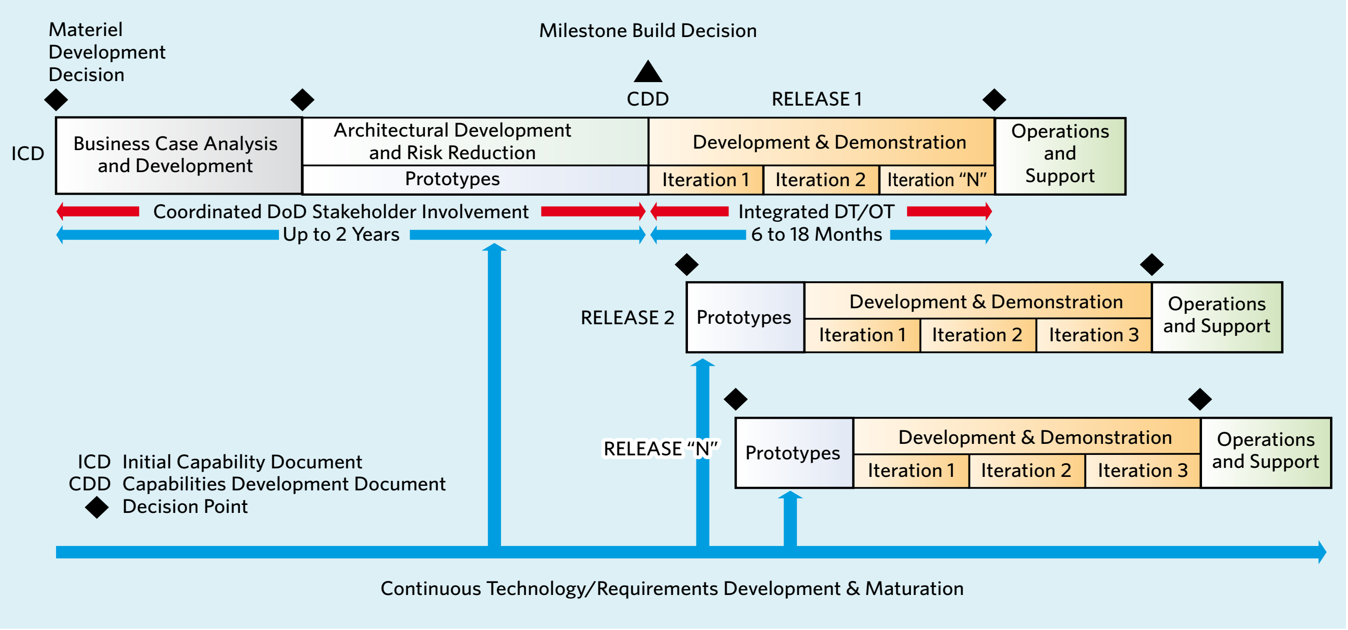


The DSB-IT describes the current DoD IT acquisition process as a “big bang approach,” meaning we try to get everything in the first increment. The report describes the approach as one that “begins with an analysis phase followed by an equally long development phase that culminates in a single test and evaluation event.” The DSB-IT cited an analysis conducted by the assistant secretary of defense for networks and information integration of 32 major automated information systems that showed the average time to deliver an initial capability is 91 months! Figure 1, 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.”

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 2. 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 and operational test.

Test and evaluation 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 operational test and evaluation on production representative systems with trained users. Figure 3 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

Figure 2. **Proposed IT Acquisition Process**


Materiel Development Decision
Milestone Build Decision
CDD
RELEASE 1
ICD
Business Case Analysis and Development
Architectural Development and Risk Reduction
Prototypes
Development & Demonstration
Iteration 1
Iteration 2
Iteration "N"
Operations and Support
Coordinated DoD Stakeholder Involvement
Up to 2 Years
Integrated DT/OT
6 to 18 Months
RELEASE 2
Prototypes
Development & Demonstration
Iteration 1
Iteration 2
Iteration 3
Operations and Support
RELEASE "N"
Prototypes
Development & Demonstration
Iteration 1
Iteration 2
Iteration 3
Operations and Support
ICD Initial Capability Document
CDD Capabilities Development Document
◆ Decision Point
Continuous Technology/Requirements Development & Maturation

Cycle Management System chart (<https://acc.dau.mil/IFC/index.htm>). Despite today's increased emphasis on integrated testing, test, evaluation, and certification activities are still concentrated at the end of development. Moreover, the DoD version of the V, as depicted in Figure 3, does not connect the early test activities to the initial operational test and evaluation (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 vs. integrated), and always with a mission focus.

One of the concerns with the process depicted in Figure 3 is that programs engage different test organizations at different times, or change them mid-stream. That is particularly evident in the transition from the developmental tester to the independent operational test agent and may explain the disconnect I've noted. For IT capabilities, the interoperability tester and the security (information assurance) tester conduct assessments and report results for separate decision-making (certification) purposes. The 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 test, evaluation, and certification 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. IOT&E 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 major defense acquisition programs for "the purpose of determining the effectiveness and suitability of the weapons, equipment, or munitions for use in combat by typical military users." DoD 5000 applies that requirement to major automated information systems. IOT&E is a complex endeavor; it takes a long time to plan; and it 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. In 2006, the National Research Council observed that "DoD is fast approaching a period in which a single all-encompassing large-scale operational test, as currently practiced, will cease to be feasible" (Testing of Defense Systems in an Evolutionary Acquisition Environment report). 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. That 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 4 portrays a high-level view of the IOT&E test execution window for IT capabilities. Depicted in the figure are the various test, evaluation, and certification and supporting activities to satisfy the three decision-making processes necessary to field new IT capabilities:

- Joint interoperability certification from the Joint Staff, J6
- Information assurance certification and accreditation (IA C&A) from the designated accrediting authority

- The acquisition decision from the milestone decision authority.

There are likely to be several developmental test 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 operational test to obtain an authority to test, while interoperability testing may be a separate activity or in conjunction with the operational test. All of those events set the stage for the operational test to confirm that the capability is ready for fielding.

The timeline in Figure 4 depicts a mix of both policy and practice. For example, policy requires a test concept brief 120 days prior to operational test and test plan approval 60 days prior for programs on the T&E oversight list. In practice, operational test duration varies by system; some tests can exceed what is shown by months. Likewise, final evaluation report preparation varies, and the 60 days shown is probably conservative. Hence, the IOT&E test execution window can exceed six months. Figure 4 is not intended to imply that either interoperability or information assurance certification occurs within the time blocks shown; merely that the activities form an essential part of the IT T&E strategy and must be planned and resourced accordingly.

As I've stated, 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 designated accrediting authority may deny operation on the 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

Figure 3. **T&E in the Systems Engineering "V"**

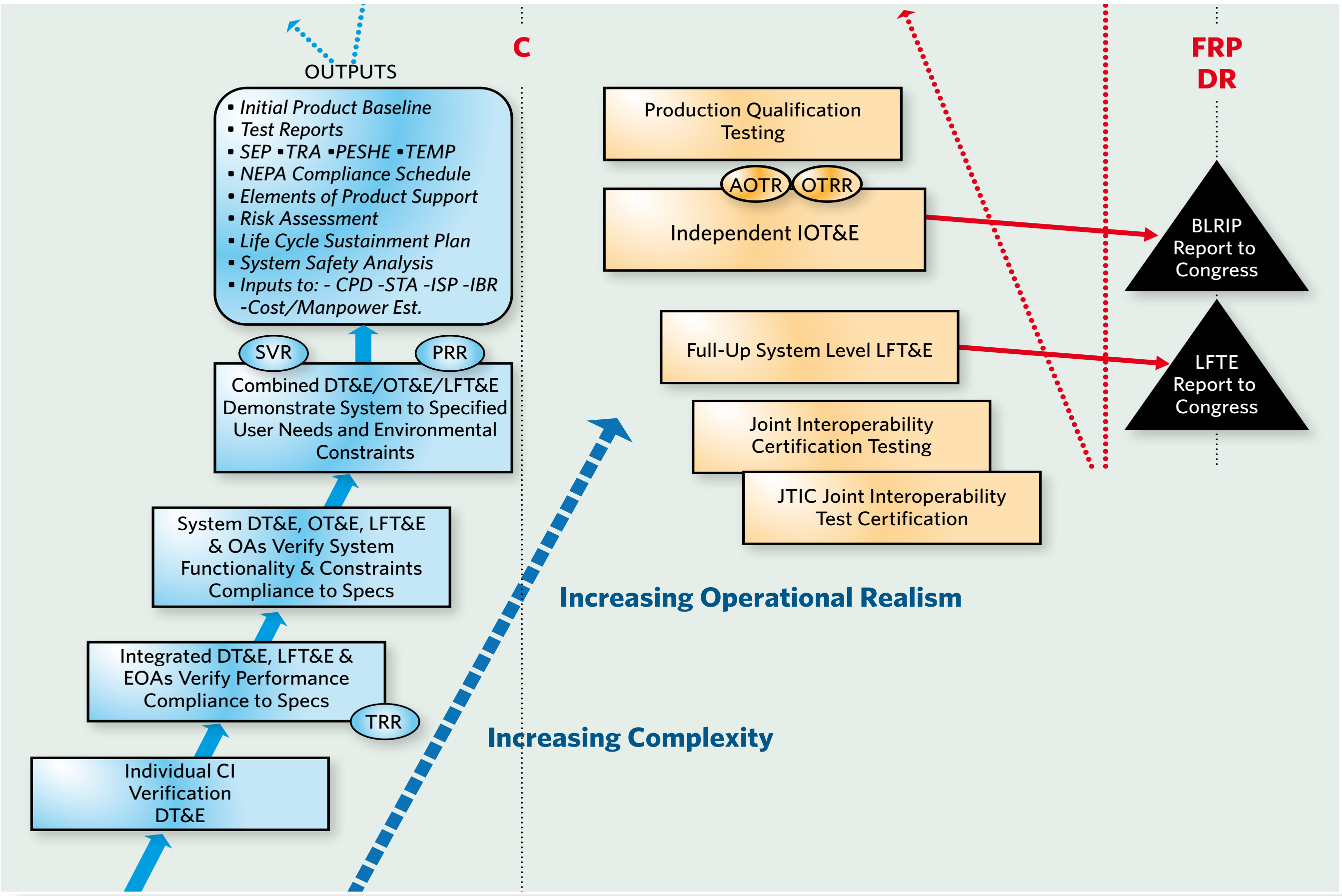
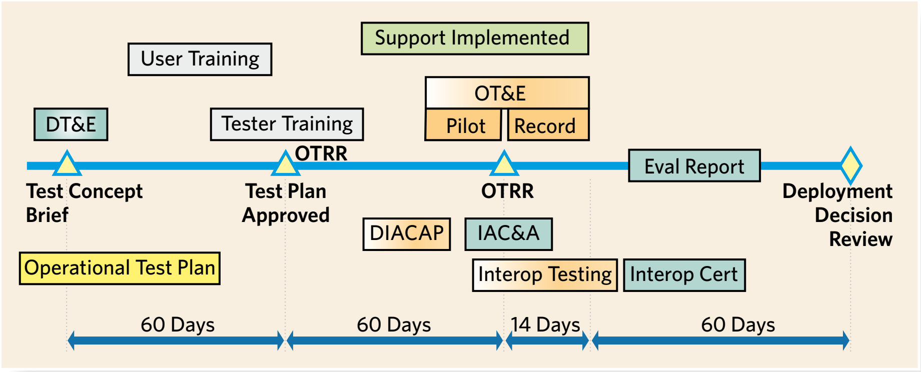

OUTPUTS
• Initial Product Baseline
• Test Reports
• SEP •TRA •PESHE •TEMP
• NEPA Compliance Schedule
• Elements of Product Support
• Risk Assessment
• Life Cycle Sustainment Plan
• System Safety Analysis
• Inputs to: - CPD -STA -ISP -IBR -Cost/Manpower Est.
C
SVR
PRR
Combined DT&E/OT&E/LFT&E Demonstrate System to Specified User Needs and Environmental Constraints
System DT&E, OT&E, LFT&E & OAs Verify System Functionality & Constraints Compliance to Specs
Integrated DT&E, LFT&E & EOAs Verify Performance Compliance to Specs
TRR
Individual CI Verification DT&E
Production Qualification Testing
AOTR
OTRR
Independent IOT&E
Full-Up System Level LFT&E
Joint Interoperability Certification Testing
JTIC Joint Interoperability Test Certification
FRP DR
BLRIP Report to Congress
LFTE Report to Congress
Increasing Operational Realism
Increasing Complexity

Figure 4. **Test Execution Window**



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 program manager responsible for interoperability testing or is the operational test agent? Who approves the interoperability test plan? Should the Joint Staff, J6, sign the T&E master plan?

Interoperability is a key performance parameter, 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 Project referred to the interoperability KPP as one "for which there is no method of testing." From August 1999 to present, the interoperability KPP has been defined and redefined four times.

The Interoperability KPP (I-KPP) was first introduced in the Requirements Generation System in the August 1999 issuance of CJCSI 3170.01A. The methodology for assessing the I-KPP based on "information exchange requirements" followed in the May 2000 CJCSI 6212.01B. The Joint Staff canceled the Requirements Generation System 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 information exchange requirements to technical compliance attributes such as the "Net-Centric Operations and Warfare Reference Model," "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 Net-Centric Operations and Warfare Reference Model, and introduced Global Information Grid Enterprise Service Profiles—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 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, IA is governed through the DoD 8500 series and the CJCSI 6510. 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 designated accrediting authority sign the T&E master plan?

DoD implemented IA certification and accreditation 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 Net-Ready KPP. In July 2006, the ASD(NII) canceled DITSCAP, issued interim guidance, and then in November 2007, the 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 Net-Ready 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, issued the Policy for Operational Test and Evaluation of Information Assurance. The policy required the independent operational test authorities 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 [*test team authorized to conduct threat-based computer network operations*]" 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 certification and accreditation process, each information system has a designated accrediting authority appointed by the component head or the mission area principal accrediting authority. The designated accrediting authority 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 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 Defense Science Board Task Force observed that one cause of redundant testing is that "Testing, evaluation, and certification that are performed by one Service or one agency are most often not accepted by other Services or agencies." The Defense Science Board therefore recommended a new mandate: "Test by one, accept by all." On July 23, 2009, DoD principal accrediting authorities signed a policy for reciprocity to accept each other's security assessments (DoD Memorandum, Subject: DoD Information System Certification and Accreditation Reciprocity). The policy is a very positive step towards 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 developmental test/operational test (refer back to Figure 2). 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 is accomplished prior to operationally fielding a release." That 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 test, evaluation, and certification activities), then the desired 18-month release cycle may in reality approach 24 months. More important, however, is that 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 where 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.

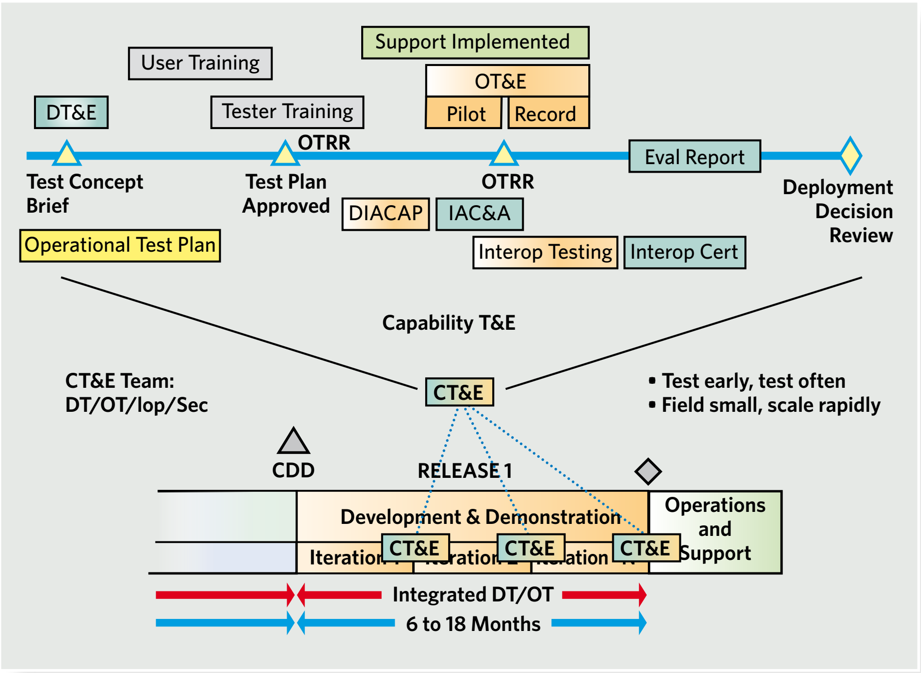
Towards an Agile IT Acquisition and Test, Evaluation, and Certification System

The preceding sections have made the case that acquisition of information technology in 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 test, evaluation, and certification processes that ensure capabilities are effective, suitable, interoperable, and secure.

From beginning to end—requirements definition; capability development; test, evaluation, and certification; governance; and operations—the department lacks agile processes designed for IT. An agile IT acquisition model must begin with

The fundamental reason the Defense Acquisition Management System model does not work well for IT capabilities is that we typically want a very short time between user need definition and initial operational capability.

Figure 5. **Agile T&E**



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 life cycle (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/Defense Business System Management Committee governance bodies) to provide a single governance and decision support framework to enable faster delivery of business capabilities" (see <http://www.bta.mil/products/bcl.html>). The BCL leverages the Enterprise Risk Assessment Methodology "to reduce systemic risk and support informed decision making" (see <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 appearance of being a one-way path, the agile development life cycle is more iterative and less sequential. The test, evaluation, and certification 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 developmental test, operational test, interoperability, and security test activities into a comprehensive test, evaluation, and certification 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 5 depicts the test, evaluation, and certification paradigm shift. That can be accomplished only through a highly collaborative process that is responsive to changing requirements priorities and developer agility. Essential to the approach will be early and continuous involvement from the user community. In the 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.

Implement an Agile Process Now

Information technologies evolve rapidly, as is abundantly evident in the commercial sector. As 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.

The author welcomes comments and questions and can be contacted at steven.hutchison@disa.mil.