Let's Cure Defense Enterprise Information Technology Acquisition with a Dose of its Own Medicine

Chris Gunderson, Naval Postgraduate School

Abstract— **The Defense Community's inability to realize its "enterprise" vision for the Global Information Grid (GIG) has reached crisis. The Defense Science Board (DSB) reports that a new acquisition process, aligned with commercial best practice, is required. Commercial best practice is all about leveraging economy of scale to achieve better-speed-to-better-capability than the competition. Successful firms subscribe to a universal model for value-based evolutionary development. The iPhone is a good metaphor for that model. The Defense Enterprise acquisition process can support the same model by morphing existing serial, paper-intensive compliance artifacts and processes into a continuous, parallel, automated process in a persistent virtual environment. However, morphing for success will require courage and creativity from rank-and-file members of the Defense Acquisition community.**

I. DEFENSE ENTERPRISE INFORMATION TECHNOLOGY (IT) ACQUISITION BACKGROUND.

Per various watchdog reports, the Defense Community's inability to realize its "enterprise" vision for the Global Information Grid (GIG) has reached crisis [1]. Defense information systems -- which are deliberately firewalled from the rapidly evolving open Internet and associated development processes -- are generally over-budget and behind schedule [2]. Meanwhile international terrorists and criminals effectively use the Internet and World Wide Web (WWW) to support their enterprise objectives [3]. The Defense Science Board (DSB) suggests information technology (IT) acquisition policy changes are necessary to mitigate the crisis [4]. Surely such policy should identify proven success criteria and best practices, and incentivize their adoption.

Consider the meteoric pace of technology evolution on the WWW and the success of enterprises like iPhone, eBay, Amazon, FedEx, eFile, etc. Clearly, when it comes to large distributed, information-centric enterprises, the universal success criterion is better-speed-to-better-capability than the competition. "Best practices" are techniques that evolve ever-improving value-delivery chains for consumers. Best practices inevitably leverage the massive economy of scale of the commercial marketplace, and include customers as partners in the development process. They typically follow this general model for value-based evolutionary acquisition:

- Business process improvement loop that includes customer-value-based lag metrics, transaction analysis, internal system performance lead metrics, beta development process, and a workflow optimization governance process that effectively couples these components to achieve enterprise objectives.
- Scalable, COTS, product line network architecture built on routable Wide Area Networks (WAN) and Local Area Networks (LAN), and that seamlessly deliver value-added applications to decision making nodes.
- Federated governance model that includes objectively specified enterprise delivery "platform", branding criteria, and incentive model.

iPhone enterprise example

To demonstrate the model, consider the iPhone "enterprise" from the perspective of an individual application developer, say, Pandora Radio (see www.pandora.com). In this case, "federated governance" includes agreement among application developers to use the iPhone as their delivery "platform". iPhone "branding" means building to the various Apple proprietary specifications. The "incentive" is that it is cool to be an iPhone app, and developers can make lots of money from selling their

apps and/or from selling advertisements that ride on top of their apps.

Pandora Radio uses the massive scale of the WWW to create automated personalized music streams for its subscribers. If the WWW did not exist as enterprise infrastructure, and if the various music providers were not discoverable nodes, Pandora Radio could not succeed. Pandora did not invest to create the WWW or to create the music provider nodes. Pandora does pay for Internet services, and Pandora investments do contribute to improving the infrastructure of the WWW.

Pandora Radio's "business process improvement loop" aims to create a value delivery chain for its subscribers. The user-friendly Pandora Radio portal continuously and conveniently collects input from music consumers. Backend algorithms refine output on the fly. The value-based hypothesis is: "if Pandora delivers increasingly more valued music; then it will earn more listeners, who will each listen longer, making advertising on Pandora more lucrative." Lead metrics are increasingly positive consumer feedback regarding the automatically delivered musical offerings. Lag metrics are increasing advertising revenues.

Defense Enterprise opportunity

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 [5]. 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) [6] "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 *maintenance* phase of an IT capability life cycle. In those success maintenance cases, the government effectively peers with industrial providers to get good off-the-shelf value for its Operations and Maintenance (O&M) investments.

For modern information systems, "maintenance" is equivalent to "tech refresh". The objective of "tech refresh" is *continuous improvement* rather than continual repair. Given that a primary objective of an "enterprise" approach is to leverage economy of scale, there should be no fundamental difference between "tech refresh", i.e. upgrading components of an existing shared IT infrastructure, and "developing" a new enterprise IT capability. In both cases the core infrastructure already exists and the objective is to quickly and continuously deploy improved capabilities.

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 [7].

Having made the case that successful rapid evolutionary IT acquisition is possible in the existing defense community policy regime; the task becomes to make it common. Creatively applying the existing defense acquisition policy compliance artifacts, as described in the Joint Capability Integrated Development System (JCIDS) Manual [8], can institutionalize best practices across the Defense Enterprise.

II. DEFENSE ENTERPRISE IT *ACQUISITION PROCESS* AS A JCIDS "CAPABILITY"

A. Eating the Elephant.

Various authorities, such as the Secretary of Defense, Chairman of the Joint Chiefs of Staff, Director of National Intelligence, and others have issued the myriad, detailed, arcane, and relatively static policies that govern Defense Enterprise acquisition. The current Defense Enterprise acquisition process delivers a series of detailed, static, artifacts that document *intended* compliance with those policies. The "elephant in the room" is

that this long, expensive, manual process is almost never successful.

Industrial best practice suggests a fundamentally different, automated approach. In particular, Hopkins and Jenkins [9] describe a metaphorical "Elephant Eating Machine" based on their study of rare successes, and many more failures, of large IT projects. Their Elephant Eating Machine employs automated templates to collect various "views" of design objectives across the broad landscape of large IT projects. Those views collectively constitute a searchable "inventory" of the requirements, constraints, and alternatives. In their model, "transforms" cross correlate multiple views. These transforms continuously re-generate "artifacts" that measure both the level of consistency across views, and demonstrated performance against design objectives. These *diagnostic* artifacts are frequently generated, iterative, automated, and objectively specific. They contrast starkly with the static, subjectively generic, *prognostic* artifacts typical of the Defense Enterprise acquisition process. The following paragraphs explain how the Defense Enterprise can apply this kind of Elephant Eating Machine thinking to fix its failed IT acquisition process ... within the constraints of current policy.

B. Online machine-readable Defense Enterprise IT acquisition policy directives and compliance reporting artifacts.

Reducing bureaucratic overhead will require turning the thousands of pages of redundant or conflicting written policy into a relatively short list of clear, enforceable elements. To do that, we can capture all defense acquisition policy directives in machine-readable form. For shorthand, use the term "Defense Enterprise Policy Markup Language" (DE-PML) to represent any number of semantic and/or modeling software languages adequate for that purpose.

Use automated semantic techniques to crosscheck the multitude of – now machine-readable -- policy directives issued by various Defense Enterprise authorities. Discover and rationalize the policy conflicts. Distill and parameterize the essential, enforceable, points. For example, a parameterization of an "evolutionary acquisition" policy might be a specified, reportable, minimal period between delivered capability incremental upgrades. Likewise, a parameterization of "Open Modular Design" (OMD) policy might be specified contractual Service Level Agreements (SLA) for treating Intellectual Property Rights (IPR). In this case, IPR includes Government Purpose Rights (GPR) to share capability across the Defense Enterprise. Another parameterization of OMD policy could be live, online, endpoints to a Defense Enterprise test harness such as the Joint Interoperability Test Command (JITC) Open SOA Test Framework (OSTF) (Rick Toliver, Chief Scientist W2COG, live demonstration of OSTF, various dates November 2009 – March 2010).

Generate corresponding DE-PML acquisition compliance reporting templates. This is a

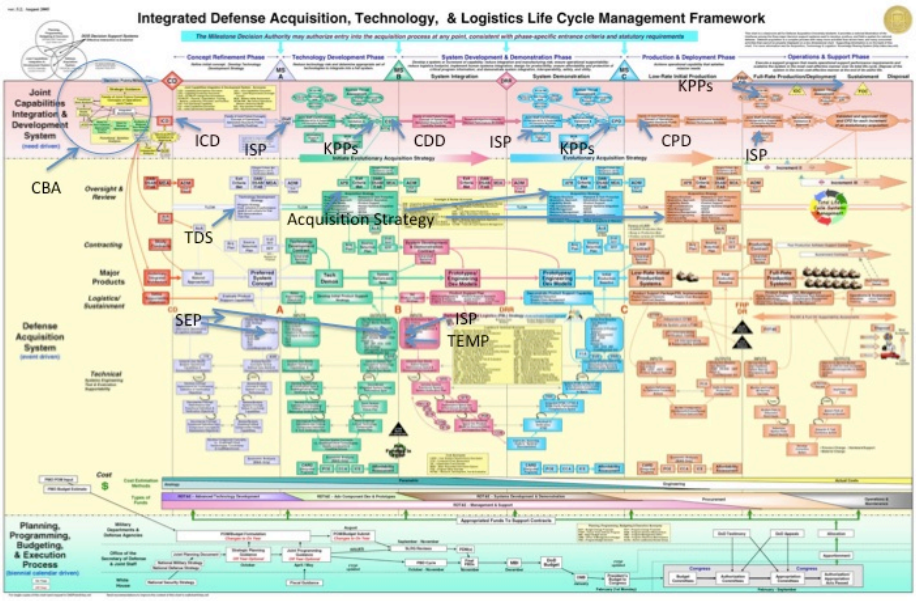

Figure 1: Defense Enterprise "as is" acquisition process. The DE-ICD converts the ponderous static artifacts into machine-readable templates that collect objective views of policy, use cases, constraints, and alternatives. The Value-based Acquisition Framework transforms those views into continuously evolving design artifacts focused on delivering Better-Speed-

fundamental change from requiring programs to deliver static, end-to-end artifacts that document *claimed* compliance with enterprise objectives. Rather, programs enter objective information and received automated confirmation of, or instructions about how to achieve, compliance. An analogy is eFile tax return software. Complicated compliance requirements, i.e. the tax code, are programmed in "backend" software. A simple online interface at the "front-end" collects required information. An online backend machine automatically checks for compliance and either delivers the required reporting artifact, or offers corrective guidance. Provide these machine-readable, re-usable, templates online, as GFE, to the global IT developer community.

Align the templates with the JCIDS Manual descriptions of the required Defense Enterprise acquisition compliance *views* per the following paragraphs. See Figure 1 for reference. Notice that aspects of these new compliance views are redundant with each other … just as they are in the traditional approach. However, unlike in the traditional, manual, paper-intensive process, redundancy is not an issue in this automated approach. We can capture the same information once, and then easily and accurately re-use it as necessary. When the information changes, the updates occur automatically across all the views and appear in any newly generated artifact.

C. Defense Enterprise IT Acquisition Capability Based Analysis (DE-CBA).

The JCIDS manual suggests using reports prepared by experts as the basis for CBA. In that spirit, we might stretch a point and consider the Mar 2009 DSB report on IT Acquisition to constitute a de facto CBA. This DE-CBA addresses Defense Enterprise IT acquisition *process* per the following argument.

Enterprise IT Architecture as a value-delivery-chain

Successful e-businesses would agree with the following generic description of functional "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

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 associated with the first two bullets. Rather, they employ value-delivery-chains that continuously collect customer feedback, via the first two bullets, and drive IT investments in the third bullet. Any federation of these e-businesses that leverage each other by sharing infrastructure constitutes an enterprise. Their mutually supportive activity constitutes a SoS.

Use of enterprise IT Infrastructure is not necessarily free. It will likely require fees for services, purchasing equipment, giving up privacy, accepting security risks, accepting generic rather than tailored features, etc. However, businesses join the e-enterprise because these costs are clearly worth the tangible benefits they return.

Requirement for a Defense Enterprise IT value-delivery-chain

Defense policy specifies a requirement for "Netcentric Operations" (NCO). One interpretation of NCO is effective, distributed, Command, Control C2, Intelligence, Surveillance, and Reconnaissance (C2ISR) across independent self-synchronizing members of the Defense Enterprise. In this interpretation, "effective" means "resulting in an asymmetric advantage with respect to targeted mission outcomes" [10]

Accordingly, the GIG aims to be a distributed Computer and Communications network that allows independent systems such as weapons, sensors, and platforms, to "self-synchronize" into a "netcentric" C2ISR System-of-Systems (SoS). In other words, the GIG aims to be IT Infrastructure for the Defense C2ISR Enterprise.

However, the DE-CBA has determined that the existing Defense Enterprise IT Infrastructure is not sufficient to realize the objectives of the GIG. Apparently, the cost associated with using the existing Defense IT infrastructure to collaborate across defense "business units" is greater than the perceived benefits. The DE-CBA concludes that this insufficiency constitutes a critical capability gap.

The DE-CBA notes that the myriad programs that have attempted, and/or are attempting, to address the issue have been generally failing for a decade. Defense programs do not identify testable enterprise-level requirements for their interoperability

certifications (Steve Bridges, Chief Engineer, Joint Interoperability Test Command, personal interview, December 13, 2009.) Therefore, the E-CBA concludes that the current Defense Enterprise IT business process is insufficient to close the gap. In other words, *there is no existing Defense Enterprise IT value-delivery-chain*. Therefore, the DE-CBA recommends creating a better IT acquisition process.

Notice that the DE-CBA recommendation is to apply a non-material solution, i.e. institute a better process, to resolve a critical capability gap. JCIDS guidance clearly encourages non-material solutions whenever possible.

D. Defense Enterprise IT Acquisition Process Initial Capability Document (DE-ICD).

We can now precipitate a DE-ICD for "Defense Enterprise IT Infrastructure Acquisition ***Process***" from the DE-CBA.

Components of an IT value-delivery-chain

The DE-ICD identifies a requirement to institute an IT value-delivery-chain across the Defense Enterprise. Best practices associated with successful IT value-delivery-chains include Business Process Analysis (BPA), Managed Workflow, Beta Development Communities, and "dashboards" that link system-level performance metrics and business process-level metrics to measurable Return on Investment (RoI). Current industrial shorthand (i.e. buzzword) for best practices associated with creation and maintenance of value-delivery-chains is "Business Process Management Suites" (BPMS).

Accordingly, the DE-ICD identifies requirements for Defense Enterprise Business Process Analysis (E-BPA), managed Defense Enterprise Workflow (E-Workflow), a Defense Enterprise IT Beta Development community, and a suite of Defense Enterprise value-based system-level, process-level, and outcome-level Key Performance Parameters (DE-KPP) [11]. We might collectively describe these views as DE-BPMS

Enterprise value proposition

An "enterprise" is a federation of semi-autonomous organizations that each recognize the value of, and therefore participate in, collaboration. In that spirit, the DE-ICD does not address any particular individual acquisition program. Rather it provides a process for all programs to both leverage, and contribute to, Defense Enterprise IT infrastructure.

The concept of a "Defense Enterprise" is scalable. The concept can apply across all Defense Department, Intelligence Agency, and Law Enforcement Agencies, or, it can apply across any subset. Indeed, the concept can scale to encompass the entire Federal Government and beyond. The suite of proposed Defense Enterprise IT Acquisition Process compliance templates are designed to scale accordingly. Note that in this sense "compliance" means conforming to the minimum set of best practices agreed among members of a federation, i.e. participating in *federated governance.*

"Compliance", then, is analogous to earning commercial logos such as ITIL, UL, Lean Six Sigma, CMMI, etc. User-friendly, re-usable, machine-readable, online, tools analogous to TurboTax will enable "compliance". "Compliance" is in lieu of, rather than in addition to, the traditional paperwork-intensive approach. Therefore "compliance" with this new enterprise business process is obviously useful rather than onerous. "Compliance" can align subsets of individual programs, align programs across a particular military service, and/or align joint and coalition capabilities.

E. Defense Enterprise IT Architecture (DE-A), Information Support Plan (DE-ISP), Key Performance Parameters (DE-KPPs), and Reliability, Availability, and Maintenance (DE-RAM).

Defense Enterprise IT Architecture

DE-A consists simply of wireless and wired WANS, that are connected by router to wired and wireless LANS, that are connected to routable computing devices, that execute open standard enterprise applications, that seamlessly deliver value-added decision support services to decision making nodes. See Figures 2 and 3. The Defense Enterprise should make on line, machine-readable specific views of this architecture openly available to developers as GFE.

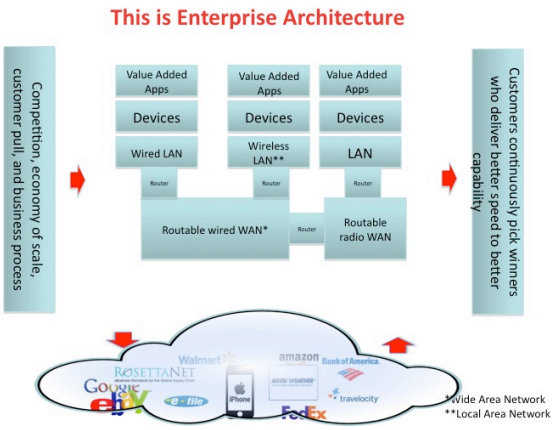

Figure 2: Enterprise Architecture in the Real World

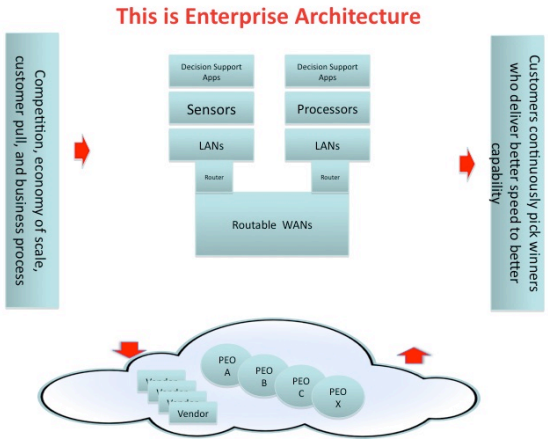

Figure 3: Defense Enterprise Architecture (if we finally get it right…)

Defense Enterprise KPPs

DE-KPPs serve the function of "transforms" in Hopkins's and Jenkins's Elephant Eating Machine metaphor. That is, DE-KPPs cross correlate various views of policy, requirements, alternatives, and constraints in an objective Value-based Acquisition Framework (VAF). VAF allows programs to manage the complexity by iteratively generating pragmatic artifacts that govern IT acquisition in small evolutionary increments.

The mandatory Defense Enterprise IT Acquisition Process KPPs are the DE- Sustainability KPP (DE-S-KPP) and DE-Net-ready KPP (DE-NR-KPP).

Defense Enterprise Sustainability KPP

Historically S-KPPs are system-level performance metrics that address Reliability, Availability, and Maintainability (RAM) of a system throughout its lifecycle [12]. "Availability" is defined as "up time" divided by "total time." "Useful time" is the critical parameter and the objective is to optimize acquisition options accordingly.

Consistent with the need for better acquisition process, the DE-S-KPP is a *process-level* metric that transforms "sustainability" to "speed-to-capability". In other words, the ability to rapidly and continuously refresh technology, including retiring superseded technology, is equivalent to sustainability of a modern enterprise information system. In still other words… if you can't keep up you die!

We can parameterize the DE-S-KPP as "Availability of Net-readiness" (A_{nr}). The critical parameter is still "useful time," but in this case it is the time it takes to deliver capability. To calculate A_{nr}, we estimate a reasonably short time required to deliver a small increment of capability. Then we compare the initial estimate of "capability development time" to the current estimate. As schedules slip, and the denominator becomes increasingly larger than the numerator, A_{nr} decreases from the "objective" value. If A_{nr} slips below some "threshold" value, the program must re-scope its efforts.

Defense Enterprise Net-ready KPP

At a high level, Commander, Joint Chiefs of Staff (CJCS) policy defines the NR-KPP in terms of the ability of information exchanges across the GIG to enable better operational outcomes [13]. A reasonable transformation of that objective is to define "net-readiness" of any system, or system component, as its ability to connect via Defense Enterprise IT infrastructure and contribute positively to the enterprise C2ISR SoS. Accordingly, we can parameterize DE-NR-KPP as "Availability of Information Value" (A_{iv}).

A_{iv} is a SoS performance metric that transforms "net-readiness" policy into a demonstrated positive correlation between objectively measured Information Processing Efficiency (IPE) and Delivered Information Value (DIV). In other words, the DE-NR-KPP defines IPE in terms of a SoS's measured ability to improve desired operational outputs such as Probability of Kill (Pk), reduced fratricide, planning cycle compression, force readiness, etc. "Reliability" is an included aspect of IPE. See Appendix C: DE-S-KPP & DE-NR-KPP Formulation.

Defense Enterprise KPP dashboard

The DE-KPPs apply to individual program components. Aggregating DE-KPP performance across the programs of interest will provide an assessment, or "dashboard", of the Defense Enterprise IT Acquisition Process as a whole. Again, the overall enterprise objective is better-speed-to-better-capability. The following are alternative metrics to assess any subset of the Defense Enterprise against that broad objective:

- Better overall enterprise mission performance per aggregated mission-outcome metrics
- Faster average speed to capability
- Reduced average cost per capability delivered
- More predictable cost per capability delivered

Notice that reducing IT cost is not a stated business objective. The premise is that sustaining and properly managing investment in an IT value-delivery-chain will cause improved business outcomes.

Enterprise RAM and ISP

It follows that the DE-RAM high-level requirement is to continuously deliver measurably faster speed, to measurably better, capability. DE-S-KPP and DE-NR-KPP provide the measurement tools and framework for managing options.

The DE-ISP, then, is the plan to implement DE-BPMS: i.e., the plan to conduct continuous BPA, in partnership with the Defense Community Beta Development Community, and to refine and address specific DE-RAM requirements accordingly. See Figure 4.

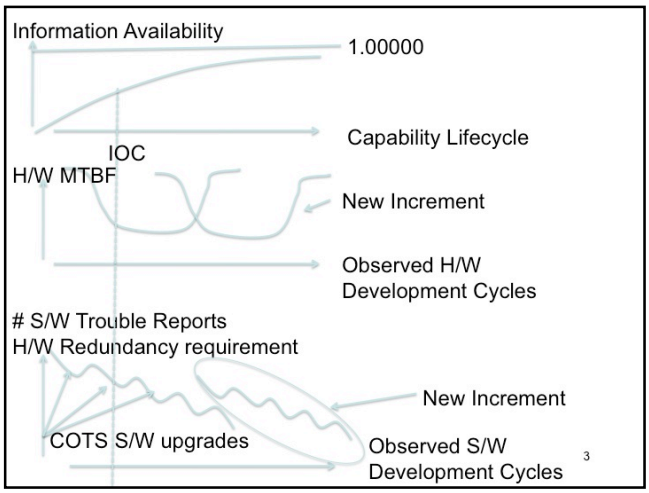

Figure 4: Enterprise RAM process should anticipate capability increase associated with inevitable software improvements. Deploy capability at some "threshold" performance level. Manage improvement toward an "objective" performance level later in life cycle. In other words, deploy "good enough" capability and then work with customers to continuously improve it.

F. Defense Enterprise Information Technology Development Strategy (DE-TDS).

The main tenet of the DE-TDS is to "buy down" risk by addressing as much as possible of the total defense requirement with continuous COTS tech refresh. Use DE-BPA to identify the gap between delivered COTS capability and the essential and unique Defense Enterprise infrastructure requirements. (Information Assurance (IA) and Semantic Interoperability (SI) are obvious gaps between COTS capability and Defense Enterprise requirements.) Invest Science and Technology (S&T) and Research and Development (R&D) funds to close the technology gaps in short iterative spirals. Employ COTS vendors, open standards, and open source licenses, as appropriate, in this process. Exercise GPR to distribute results of R&D and S&T broadly across the industrial base.

G. Defense Enterprise System of Systems Engineering Plan (DE-SEP)

The DE-SEP is an implementation of a Defense Enterprise variant of Hopkin's and Jenkin's Elephant Eating Machine concept. That is, the DE-SEP describes in detail how the components of the Defense Enterprise acquisition process, described herein, continuously and iteratively perform the following:

- Collect and refine views of policy, requirements, alternatives and constraints
- Create searchable inventory of views
- Develop transforms that cross correlate views
- Generate artifacts that enable and/or evaluate compliance with design objectives.

Program requirements.

Detailed views evolve from continuous analysis of mission use cases, i.e. mission level workflow, and legacy architectural constraints. The analysis includes developing and evaluating *reference implementations* of potential solutions. That work is performed in partnership with operational practitioners.

An online repository of machine-readable, objective policy statements, use cases, constraints, and reference implementations constitutes an inventory of views. The Value-based Acquisition Framework provides the basis to transform

constraints, requirements, and alternatives, into evolving design artifacts.

Testing and certification

The Defense Enterprise Test and Evaluation Master Plan is a "living" artifact delivered by the DE-SEP.

Technical staff and organization

DE-SEP specifies that program must include a beta development community of operational practitioners. Note that the same beta community members will support various programs' requirements. The approach must not over-burden operators. Rather, the enterprise IT infrastructure itself should include low friction tools for collecting DE Beta Community input. Contracts must include SLAs that require vendors to cultivate Beta Development Communities among members of the Defense Enterprise and beyond.

Technical baseline

The Defense IT Enterprise favors mainstream COTS standards as defined by reputable standards bodies. In this model, the Defense Enterprise certifies the standard-developing processes used by the various standards bodies, rather than try to perform the impossible job of staying up to date with each individual standard. In other words, the Defense Enterprise will simply "transform" the outputs of vetted groups such as IEEE, OMG, OGC, W3C, IETF, etc, into instances of the "industrial best practice" mandated by policy. Programs will use the DE-KPPs to measure and report compliance with this baseline. That is, their choice of appropriate commercial open standards must result in their ability to achieve acceptable DE-KPP objectives, i.e. better-speed-to-better-capability.

Defense Enterprise Overall management objectives

E-workflow management tools will coordinate program developmental activity with designated technical compliance authorities. For example, automated lightweight web-based tools can help a program cross check to see if a required capability already exists, has already been certified, and/or is already under contract. The same tools can coordinate T&E, V&V, and C&A for similar capabilities being developed across program boundaries.

H. Defense Enterprise IT Acquisition Strategy (DE-AS)

Per industrial best practice, DE-AS will favor firm fixed price contracts to purchase pure COTS software offerings wherever possible. Whenever the government needs true "discovery," Level of Effort (LOL) contracts -- wherein government and commercial partners share risks for software development are appropriate [14].

The DE-AS will leverage the huge magnitude of the total Defense Enterprise IT investment to negotiate favorable terms with commercial providers. Negotiations will include non-traditional, approaches to managing Intellectual Property Rights (IPR) and Government Purpose Rights (GPR) across the Defense Enterprise. Elements of the DE-AS include:

- Negotiating cost-effective means, beyond traditional license agreements, to distribute government-funded capability broadly as GFE
- Paying vendors to develop and maintain essential portable GFE infrastructure components, e.g. for IA and SI, under open source licenses.
- SLAs and associated performance-based contract incentives tied to the DE-KPPs.
- SLAs require establishing beta development communities that include operational practitioners and leverage larger industrial beta development communities.

I. Defense Enterprise IT Acquisition Process Test and Evaluation Master Plan (DE-TEMP).

The DE-TEMP is tightly integrated within the DE-ISP , i.e. the DE-BPMS. The DE-TEMP will employ DE-Workflow to create a persistent virtual environment for continuing Test and Evaluation (T&E), Validation and Verification (V&V), and Certification and Accreditation (C&A). That effort will occur in parallel with small incremental developmental spirals, and in parallel across programs. For example, many programs need to integrate security services with their business process applications. DE-Workflow tools can coordinate multiple programs' development activities together with the appropriate certification and approval authorities to perform IA certification in parallel.

"Net-readiness" is a defense enterprise requirement. Per Chairman, Joint Chief of Staff CJCS direction [15] IA and SI are included aspects of net-readiness. Hence, DE-NR-KPP certifications will objectively quantify IA and SI performance of the tested artifacts. IA is equivalent to a SoS's ability to predictably and appropriately protect and/or make information available. SI is equivalent to any sub system's ability to find actionable information wherever it exists in the Defense Enterprise C2ISR SoS, and/or deliver actionable information to decision-making nodes across the Defense Enterprise C2ISR SoS. Need-to-protect vs. need-to-share

considerations are inherent in the DE-NR-KPP formulation. In this way, DE-NR-KPP certification can provide the basis of IA C&A for the appropriate DAA.

Per Director of National Intelligence and DoD guidance [16] [17] all Designated Approval Authorities (DAA) are required to recognize each other's certifications and accreditations. DE-TEMP will address that requirement by publishing re-useable reference implementations of successful DE-NR-KPP certification.

J. Defense Enterprise IT Acquisition Process Capability Development Document (DE-CDD).

introductory paragraph. The DE-CDD consists of the following conceptual components:

Business process improvement loop

The objective is to create a value delivery chain. A first step is to create a Defense Enterprise Beta Development Community who will define "value" from the customer's perspective. E.g.:

- Vendor SLAs require continuous "customer" feedback
- Use data collection tools embedded in "business" applications, per commercial model

Perform transaction analysis to define Valued Information at the Right Time (VIRT). E.g.:

- Continuously capture operational use cases

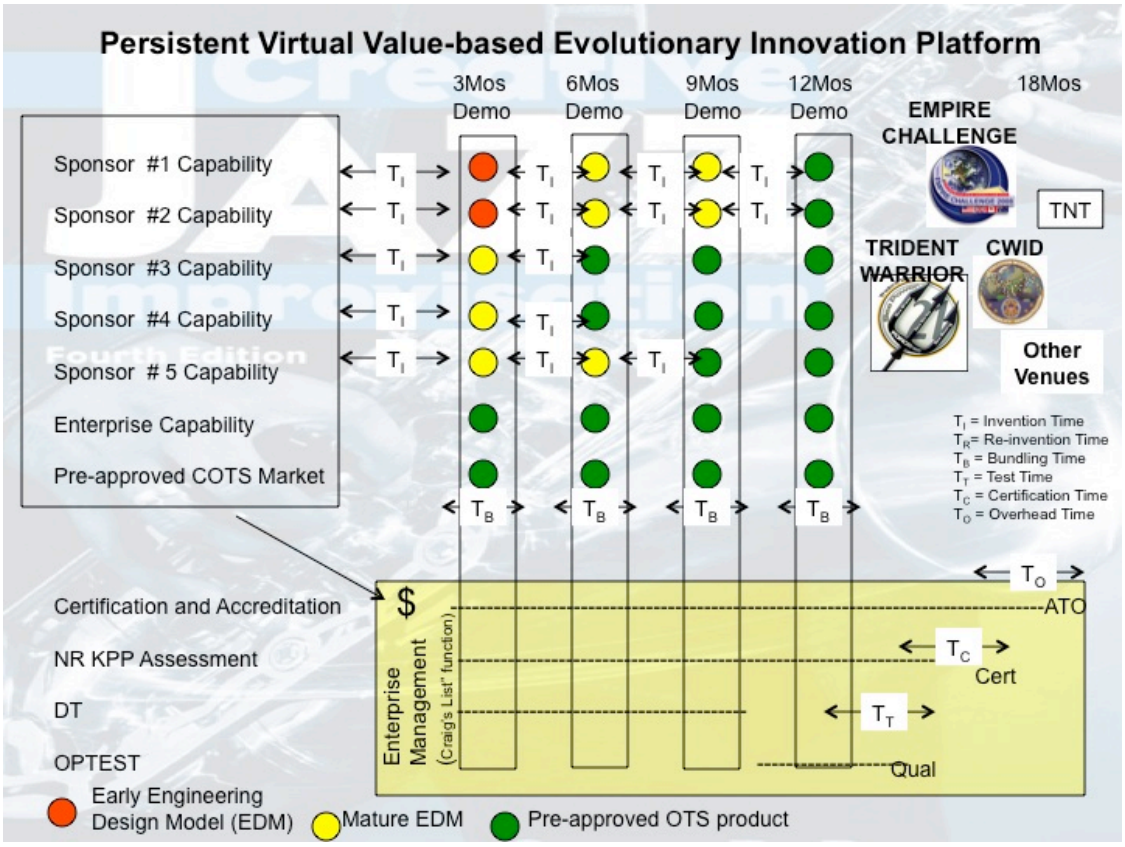

Figure 5: A Persistent D, T&E, V&V, and C&A environment and workflow management process. The "Enterprise" process is essentially a Craig's List resource to capture and share best practice, and broker providers and consumers of net-enabled capability.

All the DE-Acquisition artifacts described above inform the DE-CDD. The DE-CDD will explain how to create "federated governance" across the defense enterprise. This is largely a non-material, process-level, solution to implement the value-based evolutionary acquisition model described in the

including mission threads, i.e. mission-level workflow

- Continuously audit DE-NR-KPP performance, i.e. correlation between SoS performance lead metrics and mission outcome lag metrics

Create a persistent virtual environment to develop and demonstrate capability to deliver VIRT. (See Figure 5.) E.g.:

- Regularly scheduled, e.g. quarterly, bundling events per published use cases including approval and certification authorities
- "Graduation" process for successful COTS/GOTS reference implementations to pre-approved product lists and Indefinite Delivery, Indefinite Quantity (IDIQ) and/or similar contract vehicles

Ubiquitous COTS Network Architecture

The Defense Enterprise should leverage the commercial network transport layer, i.e. the open Internet, just as it leverages the global commercial transportation network. I.e. DE IT Architecture consists simply of the following:

- Federated routable wired and wireless WANs and LANs
- Routable open standard computing devices
- Enterprise open standard applications that seamlessly deliver value-added to decision making nodes.

Risk Adaptive Access Control (RAdAC)

To make it possible for the Defense Enterprise to truly leverage the commercial Internet, the eventual IA goal is a black core. "Black core" means a single point of entry into any generic routable network, with multiple dynamically assigned, levels of access. NSA calls this concept Risk-adaptive Access Control (RAdAC) [18] RAdAC requires:

- High assurance IA services
- Dynamic policy defining emergent need-to-know vs. need-to-share

Figure 6: Federated Governance Model

Federated governance model (See Figure 6)

Specify Defense Enterprise network capability delivery "*platform*," i.e. Defense Enterprise network "Tier 0" specifications. E.g.:

- Unambiguously specified enterprise network "dial tone"
- Universal online access to persistent development, T&E, and C&A environment

Establish "*branding*" criteria, i.e. a Defense Enterprise "Net-ready Logo." E.g.:

- Pre-approved GFE components
- Objective DE-KPPs
- Streamlined enterprise, modular component-based certification process per "net-ready logo" criteria.

Establish a clear *incentive* model. E.g.:

- Level playing field across all of industry rather than traditional Defense "Cottage Industries"
- Reduced developers' costs for marketing to the Defense Enterprise
- Increased developers' speed to market
- Opportunity for industry to leverage Defense Enterprise research investments for commercial applications
- Patriotic opportunity to make a difference in an important cause

Return on investment

Again, aggregating performance against the DE-KPPs across the components of enterprise should demonstrate:

- Better aggregate mission-outcome metrics
- Faster average speed to capability
- Reduced cost per capability delivered
- More predictable cost per capability delivered

See Appendix F: Notional DE-CDD.

H. Defense Enterprise IT Acquisition Process Capability Production Document (DE-CPD)

DE-CPDs address tools for managing Defense Enterprise IT Acquisition business processes such as E-Workflow. DE-CPDs also provide guidance for acquiring generic enterprise infrastructure components. As ever, emphasis is on off-the-shelf capability. Accordingly, the DE-CPD is essentially a "living" consumer reports, catalog of pre-approved products, and "Craig's List" of providers and consumers of net-enabling capability. See Figure 7.

III CONCLUSION

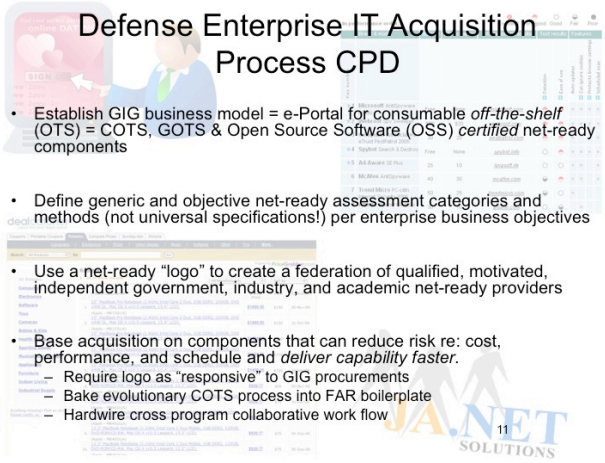

Figure 7: The Defense Enterprise Capability Production Document should be a portal to make it easy to consume enterprise-enabled capability. I.e., consumer reports + online test environment + brokering service + pre-approved online purchasing vehicle

We members of the Defense Enterprise acquisition community owe the young people fighting our wars better than we're giving them. We owe them the to best tools available… applied against their most critical concerns. The fact that terrorists and criminals have better information processing tools than our forces do is unacceptable.

We have all the policy we need to reverse our current unacceptable level of performance. However, we must acknowledge that the approach that got us into this unacceptable state will not get us out.

We must exercise enough courage and creativity to try another approach. That approach must build on top of the same ready access to generic COTS and the WWW that terrorists have. In other words, *we've got to deliver baseline COTS plus value-added MILSPEC….and do it at Internet speeds.* Any paperwork that prevents us from succeeding at that task is value-subtracted.

In our case "the emperor" is not naked; the emperor is wearing a ball and chain that he doesn't seem to see. We need to take it off his leg and lace up a pair of Nikes at the same time. Then we need to "just do it!"

IV REFERENCES

[1] FY 2010 National Defense Authorization Act, Sec 804
[2] GAO. Defense Acquisitions: Charting a Course for Lasting Reform. Apr 30, 2009.
[3] Martin , A. *Al Qaeda- A Lesson in Networked Warfare?* Canadian Forces College (CFC) . Toronto: CFC . Royal Air Force Wing Commander Martin explains how Al Qaeda uses the Internet as its Global Information Grid to achieve asymmetric advantage through information superiority.
[4] Defense Science Board. (2009). *Report on DoD Policy and Procedures for Acquisition of Information Technology.* Washington DC: GPO.
[5] Department of Defense (DoD). (2008). DoD Instruction 5000.02: Operations of the Defense Acquisition System. DoD.
[6] Federal Acquisition Regulations, retrieved from https://www.acquisition.gov/FAR/, May 2, 2010.
[7] Boudreau, Michael. Acoustic Rapid COTS Insertion: A Case Study in Spiral Development, 30 October 2006, Naval Postgraduate School
[8] CJCSM 3170.01C. Operation of the Joint Capabilities Integration and Development System, 1 May 2007
[9] Hopkins, R. & Jenkins, K., (2008). *Eating the IT elephant: moving from greenfield to brownfield development.*: Pearson, plc
[10] Cebrowski, A., & Gartska, J. (1998). Network-Centric Warfare (NCW): It's Origin and It's Future. *Naval Institute Proceedings , 124.*
[11] GAO. Stronger Practices Needed to Improve DoD Technology Transition Processes, Sept 2006
[12] CJCSM 3170.01C. Operation of the Joint Capabilities Integration and Development System, 1 May 2007
[13] CJCSI 6212.01 Interoperability and Supportability of Information Technology and National Security Systems, 15 Dec 2008.
[14] Popendieck, Lean Contracts, retrieved from http://www.poppendieck.com/contracts.htm, retrieved May 2, 2010.
[15] CJCSI 6212.01 Interoperability and Supportability of Information Technology and National Security Systems, 15 Dec 2008.
[16] Intelligence Community Directive #503. Intelligence Community Information Technology System Risk Management, Certification, and Accreditation, 15 Sept 2008. ICD 503
[17] DoD Memo Subj DoD Information System Certification and Accreditation reciprocity, 23 Jul 2009.
[18] NSA GIG IA Architecture