INDUSTRY TASK FORCE REPORT

2010 NATIONAL DEFENSE APPROPRIATIONS ACT
SECTION 804

Industry Perspectives on the Future of DoD IT Acquisition

June 6, 2010

The Association for Enterprise Information
An Affiliate of the National Defense Industrial Association

2111 Wilson Boulevard, Suite 400
Arlington, Virginia 22201
www.afei.org

2111 Wilson Blvd., Suite 400 • Arlington, VA 22201-3061 • www.afei.org

Mr. Timothy Harp
Deputy Assistant Secretary of Defense
C3ISR and IT Acquisition
Assistant Secretary of Defense, Networks and Information Integration
6000 Defense Pentagon
Washington, D.C. 20301-6000

June 6, 2010

Dear Mr. Harp,

I am pleased to submit this product of the AFEI Industry Task Force assembled to address industry perspectives on new acquisition processes for information technology.

Industry believes that the most difficult challenges lie with changing how Government views IT acquisition and the processes used to define and buy essential capabilities. The purpose of this work is to offer unsolicited views of a team of industrial and academic experts to inform the OSD report to Congress on "Implementation of New Acquisition Process for Information Technology" mandated by section 804 of the 2010 National Defense Appropriations Act (NDAA).

You will notice that many people made contributions to the creation of this report, including members of the military and civilian employees of DoD. We felt it was crucial to add their perspectives to those of industry and academia because, simply put, we are all in this together. AFEI is grateful for the efforts of those who edited and contributed to the report, as well as those who participated in the many discussions.

The Association and its members are pleased to support the efforts of the DoD CIO and defense community, and look forward to continuing to develop the concepts, ideas and recommendations contained in the document.

Respectfully,

David E. Chesebrough, P.E.
President

(This page intentionally left blank)

Acknowledgements

AFEI wishes to acknowledge the contributions of all those who made their time and skills available to complete this project. In particular, AFEI thanks Chris Gunderson, NPS, Tim Pavlick, IBM and Dave Mayo, Everware CBDI who provided their insights and expert coordination, guidance and editorial knowledge.

AFEI also acknowledges the invaluable contributions of the major contributors to the report, who spent a great deal of time and energy in discussing and debating the issues.

There were many others who participated in some aspect of the development of this project, and AFEI thanks them and their organizations for their support.

Finally, AFEI thanks the Office of the Assistant Secretary of Defense (Networks and Information Integration) / Chief Information Officer, DoD for the opportunity to provide and industry perspective on this critical transformational initiative.

AFEI is deeply indebted to all of the organizations who willing provided their best talent to participate in developing this report. This is an excellent example of the results that can be achieved when industry and government enter into collaborative efforts for the good of the community.

(This page intentionally left blank)

INDUSTRY TASK FORCE REPORT

2010 NATIONAL DEFENSE APPROPRIATIONS ACT SECTION 804

Industry Perspectives on the Future of DoD IT Acquisition

Submitted to

Mr. Timothy Harp
Deputy Assistant Secretary of Defense
C3ISR and IT Acquisition

May 25, 2010

Abstract

The purpose of this work is to offer unsolicited views of a team of industrial and academic experts to inform the OSD report to Congress on "Implementation of New Acquisition Process for Information Technology" mandated by section 804 of the 2010 National Defense Appropriations Act (NDAA). This report focuses on required changes in behavior and pragmatic means to incentivize those behavior changes within the realistic constraints of the "as is" Defense acquisition landscape.

The over-arching recommendation is to institute continuous, iterative, development, test, and certification processes that drive the commercial IT state-of-the-art to deliver more trusted, standard, off-the-shelf building blocks. In this model the ability to "bundle" trusted components becomes a critical unit of production. The DoD should begin implementation of the improved IT acquisition process immediately by chartering a number of independent, three-year pilot projects who's sponsors are incentivized for their own reasons to develop enterprise capability. These pilots will lead to a self-sustained persistent Development, Test, and Certification environment associated with a flourishing marketplace of "net-ready" re-useable components.

Editors, Contributors and Participants

Editor:

Chris Gunderson, Naval Postgraduate School on behalf of Joint Interoperability Test Command

Co-editors:

Dave Mayo, Everware CBDI

Dr. Tim Pavlick, IBM Federal

Major Contributors:

Frank Alvidrez

Rick Boike, Naval Undersea Warfare Center Division Keyport

Paul Brubaker, Cisco Systems, Inc.

Rex Buddenburg, Naval Postgraduate School

Dr. Brad Cox

Dr. Peter Denning, Naval Postgraduate School

Jessie Fewell, Program Management Institute

Dr. Rick Hayes-Roth, Naval Postgraduate School

LT Dennis Holden, USN, Naval Postgraduate School

Dr Suzette Johnson, Northrop Grumman

Mary Ann Lapham, Software Engineering Institute, Carnegie Mellon University

Angela Llamas-Butler, Software Engineering Institute, Carnegie Mellon University

David Minton, Raytheon

Maj Brian Rideout, USMC, Marine Corps Systems Command, Program Manager Intelligence

Rick Toliver, Teledyne Solutions

Dr. Dennis Volpano, Naval Postgraduate School

Rob Walker, Oracle

Lt Col Dave Yost, USMC, Marine Corps Combat Development Center

Editors, Contributors and Participants

Participants:

Rick Brennan

Kelly Brown, EM Solutions, Inc.

Mike Carrucci, HandySoft

Richard Cheng, Excella

Dave Huff, USN

David Janot, DMO Acquisition Manager

Dr. Marv Langston, Marv Langston Associates

Tony Lengerich, Oracle

David Morsberger, Northrop Grumman

Dennis Sawyer

Vince Snyder, Lockheed Martin

Matt Vandergraf, Deloitte

Lt Col Dan Ward, Chief, Acquisition Innovation, Acquisition Chief Process Office (SAF/AQ)

Table of Contents

Table of Contents (cont'd)

AFEI INDUSTRY TASK FORCE REPORT RE 2010 NATIONAL DEFENSE AUTHORIZATION ACT SECT 804

Executive Summary

This "Task Force 804" (TF 804) report, prepared by a team of industrial and academic experts, aims to inform the OSD report to Congress on "Implementation of New Acquisition Process for Information Technology" mandated by section 804 of the 2010 National Defense Authorization Act (NDAA.) The authors recognize "Einstein's Dilemma," i.e. "the same thinking and processes that created your problem won't solve it." Therefore, this report focuses on required changes in behavior and pragmatic means to incentivize those behavior changes within the realistic constraints of the "as is" Defense acquisition landscape. Generally, we propose a *framework for transformation* of the Defense Enterprise IT lifecycle and acquisition. The framework requires a combination of architected and agile approaches. A complicating issue is that the engineering and architectural discipline of IT generally is less mature than other disciplines. While IT professionals agree that their objective is to deliver *trusted*, standard, off-the-shelf-components -- to use the construction industry as a metaphor -- the state-of-the-art in software engineering is still largely artisan "mud brick" components rather than factory-spec commodity "standard bricks." With that background, the report suggests how to implement the findings of the Mar 2009 Defense Science Board (DSB) Report on Department of Defense (DoD) Policies and Procedures for the Acquisition of Information Technology via four imperatives mandated by Sect 804: *(1) involvement of the user; (2) rapidly executed increments* (3) *evolutionary approach; (4) modular, open systems.* Our approach is to evaluate each of these imperatives in context with the following implementing tools and considerations: (a) *requirements and capabilities;* (b) *testing*; (c) *information assurance (IA) (including, but not limited to, security)*; (d) *architecture and engineering*; (e) *culture and behavior*; and (f) governance, *legal issues and* contracting. The over-arching recommendation is to institute continuous, iterative, development, test, and certification processes that drive the Commercial IT state of the art to deliver more trusted, standard, off-the-shelf building blocks. In this model the ability to "bundle" trusted components becomes a critical unit of production. Specific recommendations are summarized as follows:

- Approach IT acquisition strategy as continuous "Tech Refresh" throughout system development and lifecycle. Buy-down risk with as much pure COTS[1] as possible.

[1] "Pure COTS" means truly out-of-the box functionality together with lifecycle support.

- Contractually require providers to nurture "Beta Development Communities[2]" among operational customers.

- Enforce two basic network architectural principles: (1) All devices must be routable nodes of Local Area Networks (LAN); (2) All LANS must be routable nodes on Wide Are Networks (WAN).
- Invest in basic research to close COTS gaps re Defense Enterprise requirements and "open source" the results. In particular:
    - Fund COTS IT vendors to develop improved Information Assurance (IA) and Semantic Interoperability (SI) solutions
    - Provide developed GOTS IA and SI components as Government Furnished Equipment (GFE) to industry at large.
- Develop automated test, certification, and accreditation (C&A) for IA and Interoperability process based on modular risk vs. reward trust model (evaluate relative need-to-protect vs. need-to-share.) Provide reusable end-to-end security tools, templates, and policy that allow quick introduction and use.
- Include continual post-deployment testing as an aspect of life cycle support.
- Categorically define "open, modular, scalable, architecture" via a suite of "enterprise[3]" level requirements and associated objective value-based metrics for desired operational outcomes, need-to-know vs. need-to-share, information processing efficiency, and acquisition process efficiency across an enterprise system. Use these objective metrics as basis of source selection and contracting; demand creative contracting per acquisition imperatives!
- Create a persistent, virtual, online, service-based, enterprise Development, Test, and Certification environment including enforced cross-program workflow, i.e. federated governance.
- Empower engineering-level government officials as Enterprise Chief Information Officers and Enterprise Chief Architects, with mandate, training, and scope-of-authority necessary to deliver enterprise capability rapidly, innovatively, and incrementally.
- Create a living executive dashboard that informs continuously evolving acquisition policy per all the above.

These recommendations apply equally to all Defense activity that involves IT. Even programs that aim to develop platforms, (in this sense "platform" means military vehicles like missiles, ships, tanks, etc.) weapons, or sensors over long time frames must continuously evolve their IT components to avoid becoming obsolete before Initial Operating Capability (IOC). The DoD should begin implementation of the

[2] "Beta development communities" are technically savvy operational users who are included in a continuous, development, test, and evaluation feedback loop.

[3] "Enterprise" in this case means agreed collaboration to achieve mutual objectives across communities of independent verticals.

improved IT acquisition process immediately by chartering a number of independent three-year pilot projects who's sponsors are incentivized for their own reasons to develop enterprise capability. These pilots will lead to a self-sustained persistent Development, Test, and Certification environment associated with a flourishing marketplace of "net-ready" re-useable components. New policy and training should follow observed successes in this pilot initiative. New legislation should learn from the unintended consequences of previous legislation such as Goldwater-Nichols, Clinger-Cohen, and FY07 NDAA re Major Automated Information System (MAIS) reporting. These laws have led to de-incentives for innovative behavior, and incentives for increasing bureaucracy. New legislation should repeal MAIS reporting requirements and incentivize the desired innovative, risk-accepting, behaviors associated with successful commercial IT practitioners. In particular, it should automate oversight processes, define and mandate an enforceable enterprise-enabling innovative role for government acquisition professionals, eliminate bureaucratic overhead, and mandate and reward specifically defined better-speed-to-better-capability.

INTRODUCTION

Section 804 of the 2010 National Defense Authorization Act (NDAA) requires Office of the Secretary of Defense (OSD) to report how it will implement imperatives for improving its approach to acquiring Information Technology (IT). This "270 Day Report" is due in July 2010. The Assistant Secretary of Defense for Network Information Integration SD (NII) action officer for this report encouraged the Association for Enterprise Information (AFEI) to facilitate a consolidated industrial input. Accordingly, AFEI chartered TF 804 to collect, analyze, and organize good ideas from government, industry, and academic experts.

This "Task Force 804" (TF 804) report suggests strategy and tactics for improving Defense Information Technology acquisition per the tasks set forth in section 804. It represents an open, frank, and focused dialog across a broad landscape of industrial, academic and government experts in various aspects of the problem and solution space. It is based on close study of both past failures and successes in both government and industry.

Clearly, the Defense Community's progress toward delivering on its Global Information Grid (GIG) "netcentric" vision is woefully unsatisfactory. Watchdog reports have documented how Defense program after program fail to implement open, modular, enterprise IT capability as a result of the slow, serial, monolithic, bureaucratic, Defense acquisition process. The same reports inevitably suggest that success requires more agile, innovative, evolutionary behavior. However, attempts to implement that behavior to date have inevitably failed to address "Einstein's Dilemma," i.e. that the same process that created a problem won't solve it. Einstein would say that trying to implement agile, innovative, evolutionary, behavior with a ponderous, risk-averse, serial process is tantamount to insanity.

On the other hand, history proves that cultures don't adopt new behaviors or implement new processes simply because it is the "right thing to do". Inevitably, behaviors change in cultures because new processes make it obviously easier for practitioners to achieve greater success -- *as they understand success*. In other words, the incentive for improved behaviors must be self-evident in the new process.

That said, the discipline of IT architecture and engineering (especially software architecture and engineering) is relatively immature compared to other disciples. For example, modern construction is based on architecture that employs *trusted* building materials, like standard bricks, steel beams, etc. "Trust" in the components is key. Trust comes from testing and certification. In more primitive mud brick construction, artisans make building materials such as bricks from raw materials, like mud, found nearby. Mud brick architecture is all but gone today because without testing and certification, homeowners, mortgage brokers, and safety inspector can't know if those mud bricks are really safe. Pre-brick architecture is the cave man approach that predates using components in

construction at all. While IT professionals agree that their objective is a trusted "standard-brick" approach, the state-of-the-art is still more mud brick than standard brick, and even includes quite a bit of the cave man approach.

Accordingly this report: (1) identifies the IT acquisition process changes necessary to address the NDAA 2010 Section 804 imperatives, and (2) explicitly explains how to incentivize the necessary behavior changes. The following assertions generally frame the basis for both categories of recommendations:

> ***Policy is not an excuse*** for failure. Acquisition practitioners must deliver targeted outcomes within the existing policy constraints. That said, policy seldom, if ever, creates new behavior out of whole cloth. Rather, successful policy follows, and seeks to nurture and extend, observed good behaviors in practice. Policy makers should monitor success on the ground and evolve policy that will extend and expand the success cases.
>
> "Agile", SOA, "cloud", "open technology development" and other modern Internet paradigms and ***technology will help if applied as means to an end, not as an end*** in and of themselves.
>
> That said, there are ***two technology gaps*** on the critical path to Defense enterprise success:
>
> > ***Information Assurance (IA).*** The commercial state of the art is medium assurance at best, does not scale to the tactical edge, and does not support dynamic, risk/reward-based need-to-protect vs. need-to-share information exchange policy. We need tools that can federate across stovepipe networks on demand, i.e., dynamically create and collapse high assurance private network enclaves. We must build in whatever security we require. It is too hard and too expensive to bolt on later.
> >
> > ***Semantic Interoperability (SI)***. "Semantic Web" is immature. There are no generic commercial tools that manage the "information overload" issue, i.e., deliver critical information to critical nodes at critical times. Google is the metaphorical state-of-the-COTS-art. We can't expect warfighters at the pointy-end to "Google" under fire.
>
> Like it or not, given limited resources and the staggering rate of change in the IT landscape, the only possible path to success is for the Defense community to ***join and invest in the COTS ecosystem as a peer***. COTS-based development, or even buying COTS, is not the same thing as joining and investing in the COTS ecosystem[4].

[4] A peer in an ecosystem leverages its resources to deliberately influence market evolution in directions favorable to its goals.

You get what you measure and pay for. The Defense Enterprise must ***measure and pay for better-speed-to-better-capability***. Contract vehicles and processes must incentivize the risk-accepting behaviors, and innovative outcomes we seek. Today's defense contracts do not; nor are Defense acquisition professionals taught, or incentivized, to innovate. Program Managers, must be held accountable, and control the resources and tools (e.g. contract vehicles) necessary, to deliver better-speed-to-better-capability.

BOTTOM LINE

1. Applicable Categories of IT Acquisition

The recommendations distilled from this report's analysis apply equally to all Defense activity that involves IT. Even programs that aim to develop platforms, weapons, or sensors over long time frames must continuously evolve their IT components to avoid becoming obsolete before deploying.

2. Implementation Schedule

"Best practice," useful standards, and good architecture all follow repeated success on the ground. So, therefore, does good policy. Hence, the best way to implement these ideas for improved IT Acquisition is to ***immediately and continuously seed multiple small pilots****, expecting many to fail, and with a view toward learning from both successes and failures. This effort must include a "hands-on" Chief Architect as defined in subsequent paragraphs who is empowered to link the piloted capabilities across an enterprise composed of the pilot projects.*

These multiple pilots should share, as Government Furnished Equipment (GFE), a persistent, virtual, environment for parallel development, testing, and certifying (D,T&C) capability. This "Persistent Environment" (PE) should provide, as GFE, use cases that include mission threads; associated metrics, models and simulations; and any Software Development Kits (SDK), APIs, etc, necessary to configure in the online infrastructure.

This PE approach is an industrial "e-business" best practice that includes working bottom up from customer requirements and horizontally across funding verticals. Defense leadership should treat creation of the PE as an aspect of the series of pilot projects, i.e. creating and participating in the PE is an Enterprise Requirement for all participating pilots.

The PE must include access to test and certification authorities with a mandate to adjust their tools and processes to facilitate measurably better speed to measurably better capability. Likewise, operational *beta developers*, i.e. front line operators motivated to help develop better IT tools, must participate. The PE should include Business Process Management (BPM) tools and processes that enforce and facilitate productive cross-program collaboration and interaction with customers and authorities: in other words, an *IT-value-delivery-chain.* Trainers and

educators should monitor activity, distill best practice, and develop curricula and tools.

These pilots should involve multiple independent activities all of which recognize the need for shared, open, scalable, assured, interoperable IT infrastructure. Each of these activities must identify small increments of capability it intends to field and must have sufficient scope-of-authority and resources to deliver. The independent activities should "meet" virtually for (say) quarterly bundling events together with test and certification authorities. These bundling events should generate Approved Products List (APL) and IDIQ contracts for reusable enterprise off-the-shelf components.

Participation in pilot projects should be broadly open to industry. Solicitations for participation should be simple explanations of the use cases and opportunities. Vendors should generally be self-funded beyond access to GFE because participation is both their opportunity to market their offerings and their channel to the Defense community market.

The pilot series should be funded for three years up front. The first bundling event should occur no more than ninety days after identifying the project leadership based on demonstrated aptitude for innovation, and providing the funding resources. Pilot annual deliveries should include, at minimum, the following:

Year 1.

- Online, distributed, D,T&C PE with managed workflow operational
- Net Ready Approved Product List (N-APL) established
- IDIQ contract(s) for Net Ready approved products in place
- Delivered increment(s) of off-the-shelf, customer-valued capability, certified in parallel for IA and interoperability
- More than one Designated Approval Authority (DAA) recognizes each other's accreditations, and share Authority to Operate (ATO) at some level across their network enclaves.
- Trainers, educators, and policy makers will have sufficient data to begin drafting useful directives and associated curricula.

Year 2.

- Draft policy captures observed best practices and associated success criteria, i.e. agile methods.
- Participants beyond the initial pilot members voluntarily employ the D,T&C PE

- Multiple DAAs recognize each other's accreditations and share ATO.
- Number of off-the-shelf products and services on the N-APL and available via IDIQ contract will have increased significantly
- Schoolhouses begin training, observed best IT acquisition processes

  Year 3.

- DT&E PE is self-sustained
- Several programs of record have delivered off-the-shelf customer-valued capability to the field
- Established policy streamlines Interoperability and IA C&A
- DAAs routinely share accreditations and ATO
- A growing market ecosystem continually consumes government developed IP and returns increasingly robust COTS IT for Defense Applications
- Various major programs will use the tech refresh model to continually deploy customer-defined value to the Defense Enterprise throughout program lifecycle

3. Required Legislation

New legislation should learn from the unintended consequences of previous legislation such as the Goldwater-Nichols (G-N), and the Clinger-Cohen Act (CCA), For instance, G-N legally separated responsibility for defining system requirements from responsibility for acquiring systems. Acquisition activities report to civilian Defense leadership, i.e. the Service Secretaries; requirement development activities report to uniformed Defense leadership, i.e. the Service Chiefs. In retrospect, that separation is a counter-productive artificiality that adds layers of bureaucracy. By contrast, CCA is quite enlightened. Its language requires government IT activities to behave exactly like the best run industrial IT shops. However, the Defense Enterprise has chosen to implement CCA by requiring burdensome compliance documentation that clearly has nothing to do with commercial best practice. Hence, these laws have led to de-incentives for innovative behavior, and incentives for increasing bureaucracy. Meanwhile, in response to non-performance, Defense acquisition legislation tends to periodically add even more bureaucratic burdens. For example, the 2007 National Defense Authorization Act instituted: 10 U.S.C. Chapter 144A and Major Automated Information System (MAIS) Annual Reports piled on reporting requirements without addressing the core process and expertise issues.

New legislation should address the de-incentives by repealing 10 U.S.C. Chapter 144A and perhaps even repealing aspects of G-N. New legislation should clearly incentivize the desired innovative, risk-tolerant, behaviors associated with successful commercial IT practitioners.

In particular, the new law should eliminate existing known failure modes as follows:

- Automate all paper-intensive acquisition compliance processes. Any legislation that requires oversight reporting must fund the creation of the corresponding automated reporting tool kit. Reduce Defense acquisition policies into objective, testable, machine-readable, elements. All programs develop and deliver their acquisition documentation in machine-readable, searchable, cross-referenced, formats.

- Eliminate acquisition "overhead" processes, e.g. plans, requirements, studies, etc, that are excessively long, e.g. longer than twelve months, or expensive, e.g. cost more than 20% of the overall budget

- Empower government Chief Architects with actual control, i.e. full scope of responsibility and authority over resources for design, implementation process, and timetable. Include "capability actually delivered" as performance measure.

- Empower government CIOs and/or Program Executives, or whoever supervises the Chief Architect, with the full scope of responsibility and authority to empower the Chief Architect. Include "capability actually delivered" as performance measure

- Require all government IT acquisitions to be factored into cost centers with budgets less than or equal to $30M/year.

- Require all implementation processes to deliver objectively measured value in less than 18 months from project start, at no more than 30% of the total budget.

- Require all stakeholder, including test and certifying authorities, and especially end-users, to be involved throughout the entire acquisition process. This will require a different perspective and assignment model. Maybe even a different set of job categories.

- Require that any new development has to produce anticipated and measured increases in value – as defined by end users -- delivered, and must be as good as using the lowest risk, best alternative commercial off-the-shelf solution. Performance must be measured in terms of value delivered relative to annual total cost of operation.

Having eliminated the impediments that make incremental, evolutionary development difficult, the law should also mandate that the Defense acquisition process create an IT-value-delivery-chain as follows:

- At least, say, 80% of the value to be produced must be identified and associated with practical ways to measure it
- Total life cycle cost, amortized over each year, must be accurately estimated and measureable (up to 90%)
- Plans to produce systems must be justified in terms of estimated value to cost, appropriately amortized, and compared to the alternatives of status quo and best off-the-shelf commercial option.
- Off-the-shelf commercial options must be based on guaranteed Service Level Agreements (SLAs) and no more than 3-year contracts
- Measures of value delivered must be empirically based and updated at least annually
- Estimates of value expected must be empirically based and updated at least annually
- Terminate projects that do not achieve at least 40% of their estimated value to cost.
- Projects that achieve at least 100% of their estimated value to cost will receive performance bonuses

Analysis

1. Four Imperatives From the 2010 NDAA

Section 804 of the 2010 NDAA directs OSD to addresses imperatives distilled from the Mar 2009 Defense Science Board Report on IT Acquisition. Section 804 puts particular emphasis on four of those imperatives, namely: *(1)* early and continual *involvement of the user; (2)* multiple, *rapidly executed increments* or releases of capability; (3) early, successive prototyping to support an *evolutionary approach;* and *(4) a modular, open--systems* approach. These four imperatives are very closely related and describe mutually supportive aspects of IT acquisition associated with the most successful commercial enterprises. In order to focus its analysis and dialog, TF 804 identified a number of methods and objectives applicable to implementing the imperatives, namely:

(a) Requirements and capabilities – means to describe desired deliverables

in ways that leverage the innovative power and mercurial speed to capability of the IT industrial base;

(b) Testing – means to objectively measure IT performance in context with desired operational outcomes;

(c) Information Assurance, Security, Certification and Accreditation - rationale for need-to-protect vs. need-to-share decisions and ability to perform appropriate cross enclave information transactions accordingly;

(d) Architecture and Engineering – approaches to design and developing capability that achieves measurably better IT capability at speeds commensurate with the pace of commercial IT evolution;

(e) Culture and Behavior – the attitudes, values, and beliefs, and associated activity, necessary to overcome "Einstein's Dilemma" and sanely embrace new thinking and methods to solve problems created by old thinking and methods;

(f) Governance, Contracting and Legal Issues – means to synchronize and streamline workflow activities of autonomous IT acquisition stakeholders by decreasing bureaucracy and incentivizing collaborative engineering; statutory basis for not only allowing, but mandating, faster, better, and more cost effective IT acquisition processes; principle tool set, i.e. solicitation, source selection, and monetary incentives, optimized to catalyze all of the above methods and objectives;

This section of the TF 804 Report is an evaluation of each of the imperatives in context with each of the implementing methods and objectives.

2. Early and Continual User Involvement.

(a) Requirements and Capabilities

The best commercial businesses give good training and education to good people and empower them with responsibility and accountability to support corporate objectives. These businesses maintain continuously close contact with their customers. They identify a handful of key, objective metrics "on the ground" in customer space. They roll those customer-driven metrics into executive dashboards that continuously drive policy and programmatic decisions. The executive decisions are tightly coupled to customer outcomes through contract language such as Service Level Agreements and performance-based incentives.

Think of "requirements" in terms of both capital "R" formal system-level, Capability Requirements, and small "r" feature-level, capability requirements.

Capital "R" requirements might address the IT infrastructure platform; small "r" requirements might address evolving business applications.

Commercial best practices for collecting both classes of requirements include a combination of *Customer Outreach Teams* and *Beta Development Communities*. The Outreach Team is composed of members of the provider community. The Outreach Team interacts continuously with the customer community, training them on new features, and facilitating conversations over the art-of-the-possible. The Beta Development Community is composed of members of the customer community. These customers literally partner with the provider community, by accepting early delivery of not-ready-for prime time features, and helping to iron out the bugs. Inputs from Outreach Team and Beta Community inform the continuous incremental development process. Analysis of the evolution of small "r" capability requirements for continuously improving business process, informs the evolution of big "R" Capability Requirements for next-generation IT infrastructure.

Capability modeling should be the primary requirements analysis method. This method models capabilities from the business perspective ("what" in terms of outputs and outcomes, vs. "how" it is accomplished) including priorities, dependencies, and a hierarchy of abstraction levels. Business users are the subject matter experts for developing the capability model.

The Defense IT Acquisition process should develop methods, e.g. Beta Development Communities and Outreach Team equivalents, to continuously address small "r" business process improvements, and continuously roll the small "r" requirements into big "R" infrastructure improvements.

(b) Testing

"Agile" software development methods such as e.g., "Scrum" and "Extreme Programming," provide a microcosm of rapid incremental development performed in partnership with the user community. Significantly, a tight customer connection is central to "Agile" software development processes. "Agile" best practices include "user stories" to guarantee the continuing connection to the customers' perception of value and iterate on customer input even faster than traditional beta developer and marketing outreach processes. Agile approaches inevitably include test-driven development - designing the test of the desired software capability concurrent with designing the increment of code itself. Both test designs are tightly coupled to customer requirements via the user stories.

The Defense Enterprise concept of "Mission Threads," i.e. step-by-step descriptions of military tasks that lead to desired operational effects, is similar to the Agile user story. However, the Defense Enterprise process tends to collect and implement Mission Threads by slow, formal, bureaucratic methods that prevent direct interaction between developers and end users. In that sense, Mission Threads generally represent big "R" requirements.

The Defense IT Acquisition process should take a cue from the Agile software development community and implement means to informally collect "user stories" to capture Mission Thread perspective in near real time. These Mission Thread user stories should serve as the basis for testing and developing small increments of capability.

(c) Information Assurance (IA), Security, Certification and Accreditation

"Security" and "IA" are not equivalent. "Information security" refers to how information is protected against unintended disclosure. In industrial engineering parlance, the term "assurance" generally refers to the predictability of any intended outcome such as safety, security, or "availability" of a particular asset. Likewise, the term "Software Assurance" means not only that vulnerabilities are eliminated, but also that the software functions as intended. Consistent with this engineering context, the official Defense Enterprise definition of "IA" (per DODI 8500.01) addresses not only predictable information security -- i.e. authentication, non-repudiation, integrity, and confidentiality -- but also information "availability." However, in actual Defense Enterprise IT acquisition practice, "IA" has come to mean "locking down access to network resources." Early and continual user involvement can and should overcome that fallacy. *Namely, close interaction with the Defense Enterprise user community can provide the general rationale for making decisions that properly weigh both the need-to-protect information and network resources, vs. the need-to-share them, and enable appropriate cross-enclave information transactions accordingly. In this way Information Assurance contributes directly to Mission Assurance.*

The Defense Enterprise should require developers to collect and collate need-to-protect vs. need-to-share policy precipitated from their Mission Thread user stories.

(d) Architecture and Engineering

The iterative, agile solution development process requires continuous user participation throughout the entire architecture and engineering lifecycle.

Modern COTS World Wide Web applications include automated tools to seamlessly collect user inputs. For example consider how "Pandora Radio" (www.pandora.com) conveniently sketches users' music preference profiles, and then continuously collects user inputs to refine the profile. Consider how COTS software products automatically collect data from crashed applications, or how "Help" applications collect feedback.

Defense acquisition process should require developers and vendors to provide tools embedded in their customer-facing applications aimed at collecting feedback about effectiveness of networked military applications.

Some COTS tools go beyond collecting user feedback and make it easy for users to actually develop applications. For example, Google Gadgets provides extensive

training materials and intuitive tools for that purpose. The Defense acquisition process should include the same approach.

(e) Culture and Behavior

The Defense acquisition community has a hierarchal, stable culture that resists change,. Associated behaviors include: obsessing over who is in charge or "authoritative" in any activity; avoiding perceived risk by adding layers of bureaucracy to processes; owning infrastructure and other assets; and expecting top-down policy to drive desired changes in and of itself.

On the other hand, the COTS IT marketplace of Internet-enabled developers has an open-to-change, egalitarian, chaotic culture. Associated behaviors include; self-organizing, often without benefit of any recognized "authority;" avoiding perceived risk by failing cheap and quickly; sharing infrastructure; catalyzing (often unanticipated) changes in process by delivering novel capabilities.

Nothing is inherently better about one or the other of these cultures. Further, individuals or groups might belong to both Defense acquisition, and Internet cultures. However, the Internet developers' culture and behaviors are clearly more conducive to allowing users to participate directly and impactfully in IT acquisition. Therefore, the task is to incentivize government and industry acquisition professionals to unleash their Internet personas to create social networks that include both end-users and developers. Reward operators who provide feedback on systems they use. Navy SEALs do this well, possibly because they see the fruits of their labor in terms of rapidly fielded responses to their inputs. Other organizations are less incentivized because it takes something so long to get the new capability fielded that they don't see why they should even bother testing it.

Therefore, the Defense acquisition process should use the open COTS Internet-enabled marketplace to the maximum extent possible to engage military IT users. Reward operators who provide feedback on systems they used by making "contribution to business process improvement" an aspect of performance review.

Require contracting authorities to change their behavior in favor of enticing IT vendors and developers who have been historically reluctant to deal with the Defense acquisition culture and behaviors.

Policy makers should change their top town dictatorial behaviors in favor of encouraging developers to experiment together with the user community. New policies should follow repeatedly successful acquisition patterns and institutionalize demonstrated success.

(f) Governance, Contracting and Legal Issues

As discussed in the "Culture and Behavior" section above, *top down governance is not conducive to empowering the user community. Rather, senior policy makers should provide incentives in contract language that encourage collaborative self-governance among IT acquisition stakeholders such as developers, program managers, users, testers, and certifiers. Business Process Management (BPM) tools can help synchronize and streamline user input across IT programs and test and certification activities, thereby providing disciplined accountability to the self-governance model.*

Contracts should require vendors to nurture beta developers among the targeted operational communities. License agreements should leverage the vendors' customer outreach activity to drive vendor Internal Research and Development (IRaD) in favor of Defense customers. Officials should contractually require software providers to include automated tools to collect user inputs and facilitate beta development activity.

Use Level-of-Effort contracts with software vendors to perform government-funded S&T and RDT&E in partnership with the operational beta developers. Carefully manage government rights to created intellectual property in ways that encourage re-use, such as enterprise and open source licenses.

3. Multiple, Rapidly Executed Increments or Releases of Capability

(a) Requirements and Capabilities

First and foremost, The Defense Enterprise IT acquisition process must recognize that *requirements are for capabilities*! The Joint Capabilities Integration and Development System (JCIDS) was created on that premise. However, current IT acquisition behavior does not embrace that idea. The Defense solicitation process should stop over-specifying system specifications to a small pool of niche providers. It should, rather, offer robust models of desired capabilities to large communities of innovative, potential solution providers.

The 2009 DSB Report on IT Acquisition identifies speed-to-capability as a critical failing in the DoD acquisition process. On the other hand, the best COTS IT vendors succeed precisely because they are able to achieve rapid "speed-to-market" or equivalently "time-to-value." These firms recognize that sustainability in the marketplace makes it more important to get *some* new capability deployed -- on schedule and before the competition -- than it is to address 100% of the total customer requirement in any one delivery. Best practice includes disciplined development *processes* -- with associated metrics -- that enforce time-to-value requirements. Accordingly, the Defense Enterprise needs time-to-value *process-level metrics* that are consistent with industrial best practice, but are couched in the language of the JCIDS manual.

The time-limiting factor for fielding IT is, at least notionally, *Moore's Law,* i.e., a new generation of IT evolves every 18 months or so. The Defense Enterprise should consider that fact as a boundary condition, i.e., development and delivery together must be at least as fast as the generational rate of, say, 18 months.

The applicable FAR-friendly term is "Tech Refresh", i.e. continuously intercepting new technologies and retiring the superseded technologies. Well-run Defense programs use Tech Refresh as an approach to life cycle support that contrasts with traditional "maintenance." Traditional maintenance is about fixing broken things, and/or preventing things from breaking. Tech Refresh is about continuous business process improvement[5]. It requires well-defined objectives but not over-defined requirements for each increment; evolving requirements for subsequent increments/releases; mature technologies (often with short half-lives that require periodic refresh); and *early operational release* of capability from within an increment.

The Defense Enterprise can and should apply tech refresh across the entire acquisition process from pre-engineering Analysis of Alternates (AoA), to Engineering Design Modeling (EDM), to post IOC life cycle support. In all these cases, the core infrastructure already exists and the objective is to quickly and continuously deploy improved capabilities.

If "speed-to-capability" is the critical system parameter equivalent to the commercial "time-to-value" metric, then the Defense Enterprise needs a Key Performance Parameter (KPP) to capture speed-to-capability. The suite of traditional Defense Enterprise mandatory KPPs includes a Sustainability KPP (S-KPP) that addresses "readiness," i.e. continuing preparedness of the system to perform the mission. Traditional readiness depends on Reliability, Availability & Maintenance (RAM). The traditional S-KPP metric is called "Operational Availability" = (Up Time) ÷ (Up Time + Down Time). Operational Availability is a measure of system efficiency. Obviously, the more up time, the less down time, the greater the Operational Availability and the better the readiness… all good things. This metric is very useful because it is objective, measures a critical operational parameter (i.e. useful run-time), and allows for multiple options to achieve the targeted readiness.

The commercial "time-to-value" metric assumes that "sustainability" depends on a *reliable process to continuously refresh technology rather than on an ability to maintain legacy capability*. Likewise, the new paradigm for a Defense Enterprise Sustainability KPP (S-KPP) should be a process-level approach that equates sustainability with speed-to-capability.

[5] Not to say that traditional "fixing broken stuff" will go away entirely.

The new acquisition process level S-KPP should address "network readiness," i.e. the continuing preparedness of the network to perform its mission. Call this new S-KPP "Net Ready Availability." Net Ready Availability is analogous to Operational Availability, but treats the acquisition process itself as within the boundary of the system of interest. In other words, the acquisition process is the part of the overall "system" responsible for delivering continuous improvements, i.e. *sustainability* within the meteoric pace of commercial IT evolution. This is a new definition.

Like Operational Availability, we can define Net Ready Availability as a ratio of measured times, i.e., Net[6] Ready Availability = (Planned Development Time) ÷ (Scheduled Development Time + Schedule Over-run + additional test & certification time.) In this case, the times are associated with acquisition process efficiency. The less the schedule slips, the more test and certification is accomplished in parallel with development, the greater the Net Ready Availability… all good things. This metric is very useful because it is objective, measures a critical acquisition process parameter (i.e. useful build time), and allows for multiple options to achieve the targeted net readiness.

To apply the concept of Net Ready Availability, *programs first must recognize that they need to deploy capability quickly, say between 12 and 36 months. Programs then plan to deliver a capability portfolio scoped for delivery within that 12- 36-month window. (Note that a good strategy for achieving the deployment goals is to apply multiple Agile "sprints" within the time window, recognizing that while they will deliver working code, not all the sprints will deliver deployable code, but they all will deliver valuable lessons learned.) The scoping might allow for some newly invented components, but it will mostly require re-using pre-certified COTS or GOTS components.*

In this model, the acquisition strategy is to incentivize developers to re-use capability, i.e. bundle, pre-certified off-the-shelf components together to compose capability "stacks." The concept of bundling is key. "Bundle-ability" becomes the new unit of productivity, i.e. the more bundle-able, the more useful the artifact in question. Developers will deliver several interim test bundles within the capability deployment window, and adjust their schedules after each iteration. *Their goal is to deliver as much useful capability per cost as possible, but to meet delivery schedule at all costs*. If the schedule is at risk, *i.e.* the Actual Development Time increases, and the Net Ready Availability decreases. If Net Ready Availability decreases below some established threshold, the developers must adjust to meet the speed-to-

[6] The authors are deliberately co-opting the term "Net-Ready" as in "Net-Ready Key Performance Parameter." These same ideas apply to any software-intensive system, be they networked or not. Hence, "System-Ready" might be a more appropriate term.

capability imperative. Thus, programs avoid fielding obsolete capability. Figure (1) sketches how these ideas can be captured rigorously in an acquisition framework.

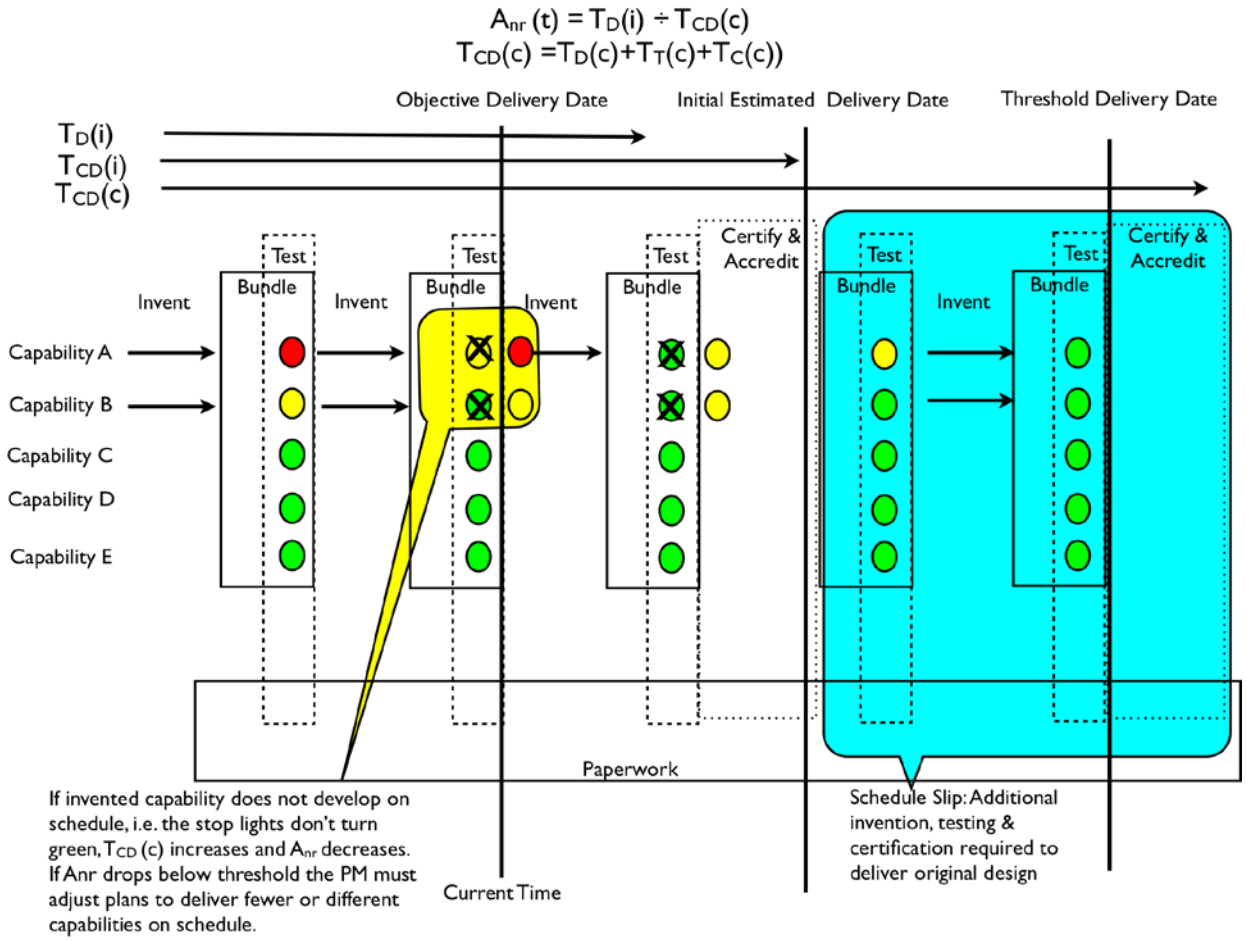

Figure 1: Net-Ready Availability" (A_{nr}) is based on speed-to-capability. A_{nr} compares initially scheduled development time (T_D) to the current estimate of capability deployment time (T_{CD}). T_{CD} is equal to T_D + any additional time required for test (T_T) and certification (T_C). This approach considers the capability delivery date to be an aspect of the KPP with established objective and threshold values. A PM's strategy is to reduce risk to schedule by bundling only small increments of newly "invented" specialized capability with existing pre-certified off-the-shelf capabilities in frequent spirals.

(b) Testing

"Test-driven development" is a commercial best practice. This practice is especially associated with rapid incremental development approaches. It is, for example, part and parcel to Agile software development. In test-driven development developers first write a failing automated test case that specifies an improved feature, then they write code to pass the test.

The Defense Enterprise should mandate, test-driven development. It should

train its acquisition professionals how to perform test-driven development, and how to contract for its inclusion in programmatic Test and Evaluation Master Plans. This is a very big paradigm shift!

(c) Information Assurance (IA), Security, Certification and Accreditation

Test-driven development best practice includes doing disciplined "do-no-harm-to-the-enterprise" (DNH) testing before deploying software applications to the IT "platform" in question. The software assurance community has tools and procedures to test for vulnerabilities and user-defined functionality.

The Defense Enterprise should work with, and invest in, the software assurance community to streamline, automate, and institutionalize DNH testing within the IT acquisition process.

(d) Architecture and Engineering

The Defense Enterprise tends to equate IT "architecture" with *architectural artifacts* such as DoDAF views. "Enterprise Architecture" (EA) in the Defense Enterprise is generally an exercise in paper compliance with top-down theory-based policies about interoperability. In contrast, successful COTS IT firms think in terms of *Product Line Architecture* (PLA.) A PLA defines a relatively stable core IT "platform" upon which new features associated with a particular product offering are readily deployed. Industrial Enterprise Architecture (EA) is the technical effort required to develop PLA(s), and federate as necessary across the PLAs, to achieve measurable enterprise objectives.

Industrial experience confirms that the only way to develop winning EA, is to empower a qualified enterprise Chief Architect. In successful industrial organizations, Chief Architects are hands-on, detail-oriented, technical people. The Chief Architect is the engineer who can explain – and is responsible for -- how all the moving parts are going to work together, on time, on schedule, at cost. By contrast, people with the title "Chief Architect" in the Defense Enterprise tend to be policy writers with no direct involvement in IT acquisition.

Defense programs whose missions require federating with other programs should mutually empower a single Chief Architect to develop the appropriate PLA(s) and/or federate across PLA(s). The Chief Architect should be equally responsible to deliver value to each enterprise stakeholder, but must be allowed to make the enterprise-level trade offs. He or she must be empowered with sufficient scope of authority and resources to execute on his or her design.

Industrial best practice is to outsource muscle, not brains. Therefore, Defense Enterprise Chief Architects should be government employees certified as experts in

software project management[7]*. Accordingly, the Defense Enterprise should continuously recruit the best and brightest industrial IT architects to serve "tours of duty" as short term government officials and mentors to a new generation of government IT professionals. This will require the creation of new job categories in the services as most of them that were applicable were removed in the 80s and 90s – as these were not the "core" business of the military*

Clearly proper application of Service Oriented Architecture (SOA) can play a critical enabling role. Success requires using SOA with a canonical foundation (data and services). Configuration Management and version control become paramount – many basic services, composite services, SLAs, test data sets, etc. must be managed:

- Capture requirements as capabilities (the ability to accomplish something of value).
- Model Capabilities– capturing definitions, dependencies, decomposition/abstraction, priorities.
- Map capabilities to the services that implement them to provide guidance and traceability.
- Base Portfolio Management on capabilities rather than systems, with services (or software components) supporting capabilities across multiple applications/systems.
- Modify the SDLC to incorporate Twin Track Development – separate design/development/provisioning of services from the solutions that consume them.
- Manage them as independent (but related) functions.
- Create a layered architecture of services to organize and manage the relationships between services.
- Develop reference architectures by domain to jumpstart projects and promote consistency.[8]

Achieving continuous tech refresh across an enterprise composed of multiple semi-autonomous verticals requires synchronization of effort. "Business Process Management" (BPM) is the "best practice" used to implement collaborative

[7] The Defense Enterprise should require certified software project managers for all efforts estimated to exceed certain cost or criticality parameters, not just "Enterprise" projects. Experience successfully managing software development efforts to completion would be the essential qualification, but it would be combined with design, development, testing implementation and support experience as both a user and as a member of the development team.

[8] See the *Practical Guide to Federal SOA* for detailed specific guidance (http://smw.osera.gov/pgfsoa/index.php/Welcome)

engineering across verticals. BPM is a disciplined approach to identify, design, execute, document, monitor, and measure both automated and non-automated business processes to achieve consistent, targeted operational results that align resources to an organization's strategic goals. The best commercial firms use BPM to achieve the following objectives:

- Visualize processes and responsibilities to: standardize repetitive operations; reduce learning curve by minimizing ambiguity; crystallize accountability.

- Enforce critical business policies/rules to: control effective policy/rule changes instantaneously; minimize business risks from uneducated decisions.

- Automate labor-intensive and prone-to-err tasks to: improve the quality of service; reduce the cost / achieve better resource utilization; gain higher productivity.

- Make business operations agile to: sense what to improve to gain competitive advantages; apply changes from the market pressures quickly and properly; continue optimizing operations

Traditionally, tools to perform BPM are proprietary to a particular enterprise, or vendor solution and relatively inflexible. Modern SOA-friendly, web enabled approaches are non-proprietary and very flexible. Hence, these approaches are agnostic to the particular "best practices" and policy compliance requirement. The BPM instrumentation, compliance tools, and dashboards ride on top of any enterprise's choice of standard Internet tools. Tools allow leadership to create machine-readable policy statements and specify their preferred process models.

Defense Enterprise policy makers should implement and tune BPM tools to require compliance and collaborative processes -- such as technology demonstrations, T&E, and C&A -- to occur on-line virtually and in parallel across program boundaries.

(e) Culture and Behavior

Commercial culture is all about delivering the new product to market in time to win competitive advantage. Defense acquisition culture is all about complying with bureaucratic requirements and accruing budget. The Defense Enterprise should incentivize new product-to-market behaviors per the speed-to-capability KPP described in the preceding paragraphs and the contract language described in the following section.

The role of the government program manger must change its focus from prescribing the build procedures and managing the build to managing the nature of the capability. In a MILSPEC model the government prescribed the 'thing itself' and oversaw the building of it. Now the innovation, since it comes primarily from the commercial marketplace, comes to the Government already built. Hence the Government's role must change from 'build oversight agent' to a consumer of finished products. Since the Government desires to buy capabilities, the focus must change to defining the capabilities of the unit and its Qualities of service or Non-functional requirements. Another way to say it is: features plus an SLA that describes their operation. The Government should define the nature of the capability and how it should operate. Further, the Government should create market-based incentives to encourage commercial industry to deliver that capability. Once certified as "operating as designed" then the capability should become available on a standard contracting vehicle.

(f) Governance, Contracting and Legal Issues

Contractually require performers to apply test-based development. Consider contracting with Agile software developers to leverage their "user story" approach to capture user-defined informal mission threads in ways that drive rapid software development cycles.

Write policy that makes capability release schedule a priority over milestone sign off. Contractually bind funding to incremental delivery of capability per the S-KPP = speed-to-capability approach. Fully fund initial increment(s) and provide solid funding stream for next overlapping upgrade increment(s).

Base procurement source selection on the bidding solution providers' ability to credibly execute tech refresh throughout the entire acquisition process – analysis of alternatives, milestone engineering, and life cycle support. The overriding metric should be capability per cost per time increment.

4. Early successive prototyping to support an evolutionary approach

(a) Requirements and Capabilities

In industrial best practice, "rapid prototyping" is a process to quickly turn an idea into reasonably well functioning IT, so that potential early adopting customers can evaluate it and provide feedback. Defense Enterprise acquisition policy pays lip service to this commercial approach to rapid prototyping by ostensibly favoring "evolutionary acquisition" and "rapid spiral development." However, *successful commercial practitioners provide the following to their developer communities:*

- *Low barrier to entry to on-line, distributed, network development environment.*

- *Approved modular approach to test, certification, and accreditation concurrent with prototyping effort.*
- *Well-defined, pre-approved, enterprise PLAs and associated furnished SDKs.*
- *Well-defined requirements for federation among PLAs, and associated furnished SDKs.*
- *Easily accessed catalogs and vehicles for consuming approved plug and off-the-shelf offerings.*

If the Defense Enterprise hopes to duplicate the scale of commercial success with rapid prototyping, it must likewise satisfy this list of developers' requirements.

(b) Testing

JCIDS mandated a change from "system-based" to "capability-based" requirements, e.g. enterprise-wide information sharing infrastructure rather than proprietary domain-specific systems. However the Defense Acquisition doctrine for testing is still designed to evaluate systems, not enterprise capability.

For example, IA and interoperability are treated as stovepipe, serial, post-development compliance issues, rather than as a suite of integrated utilities that enable enterprise capability. By waiting until after the entire huge system is developed before certifying it for IA and Interoperability in turn, this serial system-centric approach precludes early release of capability within a development increment. It simply costs too much time and money for a program to go to the trouble to OPTEST, and then certify and accredit an incremental pre-IOC prototype for IA and interoperability.

To address this disconnect, the Defense Enterprise test model should enable the commercial enterprise app development within the reality of the Defense acquisition process as discussed in the "Open Modular Systems Approach" section on testing. The rapid prototyping test suite would be a federation of service architectures, readily accessible via single sign-on, with the following interoperable functions and characteristics:

- Testing-as-a-service, i.e. multiple tools that evaluate function, performance, vulnerability, security across a large, heterogeneous, networked, software-intensive, system of system
- Live, Virtual, and Constructive Models and Simulations of mission scenarios and metrics; Defense platforms, sensors, and weapons; realistic network characteristics.
- Plug and play middleware stack representing approved Defense PLA

(c) Information Assurance (IA), Security, Certification and Accreditation

The Defense Enterprise should apply high assurance (Common Criteria Evaluation Assurance Level (EAL) 5 and above) service architecture to build the IA components into the prototype development environment itself. Calls the collection of high assurance IA components the "Trusted Computing Base" (TCB). The TCB is a metaphorical "Trusted Enterprise Service Bus" (T-ESB) that choreographs the IA service sequences. The task is to design, test, and certify and accredit a TCB within the development, test, and certification environment. Given the existence of an accredited TCB as an integral component of the development environment, the successfully generated DNH test artifacts would provide objective documentation the IA pedigree of an artifact under test. The Defense Enterprise should use that documentation to streamline C&A, and enable cross-enclave Authority To Operate (ATO).

(d) Architecture and Engineering

Rapid prototyping is a key aspect of the tech refresh approach to architecture and engineering. The long pole for tech refresh via rapid prototyping is how to efficiently transition potentially useful inventions to adopted and sustained capabilities.

The commercial best practice re IT rapid prototyping, i.e. to support enterprise app development, is to front-end-load the on-boarding requirements. That is, the enterprise provides a rapid prototyping on-line development environment -- a metaphorical "sandbox" -- that simulates the operational environment. Developers can readily access the sandbox by agreeing to behave by certain rules of enterprise behavior with respect to intellectual property rights, security, profit sharing, standards, etc. Developers receive Software Development Kits (SDK) that align with the enterprise PLA and associated test and certification requirements. They are given access to cordoned network enclaves in which to invent their prototypes.

When developers believe their prototype inventions are enterprise-ready, they submit them for final on-line certification. Developers either receive certification, or feedback regarding required fixes, very quickly. Successful prototypes are thus quickly made sufficiently robust to, seamlessly transition to operations.

With respect to SOA, Prototyping applies at the service level as well as the solution (ie, application or system) level:

- Succession framework for moving services and solutions from prototype to production must be established.
- Apply the Pareto principle (20% of the development satisfies 80% of the (priority) requirements) and expand from there.
- Be ready to re-factor what is in production based on new capabilities to be added at each increment.

(e) Culture and Behavior

Defense acquisition policy pays lips service to "commercial best practice" and "evolutionary development" of IT capability. However, acquisition policy directives overwhelmingly focus on compliance reporting rather than actually institutionalizing commercial best practices within the Defense IT systems engineering process. In particular, the Defense acquisition policy directives do not provide tools or incentives to encourage innovative or enterprise behavior. Not surprisingly, programs deliver compliance artifacts that are typically expensive, take a long time to develop, are delivered serially, and are redundant across stove-piped funding activities.

Nevertheless, some defense community activities have succeeded at value-based evolutionary acquisition. According to the Federal Acquisition Regulations (FAR) "Acquisition" includes all the end-to-end activities associated with basic and applied research, developing, fielding, maintaining, and retiring equipment. Given that end-to-end landscape, successful value-based evolutionary acquisition among the defense community is most common during the post-IOC *maintenance* phase of an IT capability life cycle. In those cases, the government effectively peers with industrial providers to get good off-the-shelf value for its Operations and Maintenance (O&M) investments.

Defense Enterprise policy makers, trainers, and educators, should identify the best practitioners of tech refresh as an approach to post-IOC IT life cycle maintenance. They should work with those practitioners to distill their best practices, and turn them into pragmatic policies and training materials to address end-to-end pre and post-IOC acquisition

(f) Governance, Contracting and Legal Issues

In actual practice, an artificial difference between "tech refresh" and "development" of IT in government applications is the category of funding applied to each: O&M, and Research Development Test and Evaluation (RDT&E) respectively. By law, programs use RDT&E funds prior to Initial Operating Capability (IOC). They use O&M funds after IOC. However, programs frequently apply RDT&E funds to rapidly deploy COTS as a "stop gap" in response to program schedule slips prior to IOC. That fact proves that there is no legal barrier to using a COTS tech refresh

model to perform "development." Indeed, at least one major defense program, Acoustic Rapid COTS Insertion (ARCI) succeeded at that task as an overarching Acquisition Strategy.

Defense Enterprise policy makers, trainers, and educators, should study the success of ARCI to develop a suite of boilerplate acquisition artifacts designed to more effectively align S&T, RDT&E, and O&M investments in mutually supportive rapid prototyping.

5. A Modular, Open-Systems Approach

(a) Requirements and Capabilities

The requirement for a modular "open" systems approach is for a clear, objective, and testable definition of "open". "Open" and "interoperable" are closely related, perhaps synonymous, concepts. However, "interoperability" is a loaded term. The Defense Enterprise should consider the interoperability requirement, i.e. a notional Interoperability KPP (I-KPP,) from several perspectives.

Build-time interoperability is equivalent to how easily one component can "bundle" with others. For example Internet Explorer 8 (IE8) browser software is interoperable in build-time, i.e. bundles with, the Windows Operating System (OS). On the other hand, IE8 is not interoperable in build-time with the Mac OS. Apple's Safari browser bundles with Mac OS. The proprietary Safari and IE8 browsers, as well as the portable open source Mozilla browser, all comply with most of the same "open" industry software standards such as JavaScript. The usefulness of build-time interoperability depends on which application features are valued, as well as the targeted OS bundle.

Run-time interoperability is equivalent to how effectively one network resource can "mash up" with others. This definition, by including "effectively," considers that simply establishing communication is not equivalent to interoperability. Discoverability is clearly a necessary condition, but not sufficient to enable "effectiveness." Effectiveness depends on how well interacting resources put data in context to create *meaning* for a customer. The term "semantic" means "meaning." Hence, run-time interoperability is equivalent to *Semantic Interoperability* (SI). Semantically interoperable network resources, by definition, mine meaning from data, i.e. they mash up to create information value-delivery-chains.

For example, travelers using Mozilla, IE7, or Safari can discover online portals for airlines, rental car companies, and hotels. If the traveler wants to quickly plan and book a trip, generic "discoverability" of an unlimited number of potentially relevant data and services is not particularly useful. Discovering the Travelocity portal is more useful. Travelocity, by saving the traveler time and money, provides

a *value-delivery-chain* across the entire online travel enterprise. We can measure information value for the traveler, e.g., in terms of transaction time and cost avoided. Simply confirming that bit-level data transactions are possible does not provide that insight. Systems that put disparate data into sufficient context to decrease transaction time, or save money, are therefore measurably semantically interoperable with their client systems.

Lifecycle Interoperability is equivalent to how readily the networked enterprise can interoperate with emerging capability, i.e. evolve. An I-KPP that measures higher order *semantic* interoperability, rather than simply bit-level data standards, encourages people to create capabilities that can work with new ones. New capabilities will want to interoperate at increasingly higher levels of abstraction. Indeed, the entire history of computing shows that agility increases as the level of information model abstractness rises.

Compliance with enterprise system-level standards and specifications is a necessary condition for useful enterprise interoperability, but is not sufficient. Therefore, the I-KPP should include objective information value metrics and identify associated SLAs. The SLAs would link operations-level information value metrics to system-level standards and performance metrics. This approach is a "commercial best practice", and is consistent with CJCSI 6212.01C's requirement for "Operationally Effective Information Exchanges".

(b) Testing

In traditional interoperability testing, demonstrating ability of joint systems to communicate across specified point-to-point links was sufficient. It is less straightforward to define and test for interoperability across modern, software-intensive, many-to-many, routable networks and "service" architectures. After all, these networks and architectures are populated by overwhelming numbers of independent nodes operating simultaneously, and without benefit of circuit discipline.

Developing open modular system architecture requires an open modular approach to testing and certification. By definition, the architecture will categorically specify functions and constraints for included components and interfaces. The constraints on interfaces will define "open". *The Defense Enterprise test model must assess functional performance of candidate component solutions and their ability to plug-and-play usefully and securely across the open interfaces. The C&A model should likewise be modular. That is, candidate component solutions successfully tested as secure, useful, and open should be certified as such. Note that SOA lends itself especially well to this approach. SOA transactions can be orchestrated to consult dynamic security policies, and invoke high assurance IA services, via a*

Trusted Enterprise Service Bus[9], for example. This is not the way testing and C&A are performed in the Defense Enterprise today. Hence the Defense Enterprise test and certification authorities such as NSA, JITC, and DOT&E should work together to create and validate this new open modular model. The Defense Enterprise acquisition process should populate a continuously growing inventory of pre-approved components available conveniently via tools such as the GSA schedule and IDIQ contracts.

This approach is not the same thing as testing for conformance with a particular standard. Compliance with standards is not useful in and of itself. Compliance is useful only to the extent that it actually enables useful transactions. Hence a testable I-KPP must link objectively specified enterprise requirements to design choices and objective measures of both system performance and operational effectiveness. "Enterprise requirements" include -- among other things -- SLAs for providers and consumers of enterprise services. "Design choices" include -- among other things – picking which standards, and deciding how to implement them, in order to achieve the desired operational utility.

The need to pick and implement the right standards applies to the test mission as well as all other missions. With that in mind, *here are specific recommendations with respect to test infrastructure standards:*

- *Include test requirements as inherent elements in specification of functional capabilities.*

- *Include testing infrastructure (e.g., instrumentation points and test tools) as included deliverables within developed software.*

- *Add an "Instrumentation View" (IV) and a "Testing View" that shows the location and design of instrumentation points, along with the associated activity and flow diagrams for testing end-to-end capabilities to the suite of required architectural views.*

DoD should warranty the "monitoring-time" behavior. Monitoring & management of COTs is important to ensure the proper functioning, particularly as part of a COTs ensemble. The idea that vendors should provide "instrumentation visibility" is an important one. All responsible vendors design their software to do this or be subject to it. Government is very focused on run time standards, e.g, WS-I, however it is equally important and often under-looked are development-time and monitoring-time standards. UML & SysML are examples of dev-time standards. CBE & SNMP are

[9] This idea of high assurance SOA is consistent with the NSA GIG IA Architecture. Indeed, the NSA High Assurance Platform (HAP) program aims to make high assurance SOA practical and affordable, embedded in COTS solutions.

examples of monitoring-time standards, or protocols, that could be used to "instrument" run times. Naturally this "monitoring-time" activity must include configuration management.

(c) Information Assurance (IA) Security, Certification and Accreditation

Information assurance, i.e. the ability to make appropriate need-to-protect vs. need-to-share decisions, is a necessary condition for useful interoperability. In other words, IA is a principal enabler of trust. Trust is an essential quality of information value-delivery-chains. As a practical matter, networked components of an "enterprise" must share an "Authority to Operate" (ATO) in order to interact. Testing against universally agreed, "do-no-harm" and vulnerability criteria is the minimum requirement for achieving enterprise-wide ATO. Articulated need-to-share policy is the minimum requirement for managing trust across an enterprise network. NSA's GIG IA Architecture mandates this approach per its "Risk Adaptive Access Control" (RAdAC) policy. In short, I-KPP must assure that components can share essential information without exposing the enterprise to unacceptable risk.

Within the sphere of inherent information system interoperability lies the sphere of inherent information system security. The Defense Enterprise has tools and policy that addresses infrastructure protection. And by indirection, content security. But these tools are of limited scope -- single network segment or single system-high enclave. Reusable security tools that provide end-to-end security must compliment these tools.

Accordingly, the Defense Enterprise should require all its programs to develop clearly articulated need-to-protect vs. need-to-share policies and provide reusable end-to-end security tools and template policy that allows quick introduction and use. These policies and tools should form the basis of C&A per the previous paragraph.

(d) Architecture and Engineering

Successful e-businesses would likely agree with the following generic description of modular, open, enterprise, IT architecture:

- Federated, routable networks
  - Wired and wireless (radio)
  - Wide Area Networks (WAN) and Local Area Networks (LAN)
- Common Computing Environment (CCE)
- Interoperable, routable, computing devices
- Open standard generic software applications.
- Value added business applications

One obvious recommendation derived from this model is that the *Defense Enterprise should enforce a universal requirement that all programs that deliver*

network communications capability must make all IT devices routable nodes on LANs. Likewise all LANS must be routable nodes on WANS.

"Tiering" is another critical modularity concept. Tiering means that infrastructure must be segmented. "Cloud" models such as infrastructure-as-a-service, platform-as-a-service, software-as-a-service use virtualization technology to apply the tiering concept. The idea is to segment by functional layers & then build, test, certify, and execute SLAs within those functional areas.

However, beyond the obvious requirement for route-ability, and tiering, in terms of IT architecture and engineering "open" is a relative term. Interoperability is a design trade-off. Typically, interoperability comes at the cost of giving up specialized capability. Universal interoperability across all data, services, applications and systems is neither possible nor desirable. Any engineer's job is to make the trade offs necessary to build useful capability, on time, and at reasonable cost. The job of a "network interoperability engineer" is to build sufficient interoperability to satisfy pragmatic "enterprise" requirements for information processing. Specific "enterprise requirements" for information processing will drive specific I-KPP requirements.

Consider a commercial example. Both iPhone and Android are interoperable with 3G phone networks and with the Internet. The iPhone development platform is proprietary to Apple, but "open" to thousands of apps developers willing to comply with Apple's locked down interfaces. The Android development platform is open source. Therefore, not only is Android available to an unlimited number of apps developers, the Android development platform itself is open for modification by an unlimited number of developers. Both approaches have advantages.

Relatively more proprietary approaches tend to provide relatively more control. Assuming there is a central governing authority that can enforce the proprietary standards across the targeted developers' ecosystem, it may be in that authority's best interest to do so. Proprietary commercial solutions tend to be more expensive up front. Note that proprietary architectures may include open source components. Consumers of proprietary approaches may benefit from disciplined life cycle support models for both the proprietary and open source components.

Relatively more open approaches tend to encourage innovation across a broader group of developers. Hence, open source projects can be excellent research venues. Governance tends to be a meritocracy across a federation of the willing. No one is in charge. Open source software itself is free. However, developing it and maintaining it, is not. Organizations that intend to implement and sustain open source software must either invest to develop and maintain their own organic expertise, or contract for it.

(e) Culture and Behavior

Best business practice for members of any successful e-business -- whether for-profit or not-for-profit -- is to leverage economy of scale by not re-inventing any existing infrastructure components. Rather, they employ value-delivery-chains that continuously collect customer feedback and drive IT investments.

(f) Governance, Legal Issues, and Contracting

Defense Enterprise contracts should enforce requirements for routable network communications (all devices are routable nodes on LANS; all LANS are routable nodes on WANS.)

Defense Enterprise acquisition practitioners should exercise government rights to broadly distribute any Intellectual Property (IP) developed at government expense. Consider paying vendors to maintain developed IP under open source software licenses.

By definition, any "service" (electronic or otherwise) must provide value to the consumer. Therefore "providing value" should be enforceable via Service Level Agreement (SLA) whether applied to run time SOA or applied to IT managed service contracts. Well-formed SLAs, should, therefore, verifiably and contractually *assure* the existence of customer-defined *value delivery chains* across a virtual universe of possible transactions.

Accordingly, *Defense Enterprise acquisition authorities should develop boilerplate SLAs that link objective definitions of information system "interoperability" to objective definitions of desired operational outcomes such as Probability of Kill, planning cycle compression, reduced safety mishaps, reduced inventory in the supply chain, etc. Contracts should include requirement for continuous, tiered, testing throughout capability lifecycle to enforce these SLAs.*

Summary of Recommended Actions

The following specific recommendations are collected from the italicized paragraphs in the body of the report above:

"Best practice," useful standards, and good architecture all follow repeated success on the ground. So, therefore, does good policy. Hence, the best way to implement these ideas for improved IT Acquisition is to **immediately and continuously seed multiple small pilots**, expecting many to fail, and with a view toward learning from both successes and failures. This effort must include a

"hands-on" Chief Architect as defined in subsequent paragraphs who is empowered to link the piloted capabilities across an enterprise composed of the pilot projects.

New legislation should address the de-incentives by repealing 10 U.S.C. Chapter 144A and perhaps even repealing aspects of G-N. New legislation certainly should clearly incentivize the desired innovative, risk-seeking, behaviors associated with successful commercial IT practitioners.

The Defense IT Acquisition process should take a cue from the Agile software development community and implement means to informally collect "user stories" to capture Mission Thread perspective in near real time. These Mission Thread user stories should serve as the basis for testing small increments of capability.

The Defense Enterprise should require developers to collect and collate need-to-protect vs. need-to-share policy precipitated from their Mission Thread user stories.

Defense acquisition process should require developers and vendors to provide tools embedded in their customer facing applications aimed at collecting feedback about effectiveness of networked military applications.

Some COTS tools go beyond collecting user feedback and make it easy for users to actually develop applications. For example, Google Gadgets provides extensive training materials and intuitive tools for that purpose. The Defense acquisition process should include the same approach.

… Defense acquisition process should use the open COTS Internet-enabled marketplace to the maximum extent possible to engage military IT users. Reward operators who provide feedback on systems they used by making "contribution to business process improvement" an aspect of performance review.

Require contracting authorities to change their behavior in favor of enticing IT vendors and developers who have been historically reluctant to deal with the Defense acquisition culture and behaviors.

Policy makers should change their top town dictatorial behaviors in favor of encouraging developers to experiment together with the user community. New policies should follow repeatedly successful acquisition patterns and institutionalize demonstrated success.

…. senior policy makers should provide incentives in contract language that encourage collaborative self-governance among IT acquisition stakeholders such as developers, program managers, users, testers, and certifiers. Business Process Management (BPM) tools can help synchronize and streamline user input across IT programs and test and certification activities, thereby providing disciplined accountability to the self-governance model.

Contracts should require vendors to nurture beta developers among the targeted operational communities. License agreements should leverage the vendors' customer outreach activity to drive vendor Internal Research and Development (IRaD) in favor of Defense customers. Officials should contractually require software providers to include automated tools to collect user inputs and facilitate beta development activity.

Use Level-of-Effort contracts with software vendors to perform government funded S&T and RDT&E in partnership with the operational beta developers. Carefully manage government rights to created intellectual property in ways that encourage re-use, such as enterprise and open source licenses.

… programs first must recognize that they need to deploy capability quickly, say between 12 and 36 months. Programs then plan to deliver a capability portfolio scoped for delivery within that 12- 36-month window. (Note that a good strategy for achieving the deployment goals is to apply multiple Agile "sprints" within the time window, recognizing that while they will deliver working code, not all the sprints will deliver deployable code, but they all will deliver valuable lessons learned.) The scoping might allow for some newly invented components, but it will mostly require re-using pre-certified COTS or GOTS components.

The Defense Enterprise should mandate, test-driven development. It should train its acquisition professionals how to perform test-driven development, and how to contract for its inclusion in programmatic Test and Evaluation Master Plans. This is a very big paradigm shift!

The Defense Enterprise should work with, and invest in, the software assurance community to streamline, automate, and institutionalize DNH testing within the IT acquisition process.

Defense programs whose missions require federating with other programs should mutually empower a single Chief Architect to develop the appropriate enterprise PLA. The Chief Architect should be equally responsible to deliver value to each stakeholder, but must be allowed to make the enterprise-level trade offs. He or she must be empowered with sufficient scope of authority and resources to compose the necessary enterprise-level PLA.

Industrial best practice is to outsource muscle, not brains. Therefore, Defense Enterprise Chief Architects should be expert government employees. Accordingly, the Defense Enterprise should continuously recruit the best and brightest industrial IT architects to serve "tours of duty" as short term government officials and mentors to a new generation of government IT professionals. This will require the creation of new job categories in the services as most of them that were applicable were removed in the 80s and 90s – as these were not the "core" business of the military

Contractually require performers to apply test-based development. Consider contracting with Agile software developers to leverage their "user story" approach to capture user-defined informal mission threads in ways that drive rapid software development cycles.

Write policy that makes capability release schedule a priority over milestone sign off. Contractually bind funding to incremental delivery of capability per the S-KPP = speed-to-capability approach. Fully fund initial increment(s) and provide solid funding stream for next overlapping upgrade increment(s).

Base procurement source selection on the bidding solution providers' ability to credibly execute tech refresh throughout the entire acquisition process – analysis of alternatives, milestone engineering, and life cycle support. The overriding metric should be capability per cost per time increment.

If the Defense Enterprise hopes to duplicate the scale of commercial success with rapid prototyping, it must satisfy this list of developers' requirement:.

- Low barrier to entry to on-line, distributed, network development environment.
- Approved modular approach to test, certification, and accreditation concurrent with prototyping effort.
- Well-defined, pre-approved, enterprise PLAs and associated furnished SDKs.
- Well-defined requirements for federation among PLAs, and associated furnished SDKs.
- Easily accessed catalogs and vehicles for consuming approved plug and off-the-shelf offerings.

The Defense Enterprise should apply high assurance (Common Criteria Evaluation Assurance Level (EAL) 4 and above) service architecture to build the IA components into the prototype development environment itself. NSA calls the collection of high assurance IA components the "Trusted Computing Base" (TCB). The TCB is a metaphorical "Trusted Enterprise Service Bus" (T-ESB) that choreographs the IA service sequences. The task is to design, test, and certify and accredit a TCB within the development, test, and certification environment. Given the existence of an accredited TCB as an integral component of the development environment, the successfully generated DNH test artifacts would provide objective documentation the IA pedigree of an artifact under test. The Defense Enterprise should use that documentation to streamline C&A, and enable cross-enclave Authority To Operate (ATO).

Defense Enterprise policy makers, trainers, and educators, should identify the best practitioners of tech refresh as an approach to post-IOC IT life cycle maintenance. They should work with those practitioners to distill their best practices, and turn them into pragmatic policies and training materials to address end-to-end pre and post-IOC acquisition

Defense Enterprise policy makers, trainers, and educators, should study the success of ARCI to develop a suite of boilerplate acquisition artifacts designed to more effectively align S&T, RDT&E, and O&M investments in mutually supportive rapid prototyping.

The Defense Enterprise test model must assess functional performance of candidate component solutions and their ability to plug-and-play usefully and securely across the open interfaces. The C&A model should likewise be modular. That is, candidate component solutions successfully tested as secure, useful, and open should be certified as such. This is not the way testing and C&A are performed in the Defense Enterprise today. Hence the Defense Enterprise test and certification authorities such as NSA, JITC, and DOT&E should work together to create and validate this new open modular model. The Defense Enterprise acquisition process should populate a continuously growing inventory of pre-approved components available conveniently via tools such as the GSA schedule and IDIQ contracts.

Specific recommendations with respect to test infrastructure standards:

- Include test requirements as inherent elements in specification of functional capabilities.
- Include testing infrastructure (e.g., instrumentation points and test tools) as included deliverables within developed software.
- Add an "Instrumentation View" (IV) that shows the location and design of instrumentation points, along with the associated activity and flow diagrams for testing end-to-end capabilities to the suite of required architectural views.

Defense Enterprise should warranty the "monitoring-time" behavior. Monitoring & management of COTs is important to ensure the proper functioning, particularly as part of a COTs ensemble. The idea that vendors should provide "instrumentation visibility" is an important one. All responsible vendors design their software to do this or be subject to it. Government is very focused on run time standards, e.g, WS-I, however it is equally important and often under-looked are development-time and monitoring-time standards. UML & SysML are examples of dev-time standards. CBE & SNMP are examples of monitoring-time standards, or protocols, that could be

used to "instrument" run times. Naturally this "monitoring-time" activity must include configuration management.

Defense Enterprise should require all its programs to develop clearly articulated need-to-protect vs. need-to-share policies. These policies should form the basis of C&A

Defense Enterprise should enforce a universal requirement that all programs that deliver network communications capability must make all devices routable nodes on LANs. Likewise all LANS must be routable nodes on WANS.

Organizations that intend to implement and sustain open source software must either invest to develop and maintain their own organic expertise, or contract for it.

Defense Enterprise contracts should enforce requirements for routable network communications (all devices are routable nodes on LANS; all LANS are routable nodes on WANS.)

Defense Enterprise acquisition practitioners should exercise government rights to broadly distribute any Intellectual Property (IP) developed at government expense. Consider paying vendors to maintain developed IP under open source software licenses.

Defense Enterprise acquisition authorities should develop boilerplate SLAs that link objective definitions of information system "interoperability" to objective definitions of desired operational outcomes such as Probability of Kill, planning cycle compression, reduced safety mishaps, reduced inventory in the supply chain, etc. Contracts should include requirement for continuous, tiered, testing throughout capability lifecycle to enforce these SLAs.