CWID 08 Demonstrates Rapid Evolutionary Acquisition Model of Coalition C2

C.R. Gunderson, Naval Postgraduate School & Joint Interoperability Test Command,
Chris.Gunderson@w2cog.org
David Minton, Raytheon, David_H_Minton@raytheon.com

Abstract- Coalition Warrior Interoperability Demonstration 2008 (CWID 08), Interoperability Trial (IT) #5.64 "Trusted Enterprise Service Bus" (T-ESB) demonstrates a potentially quantum improvement in the government procurement model for information systems. Joint Interoperability Command (JITC) sponsored the World Wide Consortium for the Grid (W2COG) Institute (WI) to conduct IT 5.64. WI studied the requirements of the Multi-National Information Sharing (MNIS) program to distill the following objectives:

- **"Flatten" coalition networks**
- **Enable data and service "discovery" via semantic interoperability**
- **Demonstrate rapid, adaptive, evolutionary acquisition compliant with the Federal Acquisition Regulations (FAR) and based on commercial best practice.**

The general premise is that the government should "buy down" as much implementation risk as possible of its basic information-processing requirement with true COTS capability. An issue is that government requirements, especially military requirements, are typically more stringent than commercial requirements. Security and interoperability are especially critical. True COTS offerings rarely address the total government requirement. Accordingly, IT 5.64 provided credible demonstration of the viability of the following hypothesis: i

If the government (1) continuously develops and furnishes critical raw technology to the industrial base, and (2) simply publishes its use cases, objective selection criteria, and COTS competitive procurement budget in lieu of formal Engineering Development Model (EDM)-type solicitations;

Then continuing industrial competition will generate pure COTS offerings that are ever more aligned with government requirements.

I. SUMMARY

To frame IT 5.64, the WI designed a government procurement consistent with the following hypothesis:

> *If the government (1) continuously develops and furnishes critical raw technology to the industrial base, and (2) simply publishes its use cases, objective selection criteria, and COTS competitive procurement budget in lieu of formal Engineering Development Model (EDM)-type solicitations;*
>
> *Then continuing industrial competition will generate pure COTS offerings that are ever more aligned with government requirements.*

The IT 5.64 prototype capability is designed as a vendor team response to that hypothetical procurement. Hypothetical source selection depends on actual demonstration of value added in realistic mission simulations. WI used a combined Coalition Maritime Domain Awareness (MDA) and Maritime Interdiction Operation (MIO) mission thread as the basis of the solicitation. Stated government priorities are rapid deployment, demonstrated utility, continuous improvement, re-usability within and across program boundaries, and Information Assurance (IA). In this solicitation, "IA" refers to two broad objectives. One objective is assured methodology for managing risk with respect to the need-to-share vs. the need-to-protect information. The other is assured data strategy for both discovering valued information, and preventing information overload. The WI vendor team response was a prototype web service stack designed to (1) enhance "Information Processing Efficiency" (IPE), and (2) execute dynamic need-to-protect vs. need-to-share security policy. The prototype has a "Trusted-Enterprise Service Bus" at the server end, and a Trusted Command and Control (C2) Web Portal (TC2P) on the service consumer end. The web service stack includes: Protection Level 4 (PL4) government-furnished security services; Unmanned Aerial Vehicle (UAV) sensor services; and Intelligent Agents that provide a "Valued Information at the Right Time" (VIRT) service. The VIRT service issues a browser pop up message when geospatially enabled software agents detect pre-defined critical conditions of interest (CCI). Analysis of collaborative interaction among eight multi-national C2 watch standers shows an IPE for the T-ESB/TC2P that is at least 60%, and as much as two orders of magnitude more, efficient than the baseline capability. Analysis also suggests 36-69%

value added through "need-to-share" services. The WI team used this analysis to craft a notional vendor response to the hypothetical solicitation. Vendor claims in the solicitation response are objective and supported by runtime demonstration and analysis. The hypothetical bid includes life cycle improvement, guaranteed software currency, continuing customer outreach, streamlined C&A, and objectively defined "open" architecture. The methodology allows government to transform its myriad technology demonstration venues collectively into a competitive marketplace of such capability. The demonstration venues need not be limited to scheduled, formal, large scale events. Any properly configured and certified laboratory can participate. JITC, supported by the W2COG Institute, can assist interested participants perform the requisite configuration, and develop the necessary FAR-compliant documentation.

II. BACKGROUND

CWID is an annual event mandated by the Joint Chiefs of Staff (JCS) to focus cutting-edge information technology on information sharing requirements defined by combatant commanders. CWID addresses collaborative information exchange among coalition partners, military services, government agencies, first responders and U.S. combatant commanders. Each CWID event showcases myriad separately sponsored "interoperability trials" (IT) loosely interlinked through mission scenarios. CWID is one of many venues designed to accelerate fielding advanced technology to the DoD and Intelligence community. It, as do all the others, suffers from the lack of an efficient technology transition process. [1]

Multi-National Information Sharing (MNIS) is a Defense Information System Agency (DISA) program. MNIS objectives are to consolidate and sustain current multinational information sharing systems; standardize products and services solution sets; provide product improvements to meet essential required capabilities; provide enhancements to meet emerging war fighter requirements. The CENTCOM Regional Intelligence Exchange System (CENTRIX) Cross Enclave Requirement (CCER) is a subset of the MNIS program. The CCER mission is to "converge physically separated coalition war fighting networks to provide a common suite of information services to all Mission Partners with controlled access to Command and Control (C2) and Intelligence applications on a common network -- based on country trust and user role" [2]

World Wide Consortium for the Grid (W2COG) is a self-selecting collaborative community of experts from government, industry, and academia. The Office of the Secretary of Defense spawned the W2COG with a research grant in FY05. The W2COG mission is to advance "netcentricity" by applying the best Internet collaborative and business models, and by removing the traditional barriers to cross-stovepipe collaboration.

The W2COG Institute (WI) is a legally incorporated not-for-profit, non-government organization (NGO) chartered to manage the activities of the W2COG. The Joint Interoperability Test Command (JITC) has commissioned the WI to study government acquisition process in context with best industry practice. In particular, JITC wishes WI to propose test and certification models designed to accelerate fielding netcentric capability.

At the request of Deputy Director DISA, WI has studied the MNIS program mission and requirements. In particular, WI designed and executed CWID 08 IT #5.64 to address MNIS issues by achieving the following objectives:

- "Flatten" coalition networks
- Enable data and service "discovery" via semantic interoperability
- Demonstrate rapid, adaptive, evolutionary acquisition compliant with the Federal Acquisition Regulations (FAR) and based on commercial best practice.

"Flatten" means to use the same physical infrastructure to support networked private coalition enclaves. "Discovery" means that consumers can compose their own versions of "operating pictures" dynamically by selecting critical bits of information from the huge pool of data available on the network. Flattening networks and enabling discovery requires balancing the "need-to-share" and the "need-to-protect" information.

III. APPROACH

The premise of CWID 08 IT 5.64 is that the government should "buy down" as much implementation risk as possible of its basic information processing requirement with true COTS capability. That premise infers that the best way to harvest up-to-date and viable technology is by simply purchasing it as it becomes available on the market. An issue is that government requirements, especially military requirements, are typically more stringent than commercial requirements. Security and interoperability are especially critical. True COTS offerings rarely address the total government requirement. Accordingly, the IT 5.64 hypothesis is as follows:

If the government (1) continuously develops and furnishes critical raw technology to the industrial base, and (2) simply publishes its use cases, objective selection criteria, and COTS competitive procurement budget in lieu of formal Engineering Development Model (EDM)-type solicitations;

Then continuing industrial competition will generate pure COTS offerings that are ever more aligned with government requirements.

If this hypothesis tests true, then the tasks of a Program Manager (PM) become as follows:

- Deploy the best available COTS architectures and products frequently
- Divest of legacy architectures just as frequently
- Document the COTS capability vs. total requirement gap
- Invest to develop technology to bridge the gap
- Iterate continuously

To succeed in these tasks, PMs need an objective framework to enforce policy and manage the myriad and evolving options around technology, architecture, license models, test & certification, contract vehicles, billable hours, etc. The WI team designed CWID IT 5.64 to (1) test the central hypothesis, and (2) collect data necessary to design such a framework. They assumed the following:

- Operationally expert customers must play a continuing hands-on role throughout acquisition lifecycle.
- Certification authorities such as NSA, DOT&E, JITC, DAA, must partner to streamline the acquisition process.
- Efficient technology transfer from demonstration to operations is a primary objective
- Cross-program re-use of capability is a primary objective
- Information Assurance (IA) is a primary objective including
  - An assured approach to manage risk re: need-to-protect vs. need-to-share
  - An assured approach to "discover" valued information and to prevent information overload.

WI designed CWID 08 IT 5.64 to simulate a typical vendor response to a solicitation per the hypothesis stated above. Several commercial members of the WI worked hard to do that realistically.

IV. HYPOTHETICAL SOLICITATION

The government will (hypothetically) begin to field this capability in the first quarter of FYXX ("XX" indicates an arbitrary start date). The Government strategy is to deploy best available off-the-shelf (OTS) capability and contract with material providers to continuously improve their OTS offerings, in context with emergent operational requirements, and in close partnership with the operational user community. Contract awards will depend on actual demonstration of value added in realistic mission simulations. Government priorities are demonstrated utility, rapid deployment, continuous improvement, re-usability within the network enterprise and across program boundaries, and Information Assurance (IA). In this solicitation, "IA" refers to two broad objectives. One is assured methodology for managing risk with respect to the need-to-share vs. the need-to-protect information. The other is assured data strategy for both discovering valued information, and preventing information overload. The hypothetical solicitation language is at Appendix B.

V. PROTOTYPE SPECIFICATION

In keeping with the premise for IT 5.64, vendors respond hypothetically to the hypothetical solicitation. A WI team led by QinetQ North American and Raytheon played the role of vendors. This WI team actually consulted with members of the MDA Community of Interest[3] to develop the following counter-threat mission thread.

1. Unmanned Aerial Vehicle (UAV) sensors monitor shipping traffic including AIS transponder signals.

2. Watch standers compose "User-Defined Operating Picture (UDOP)" (See Note #1) for vicinity of threat vector using the following geospatially enabled services:

   a. Automated Information System (AIS) ship tracks

   b. Meteorology and Oceanography (METOC) warnings

   c. Processed UAV sensor data

   d. Map background

   e. "Intelligent agents" [4](i.e. software 'bots.)

3. Intelligent agents monitor UDOP and deliver "pop up" message when critical conditions of interest occur.

4. Assured web services manage single-sign-on authentication and authorization throughout.

5. Senior coalition watch officer establishes appropriate need-to-know vs. need-to-share procedures and executes coalition MIO to neutralize threat vessel.

To enable this mission thread, the WI team built a demonstration network based on a prototype service stack on a Red Hat LINUX Dell blade as follows:

1. COTS Automated Information System (AIS) ship track web service. Commercial ships report location, course, speed, flag, and other information via VHF transponder. .

2. Map rendering web service built with COTS open source "open GIS" tools.

3. GOTS Meteorology and Oceanography (METOC) warning overlays for GIS web services.

4. COTS Unmanned Aerial Vehicle (UAV) sensor web service. This capability allows an occasionally connected UAV sensor suite to federate with a C2 network across an open source "Tactical Service Bus".

5. COTS Valued Information at the Right Time (VIRT) "smart push"[5] service. When various pre-defined critical conditions of interest (CCI) threshold values are exceeded this web service delivers a pop-up warning message.

6. Medium assurance (Protection Level (PL) 4) GOTS authentication (AuthN), i.e. single sign on (SSO), web service. This capability uses GOTS software and COTS Open SSO standards to allow separation of different levels of access at the same security classification on the same physical networks and/or devices.

7. Medium assurance (PL4 target) GOTS dynamic policy authorization (AuthZ) web service. This capability allows consumers to create or collapse coalition enclaves, i.e. different levels of access at the same security classification, on the same physical network. Dynamic policy that considers attributes related to access control, such as: identity, role, and emergent factors on the ground determines authorization.

The IT 5.64 prototype architecture brokers service transactions across an open source "Trusted" Enterprise Service Bus (T-ESB). The prototype delivers capability to consumers via a "Trusted" C2 Web Portal (TC2P). "Trusted" means that T-ESB assures authentication and authorization at PL4. (See Figure: 1) "Assurance" means that the capability of interest, in this case security, is predictable. "Assurance" does not eliminate vulnerability, it minimizes and quantifies vulnerability. "T-ESB" refers to server-side "back end" activity. "TC2P" refers to the service consumer's experience.

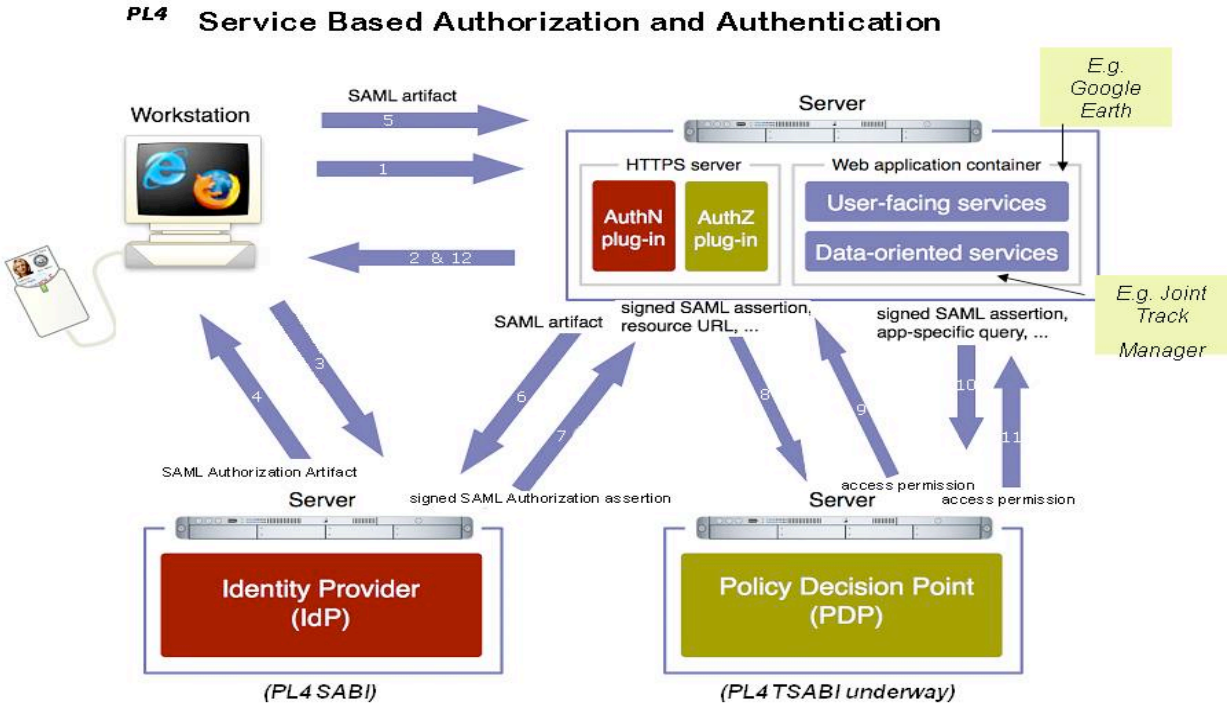

Figure 1: The Trusted ESB brokers information transactions, forcing a Protection Level (PL) 4 authentication and authorization sequence. The authorization depends on a policy provided by the service provider. When a certain individual, playing a certain role, under certain defined operational conditions, points a browser at a URL he either gets access or not. If access is denied the requestor simply receives a standard error message.

The T-ESB is agnostic of content. It simply brokers trusted transactions among a federation of service requestors and providers who accept the risk associated with the trust model. A military "coalition" is an example of such a "federation." Here are the crucial components of a trusted transaction:

1. Requester's identity credentials
2. Requester's role credentials
3. Declared "need-to-share" condition
4. Provider's authorization policy

These four components are independent. Credentials might be biometric, Public Key Infrastructure (PKI), Long Distance Access Code (LDAC), Personal Identification Number (PIN), user-id and password, IP addresses, etc. Authorization policy defines the acceptability of a particular credential format for any particular federation.

"Identity" refers to a unique individual. An individual's attributes include things like nationality, security clearance, affiliation, rank, etc.

"Role" refers to a temporary function such as "watch stander", "first responder", "commander", etc.

"Declared 'need-to-share' posture" refers to emergent conditions. Members of a coalition might agree to some pre-arranged set of events that warrant varying willingness to share information they consider sensitive. For example, they might be more willing to share sensitive information during a temporary emergency. When pre-defined events occur, an authorized watch stander might set an "emergency" condition across the coalition. When events indicate that normal conditions have returned, the watch stander re-sets "normal" policy.

"Provider's authorization policy" refers to a pre-defined set of rules set by a service provider. These rules prescribe to whom and under what circumstances to grant access. The detail of any particular provider's authorization policy is opaque to the T-ESB, and therefore to the consumer. The policy can be very dynamic and granular. For example if a Canadian military member, serving as a watch officer on a particular aircraft, under emergency conditions, may be granted access to an Australian web service. The same or different person, serving the same or different role, at the same or different location, under the same or different condition, might or might not be granted access.

Authorization policy governs the ability to set "need-to-share" conditions. Only authorized individuals serving in authorized roles under appropriate need-to-share conditions *may set* need-to-share conditions.

The WI team delivered the prototype as a lightweight "breadboard" designed in close consultation with multiple potential vendors of "production models". Vendors agreed that if the government actually issued the hypothetical IT 5.64 solicitation they would respond with robust, life-cycle supported off-the-shelf bundles.

VI. CWID 08 IT 5.64 SCENARIO

The IT 5.64 server was deployed at a single node, namely Hanscom Air Force Base. The CWID Coalition watch standers deployed to various internationally distributed sites. They registered their single-sign-on credentials, and consumed "authorized" web services transparently via Internet Explorer or Firefox web browsers. Authorization depended on national identity, mission role, and emergent situation. Therefore, the operating picture viewed at different Trusted C2 Portal nodes varied.

For demonstration purposes, IT 5.64 published arbitrary US security policy. Under this hypothetical policy, US AIS ship tracks are SECRET NOFORN. All other AIS ship tracks are SECRET REL. UAV sensor data is SECRET NOFORN. METOC littoral warnings are SECRET NOFORN. All other METOC warnings are SECRET REL. Accordingly, under "normal" security policy all coalition role players are authorized to view all SECRET REL data streams. No coalition role players are authorized to view any SECRET NOFORN data streams. Under hypothetical US National "emergency" security policy, specifically authorized coalition role players may view the SECRET NOFORN US AIS tracks and the SECRET NOFORN UAV sensor data, but not SECRET NOFORN METOC warnings. Under hypothetical US National "self-defense" security policy, specifically authorized coalition role players in imminent danger may view all SECRET NOFORN data streams. (See Figure: 2.)

NORMAL Policy

	CA	NZ	OC	US
METOC (NOFORN)				X
METOC (REL)	X	X	X	X
AIS (NOFORN)				X
AIS (REL)	X	X	X	X
SENSOR (NOFORN)				X

EMERGENCY Policy

	CA	NZ	OC	US
METOC (NOFORN)				X
METOC (REL)	X	X	X	X
AIS (NOFORN)	X	X		X
AIS (REL)	X	X	X	X
SENSOR (NOFORN)				X

CA = CANADA

NZ = NEW ZEALAND

US = UNITED STATES

OC = OTHER COALITION

SELF DEFENSE Policy

	CA	NZ	OC	US
METOC (NOFORN)		X		X
METOC (REL)	X	X	X	X
AIS (NOFORN)	X	X		X
AIS (REL)	X	X	X	X
SENSOR (NOFORN)		X		X

Details of national security policy is up to nations

Policy is presented as "black box" based on pre-agreed states of urgency

These matrices show snap shot of dynamic US national policy "under the hood" per CWID IT 5.64 scenario

8

Figure 2: Each nation would set its own granular dynamic policy based on a general set of agreed conditions and the specific operational scenario underway. In this case the US is (hypothetically) willing to share some NOFORN data with non-US coalition members under "emergency" conditions and even more under "self-defense" conditions. Which specific data to be released to which specific nation and which specific role player depends on tactical scenario.

WI programmed the intelligent agents with pre-defined critical conditions of interest and threshold values. As the CWID scenario unfolded, these geospatially-enabled agents monitored AIS tracks, METOC warnings, and UAV sensor data "looking for" suspicious activity. Accordingly, when an AIS track approached the 3 mile limit of the US West Coast, stopped squawking as a US merchant, changed course, and increased speed, the VIRT service delivered a pop up message to appropriate CWID watch officer's browser.

In response to this notification of an "emergency" situation, the watch officer immediately used a "point and click" menu to set "emergency" security policy. (See Figure: 3.) The tactical situation demanded that non-US coalition platforms interdict the threat. That situation constitutes a pre-defined "need-share" tactically significant NOFORN track and sensor data. In response, a US national watch stander used a point and click menu to authorize those specific non-US platforms emergency-level access to the C2 Portal. (See Appendix A, Note #2.)

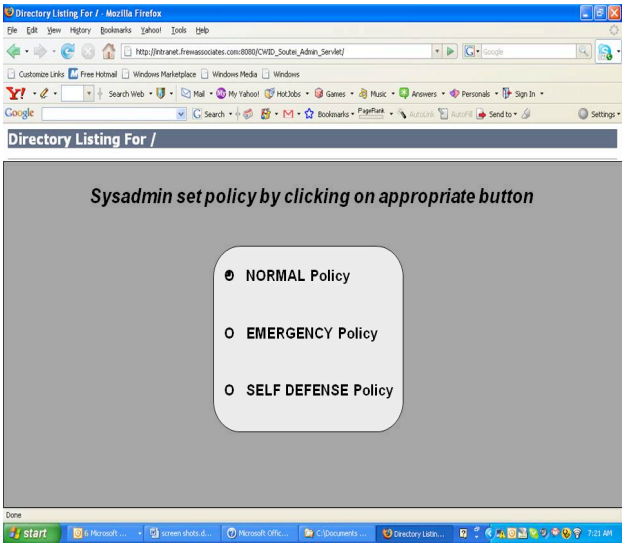

Figure 3: A watch stander with appropriate single sign on credentials can access this "sysadmin" point and click policy menu. The detail of national policy associated with each pre-agreed "need-to-share" condition is opaque to this watch stander.

In the course of the interdiction the intelligent agents "noticed" that a coalition interdiction platform was in imminent danger of entering a mine field depicted on a SECRET NOFORN METOC warning. Accordingly the VIRT service delivered a pop-up message. The alert message triggered a coalition watch officer to set "self defense" conditions. It also triggered a US national watch stander to authorize the endangered vessel to have "self-defense" level of access to the TC2P.

When the Interdiction vessel avoided the hazard and intercepted the threat vessel, the coalition watch officer re-set "normal" security policy.

VII. ANALYSIS

A. The Concept of "Information Processing Efficiency"

The WI team designed the Trusted Command and Control (C2) Portal as a collaborative "service." (See Appendix A, Note #3.) By definition, a "service" must provide value as perceived by the consumer. To "information workers", human processing time is a valuable commodity. It should be spent wisely. Military information workers, e.g. C2 watch standers, tend to be very busy managing multiple information sources. Their specialized jobs require them to spend most of their own human processing time independently. Collaboration is "expensive" because it spends multiple individuals' processing time on the same collective task. Collaboration is only valued if it achieves important objectives not obtainable individually. More bluntly stated, effective communication minimizes confusion and accelerates speed-to-decision. Accordingly, a "budget" established for managing collaborative processing would prioritize "spending" time on actionable information. The budget would limit time spent on "overhead" like establishing "situational awareness."

The WI team used this time budgeting principle to design the TC2P. There were two design objectives: (1) minimize over-all processing time required for collaboration; (2) maximize time spent processing actionable bits relative to time spent processing other bits. This approach is consistent with traditional military C2 Radio-Telephone "circuit discipline." Circuit discipline does not permit distracting idle chat; it conserves bandwidth for priority traffic; it insists on unambiguous, concise, standard language.

The objective of a budget is to achieve efficient resource allocation. Conceptually, for example, one might define "Information Processing Efficiency" as "Utility of Information Consumed" divided by "Total Bits Processed". An issue is how to define "utility" objectively. Different consumers will have different perceptions of utility. However, it is possible for subject matter experts (SME) to evaluate the value of some data types over others. One approach SMEs can use is to identify critical conditions of interest (CCI) associated with plans of action. Plans depend on assumed threshold values of CCI. When thresholds are exceeded, action is warranted. This is the approach many stock traders use. With stock trading, having the stock value information even one or two seconds in advance of others can be worth millions of dollars. These traders subscribe to various services that inform them when threshold values of CCI associated with their portfolios are exceeded. That is the time they buy or sell. In this example traders can literally determine the dollar "value" of specific timely information. In military domains the value metric may be more abstract, but the relatively greater value of actionable information remains clear.

The SMEs for this demonstration were the CWID role players. The role players were fully tasked to manage multiple disparate and overlapping events. Accordingly, they considered "relevant" information useful if it provided new situational awareness. However, they considered "actionable" information at least twice as useful. They considered "irrelevant" information useless because it distracted them from their critical functions. The role players defined "useful relevant information" as "new information pertaining to mission elements at times and places important to mission execution." They defined "actionable information" as "information that forces unplanned action." Role players considered all other information to be irrelevant.

Following this reasoning, we define "Total Bits Processed" as the sum of the Irrelevant Bits (IB), Relevant non-actionable Bits (RB), and Actionable Bits (AB)

processed. We also introduce the notion of arbitrary information "Utility Unit" (uu) to quantify the relative usefulness of messages. Per the subjective preference of the SMEs, we assign a value of 1uu to relevant useful messages, 2uu to actionable messages, and 0uu to irrelevant messages. We consider a bit of information added to browser view of an operating picture in terms of an overlay, pop-up, or track to be a "message".

We hypothesize that TC2P will increase the overall processing efficiency of the CWID information system. The analytical approach is to count the messages processed during IT 5.64, and bin them according to relative utility. We can then calculate Information Processing Efficiency, at least notionally, using the following formula:

IPE=(Utility of Information Processed)÷(Total Bits Processed)

$$IPE = (w_{IB}(IB) + w_{RB}(RB) + w_{AB}(AB)) \div (IB + RB + AB) \quad (1)$$

IPE= Information Processing Efficiency
w=weighting factor, w_{IB} = 0 uu, w_{RB}=1 uu, w_{AB}=2 uu
IB = Irrelevant Bits Processed
RB = Useful Relevant non-actionable Bits Processed
AB=Actionable Bits Processed

B. Calculating the Information Processing Efficiency of the Trusted C2 Portal

IT 5.64 scenario participants were as follows:

2 X Coalition command centers
3 X US command centers
1 X CA Aircraft
1 X NZ Ship
1 X NZ Aircraft

Uniformed military members played roles as coalition watch standers at each of these locations. These role players were involved in multiple independent or loosely coupled Interoperability Trials. They executed the IT 5.64 mission thread, with some variation, over a period of approximately two hour each eight hour day for nine days. The IT 5.64 mission thread called for collaborative activity, i.e. viewing the TC2P operating picture concurrently, three times. That collaborative activity required a total of about ten minutes. During each iteration of IT 5.64, the role players successfully detected and responded to the threat. The generic IT 5.64 mission thread, broken down message by message, is as at Appendix C.

Watch standers participating in IT 5.64 viewed a total of 34 web services messages each day. The TC2P message utility breaks out as 6 irrelevant, 16 relevant but not actionable, and 12 actionable messages. The notional Information Processing Efficiency is calculated below:

$$IPE = (w_{IB}(IB) + w_{RB}(RB) + w_{AB}(AB)) \div (IB + RB + AB) \quad (2)$$

$$IPE_{TC2P} = (0uu(6) + 1uu(16) + 2uu(12)) \div ((6) + (16) + (12)) = 1.18uu$$

What if the SMEs decide to consider actionable information that allows them to intercept WMD to be ten times more useful than situational awareness information? In that case, w_{AB} = 10 uu and the notional IPE for the IT 5.64 sequence calculates to 4.00uu.

C. Value Added by "Need-To-Share" Services

Consider steps three and five above of Appendix C. Note that without the TC2P security services -- *or in this context, "need-to-share" services* -- the messages viewed by the CA and NZ assets would not include the actionable NOFORN information. In other words, the sensor service would have provided critical information to US watch standers. The VIRT service would have alerted a US watch stander. However without a "need-to-share" service, the utility of the NOFORN information is diminished. In that case, four messages that were actionable with NOFORN information become irrelevant without it. The six messages viewed by US watch standers with the NOFORN data remain relevant, but are no longer actionable. The message utility breakout for this sequence becomes 10 irrelevant, 22 relevant but not actionable and 2 actionable messages. The IPE for that case is calculated below.

$$IPE = (w_{IB}(IB) + w_{RB}(RB) + w_{AB}(AB)) \div (IB + RB + AB) \quad (3)$$

$$IPE_{TC2Psans\,ec\,urityservices} = (0uu(10) + 1uu(22) + 2uu(w)) \div ((10) + (22) + (2)) = 0.76uu$$

The IPE without security services is 36% less efficient than IPE of the full TC2P service suite. If SMEs decide that information that allows intercept of WMD is ten times more useful than other relevant information, IPE for this case becomes 1.24uu – compared to 4.00uu is 69% less efficient than with need-to-share services.

D. Calculating Information Baseline Processing Efficiency

To provide a baseline comparison, we assume that basic CWID capability, without the TC2P, includes an AIS ship track "picture". For this baseline case, we assume that the role players simply view the AIS picture three times – the same number of viewing as in the IT 5.64 scenario. This assumption is reasonable compared to typical coalition C2 Concepts of Operations (CONOPS). The message-by-message breakdown for this baseline case is at Appendix D.

In this baseline scenario watch standers viewed a total of 24 messages. 13 are irrelevant, 11 are relevant, and 0 are actionable. The IPE for this baseline case as calculated below is 0.46uu, which is 61% less efficient than the 1.18uu efficiency of the TC2P.

$$IPE = (w_{IB}(IB) + w_{RB}(RB) + w_{AB}(AB)) \div (IB + RB + AB) \quad (4)$$

$$IPE_{Baseline} = (0uu(13) + 1uu(11) + 2uu(0)) \div ((13) + (11) + (0)) = 0.46uu$$

A typical coalition C2 CONOP, without the benefit of automated software monitoring services, calls for human watch standers to view the operating picture frequently. In the baseline scenario above, if watch standers viewed the operating picture just once every 30 minutes, i.e. four times instead of three, the calculated IPE would be 0.34uu. Each time the eight busy watch standers view a low value message, the IPE decreases geometrically. Granted, some C2 "searches" would likely return relevant or even actionable information. However, each time the VIRT service "delivers" a message guaranteed to be useful, and the security services guarantee it can be shared usefully, the IPE increases exponentially. By this reasoning it is clear that TC2P services increase the *assurance* that information processed by busy humans will be useful. This finding in no way implies that C2 watch standers should not "search" for information. Rather, it implies that smart push services -- designed to inform of known critical information elements -- can free up human processing time and provide insight for more intelligent searches. Consumers informed by these intelligent searches, may then add to or revise alert criteria in their VIRT service portfolio.

VII. RESPONSE TO THE HYPOTHETICAL SOLICITATION

Although the IT 5.64 analysis is notional, the approach is viable[6]. It demonstrates that the "value" of information, and the value of *sharing* information, can be credibly quantified through analysis of critical information transactions. This mission level model approach can be modeled in digital formats [7]. SMEs can validate any particular architecture in run-time mission simulations using network performance test tools. The realistic objective outcome are suitable for comparing relative merits of competing architectures. A notional description of such an outcome is described at Appendix E in context with the hypothetical MNIS solicitation.

IX. CONCLUSIONS

The mock off-the-shelf procurement represented by CWID 08 IT 5.64 need not have been mock. Further, the procurement need not have been limited to IT 5.64. If the government had chosen to actually solicit vendor proposals against real procurement opportunities, CWID 08 could have delivered any number of real, pre-approved, supportable, off-the-shelf network capability upgrades. The methodology demonstrated by JITC in IT 5.64 literally allows government to transform its myriad technology demonstration venues collectively into a competitive market place of such capability. (See Appendix F for a discussion of rationale.) The demonstration venues need not be limited to scheduled, formal, large scale events. Any properly configured and certified laboratory can participate. JITC, supported by the W2COG Institute, can assist interested participants perform the requisite configuration, and develop the necessary FAR-compliant documentation.

X. REFERENCES

[1] GAO. (2006). *Best Practices: Stronger Practices Needed to Improve DoD Technology Transition Process.* Washington DC: GAO.

[2] S. Pitcher *Events/Solutions/08/infosharing/files/Pitcher.pdf*. Retrieved 12 10, 2008, from AFCEA: http://www.afcea.org/events/solutions/08/infosharing/files/Pitcher.pdf

[3] Macaluso, J. (2006, Fall). *Maritime Domain Awareness Community of Interest* . Retrieved December 12, 2008, from US Coast Guard/ Proceedings:

[4] Wikipedia

[5] Hayes-Roth, Two Theories of Process Design for Information Superiority: Smart Pull vs. Smart Push, 2006

[6] Hayes-Roth, R., Pullen, M., Blais, C., & Brutzman, D. (2008). How to Implement National Information Sharing Strategy: Detailed Elements of the Evolutionary Management Approach Required. *GMU AFCEA Symposium 2008: Critical Issues in C4I* . Fairfax: George Mason University .

[7] Jain, P., & Pridemore, B. Case study: Net-centric mission threads modeling and analysis using BPMN. *Collaborative Technology and Systems 2008 International Symposium* (pp. 563-564). Irvine CA : CTS. 2008.

[8] Director Central Intelligence (DCI). (2000). *Protecting Sensitive Compartmented Information within Infomation System (DCID 6/3) Manual.* Washington DC: CIA.

[9] Chief of Naval Operations (CNO). *Maritime Domain Awareness Concept.* Washington DC: CNO. 2007.

[10] Carr, A. E. *Maritime Interdiction Operations* . Newport RI: Naval War College . 2002.

[11]Director Central Intelligence (DCI). *Protecting Sensitive Compartmented Information within Infomation System (DCID 6/3) Manual.* Washington DC: CIA, 2000.

[12] *DoD Instruction 8510.01 DoD Information Assurance Certification and Accreditation Process.* Washington, DC: DoD, 2007.

[13] Chairman Joint Chiefs of Staff (CJCS), 2007 6212.01: Interoperability and Supportability of Information Technology and National Security Systems. Washington, DC: CJCSI.

[14] Chairman Joint Chiefs of Staff (CJCS), 2007 6212.01: Interoperability and Supportability of Information Technology and National Security Systems. Washington, DC: CJCSI, 2007.

[15] Department of Defense Instruction (*DoDI) 5141.2 Director, Operational Test & Evalution (DOT&E).* Washington, DC: DoD 2000.

[16] McNamee, D., Heller, S., & Huff, D. Building Multilevel Secure Web Services-Based Components for the Global Information Grid. *CrossTalk the Journal of Defense Software Engineering* . May, 2006.

Appendix A: Notes

1. User Defined Operating Picture (UDOP) is a refinement to the traditional concept of a Common Operating Picture (COP). The idea is that pictures should not be “common”. Rather users should tailor information content based on individual mission and preference.
2. This scenario used a human-in-the-loop to set the various need-to-share conditions and authorization policies. That function can be automated, adding more risk/benefit considerations. The idea is that pictures should not be “common”. Rather users should tailor information content based on individual mission and preference.
3. HQ US Navy SPAWAR has conducted an excellent body of research on the subject of effective collaborative information sharing process. Their approach is called Cross-domain Information Exchange Framework (CIEF).
4. The M&S supporting CWID IT 5.64 was conceptual and functional rather than rigorous and performance-based. Performance based SOA testing is an immature domain and a subject of WI research. The WI can help the government apply and improve existing best-of-breed SOA performance based testing and validation and verification to support an actual procurement.

5.

Appendix B: Hypothetical Coalition C2 Procurement Language

Procurement opportunity:

The government (hypothetically) intends to field MNIS capability with as many generic off-the-shelf components as possible. In that sense the government intends that its MNIS program execution funds "seed" a market for universally useful components. Other government programs are likely to consume components that have been (hypothetically) validated and pre-approved for MNIS application.

1. $10M (hypothetically) budgeted for MNIS COTS procurement in 3Q FY(XX-1)

2. Between four and twelve Indefinite Delivery, Indefinite Quantity (IDIQ) contracts awarded (hypothetically), each with $100M/yr ceiling for FYXX-(XX+5). These IDIQ contracts will be reviewed annually. Renewal depends (hypothetically) on actual performance against source selection criteria.

Assume:

1. Multi-member international Coalition performs MDA and MIO command and control via Internet Protocol network.

2. Government furnished equipment (GFE)* includes the following:

   Government off the Shelf (GOTS) Meteorology and Oceanography (METOC) web services.

   GOTS medium assurance (Protection Level (PL) 4) GOTS authentication (AuthN), i.e. single sign on (SSO), web service. This capability uses GOTS software and open SSO standards to allow separation of different levels of access at the same security classification on the same physical networks and/or devices.

   GOTS medium assurance (PL4 target) GOTS dynamic authorization (AuthZ) web service. This capability allows creation and collapsing of coalition enclaves, i.e. different levels of access at the same security classification, on the same physical network and/or devices. Authorization is based on dynamic policy that considers identity, role, and emergent factors on the ground.

   Streamlined early adopter net-ready assessment process per DISA Federated Development and Certification Environment (FDCE) pilot project. **

*Available at https://svn.metnet.navy.mil (This site has been enabled support user identification and authentication using DoD PKI. For more information on how to get a PKI certificate please visit https://infosec.navy.mil/PKI or contact the NAVY PKI Help Desk at 1-800-304-4636/DSN 588-4286 itac@infosec.navy.mil)

** See https://www.forge.mil (This site is under construction as of 12-19-08)

Task:

The operational scenario includes a geographically distributed multinational Coalition Task Force (CTF). A known threat is that adversaries will attempt to smuggle weapons of mass destruction (WMD) into the West Coast of the US from the sea. The CTF Commander's Intent makes "Maritime Domain Awareness" (MDA) to spot potential perpetuators a top priority. Likewise, Commander's Intent makes "Maritime Interdiction Operations" (MIO) to neutralize perpetuators a top operational priority. To support Commander's Intent, the government requires an assured information system to accomplish, at minimum, the following critical tasks.

1. Establish at least two private information-sharing enclaves on an Internet Protocol network with separation assured at Protection Level 4 (PL4)[8].

2. Add value to the following Maritime Domain Awareness (MDA)[9]/Maritime Interdiction Operations (MIO)[10] threat/mission scenario:

    a. Threat CONOP is to pose as a US Merchant vessel by transmitting false information on Coast Guard Automated Information System (AIS). When threat vessel reaches three mile limit and is screened by heavy shipping and fishing traffic it stops transmitting, changes course for the nearest point of land, and increases speed. Threat CONOP includes attempts to use environment conditions such as low visibility, high seas, or degraded electro-magnetic propagation, to further mask threat vessel maneuvers.

    b. Coalition task is to uncover deception and intercept threat vessel.

Source selection criteria:

In context with the task above, the government will competitively select vendor offerings, and renew contracts, based on a numerical score of proposals. Slide presentations and white papers without substantiating objective run-time demonstrations are non-responsive. Government encourages creative responses that optimize options associated with architecture, technology, license, test & certification, contract vehicles, and billable hours. The government will consider the value attributes listed below in its scoring algorithms. Some of these attributes may be given greater weight than others.

1. Objective run-time demonstration of:
    a. Enhanced probability of coalition members detecting a covert maritime threat
    b. Reduced detect- to-engage time for coalition Maritime Interdiction Operations (MIO)
    c. Assured risk management in balancing need-to-protect vs. need-to-share information across a military coalition
    d. Assured data strategy to prevent information overload in a coalition Command and Control (C2) environment

2. Credible “net-ready” assessment timeline including:
    a. PL4 Secret and Below Interoperability (SABI) Certification[11]
    b. (At least) Interim Authority to Operate (IATO)[12]
    c. Interoperability certification[13]
    d. NR-KPP assessment[14]
    e. Operational Test [15]
3. Lifecycle maintenance model including:
    a. Continuing currency of IT architecture
    b. Continuing customer connection.
    c. Cost
    d. Cross-program re-usability of IT architecture

Appendix C: The generic IT 5.64 mission thread, broken down message by message

1. Senior Coalition Operations Watch Officer tasks all participants to view the C2 Trusted Portal for situational awareness.

   a. Watch standers across the federation view eight messages (See Figure: 4)
   b. Eight messages are relevant; i.e. all information is new, presented in mission context, and pertains to the area and time of interest.

   c. Zero messages are actionable, i.e. information provides useful situational awareness only.

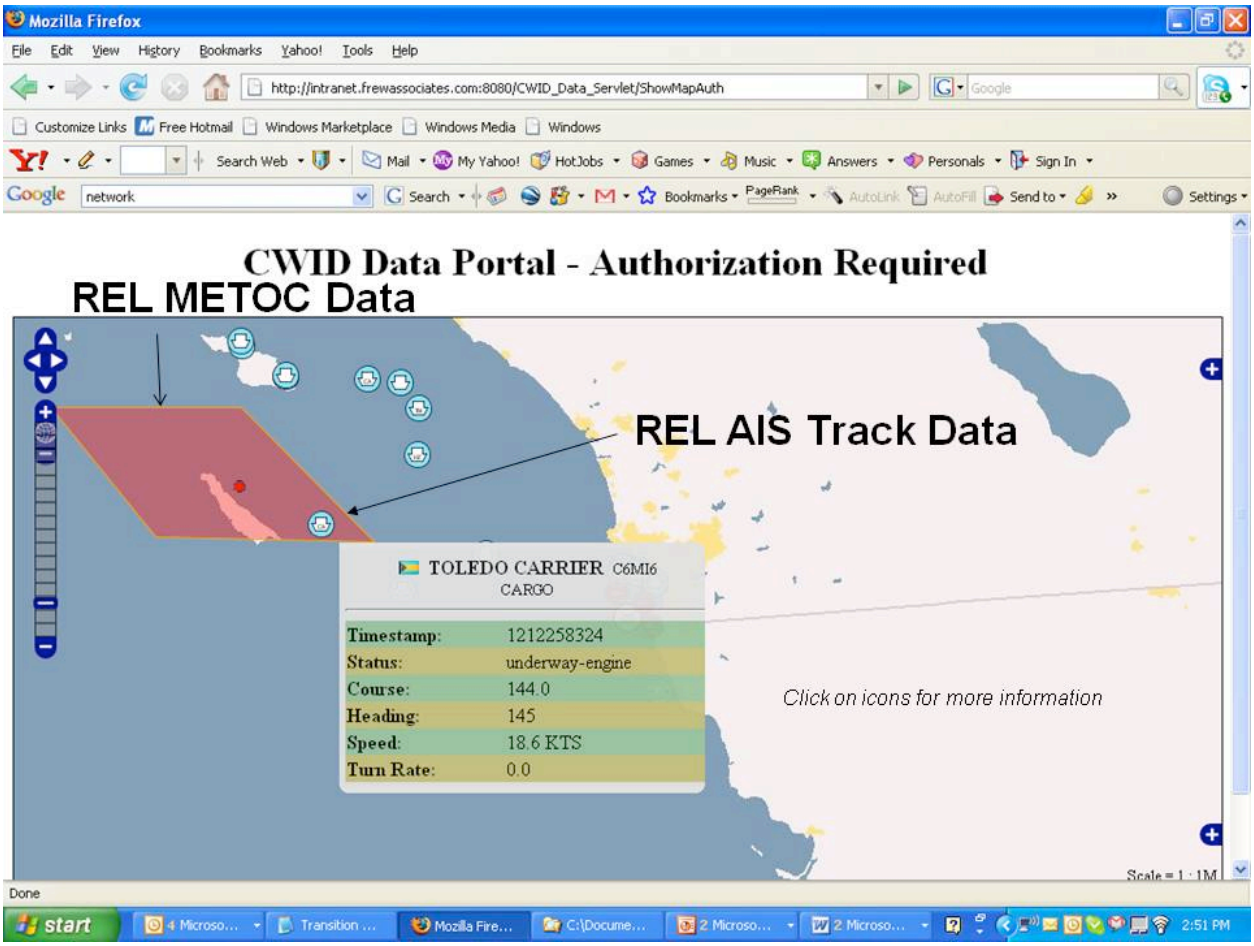

Figure 4: Information is presented as web service messages. Under "normal" conditions this is typical of a message viewed by non-US coalition members. It consists of blue ship icons and METOC warning overlays presented on a open source map rendering tool. Clicking on icons opens windows with more information. Layers of data click on and off. NOFORN Littoral METOC data, US Ship Tracks, and UAV sensor data are withheld.

2 Senior watch officer receives VIRT (Valuable Information at the Right Time) alert message that CCI thresholds are exceeded. NOFORN UAV sensor data and NOFORN ship track data trip VIRT alert message.

   a. One watch stander views one message.
   b. One message is relevant
   c. One message is actionable, i.e. CCI exceed threshold value and force unplanned response.

3. VIRT Alert service message causes senior watch officer to order an interdiction. Mission requires CA and NZ assets. Security services allow senior watch officer to change policy to give CA & NZ assets access to actionable NOFORN data. Senior watch officers tasks participants to view C2 Trusted Portal and issues tasking to CA and NZ assets.

    a. Eight participating watch standers each view a message.
    b. Six messages are relevant. Two messages viewed by the coalition command centers without the NOFORN sensor and ship track data are irrelevant. They provide no new situational awareness.
    c. Six messages are actionable, i.e. six messages viewed by 3 US, 1CA, and 2NZ participants display CCI and exceeded threshold values in mission context. The message forces and enables unplanned action. Without the VIRT service and security services these actionable messages would not have been processed.

4. VIRT Alert service informs senior watch officer that NZ ship is in danger of entering minefield. Minefield warning is SECRET NOFORN.

    a. One watch stander views one message.
    b. One message is relevant
    c. One message is actionable, i.e. CCI exceed threshold values and force unplanned response.

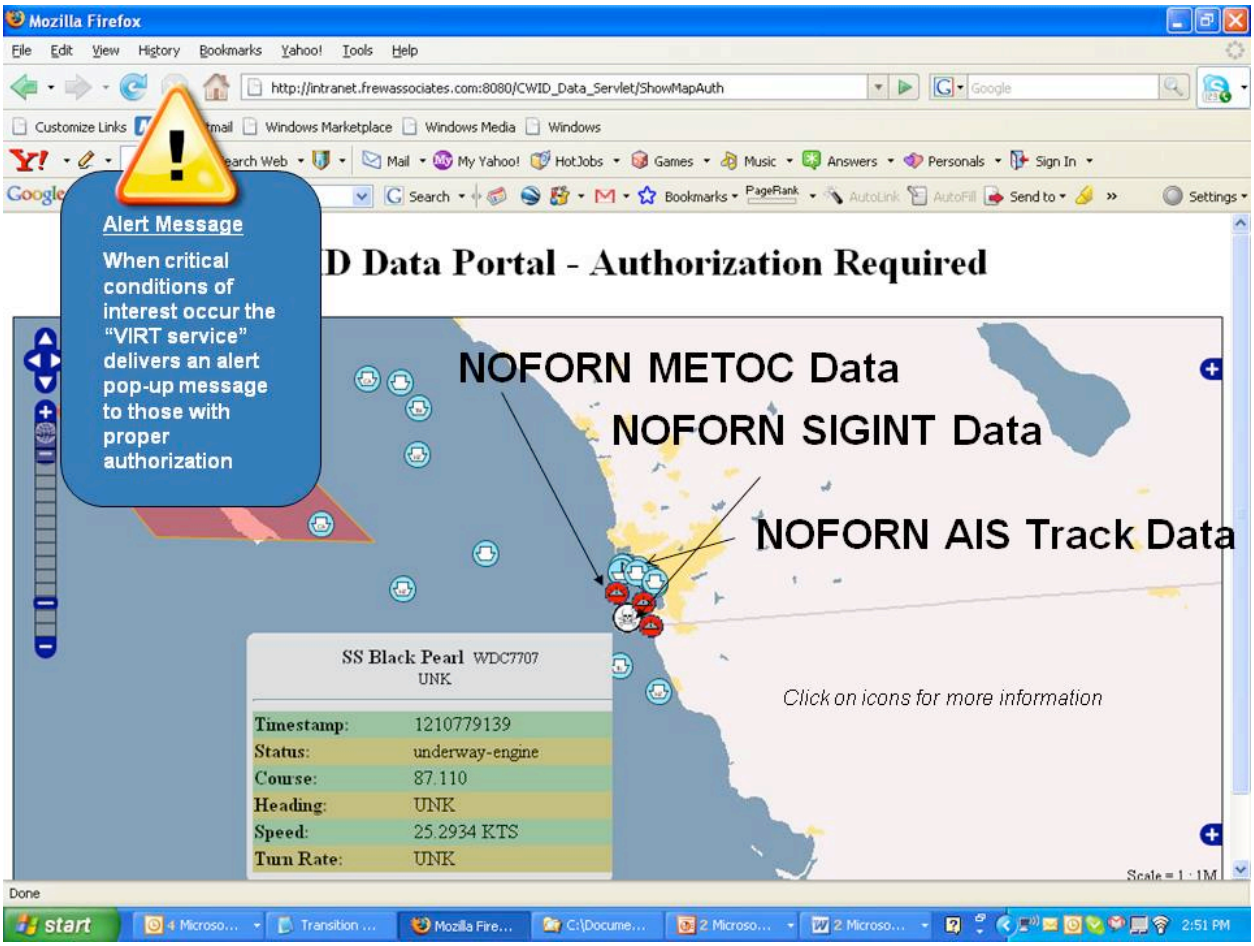

Figure 5: The VIRT service informs the authorized watch stander that a US Merchant ship hit the three mile limit, stopped squawking, and tuned inland. He sees that the SS Black Pearl icon has changed from a ship to a skull and cross bones courtesy of NOFORN UAV sensor services. The NZ interdiction vessel is going to run into one of the SECRET NOFORN mine fields depicted with red icons. This situation calls for "self defense" need-to-share conditions. At the click of a mouse, and the refresh of a browser, the NZ ship views the danger.

5. Security policy allows senior watch officer to grant NZ ship access to NOFORN METOC warnings. Tasks participants to view C2 Trusted Portal. Issues tasking to NZ ship.

a. Watch standers across the federation view eight messages. (See Figure: 5).
b. The four messages viewed by the US participants and the NZ ship are relevant. The four messages viewed by participants without authorization to see NOFORN METOC warnings are irrelevant – they provide no new situational awareness.
c. Four messages are actionable, i.e. four messages viewed by US and NZ ship provide CCI and exceeded thresholds in context that enables required unplanned action. Without VIRT service and security services these actionable messages would not have been processed.

Appendix D: Message by Message Breakdown for Baseline Case

1.Senior coalition watch officer tasks all participants to view C2TP for situational awareness.
   a. Watch standers across the federation view eight messages
   b. Eight messages are relevant; i.e. all information is new, presented in mission context, and pertains to the area and time of interest.
   c. Zero messages are actionable, i.e. information provides useful situational awareness only.

2.Senior watch officer tasks all participants to view C2TP for situational awareness. The threat vessel has stopped "squawking" and has disappeared from the cluttered picture. Even if a busy watch stander notices, there is no means to locate the missing merchant vessel.
   a. Watch standers across the federation view eight messages
   b. Three messages are relevant. The messages viewed at US sites no longer include an icon representing the threat vessel – an indicator, if they notice, of a potential threat. Five messages are irrelevant. Without NOFORN ship tracks they do not provide new information.
   c. Zero messages are actionable.

3.Senior watch officer tasks all participants to view C2TP for situational awareness. By now, if the threat has not been detected and intercepted by other means it is too late.
   a. Watch standers across the federation view eight messages
   b. Eight messages are irrelevant.
   c. Zero messages are actionable.

Appendix E: Vendor Response to Hypothetical Solicitation

"….. In context with the task above, the government will select vendor offerings, and renew contracts, competitively based on a numerical score of proposals. The government will consider slide presentations and white papers without substantiating objective run-time demonstrations as non-responsive. Government encourages creative responses that optimize options associated with architecture, technology, license, test & certification, contract vehicles, and billable hours. The government will consider the value attributes listed below in its scoring algorithms. Some of these attributes may be weighted more highly than others. "

1. Objective run-time demonstration of:

    a. Enhanced probability of coalition members detecting a covert maritime threat

In the IT 5.64 mission model and simulation (See Appendix A, Note #4). TC2P sensors services identified and "tagged" 100% of AIS tracks identified as US Merchant vessel that stop transmitting. VIRT services correlated 100% of tagged tracks against threat profile. M&S results showed 0 false alarms and 100% actual threats detected upon entering interdiction window.

    b. Reduced detect- to-engage time for coalition Maritime Interdiction Operations (MIO)

In the IT 5.64 M&S, non-US assets were required to engage threat. TC2P need-to-share services allowed real-time transmission of essential NOFORN targeting data. The current process requires a minimum of sixty minutes processing time before releasing sanitized or re-classified information.

    c. Assured risk management in balancing need-to-protect vs. need-to-share information across a military coalition

Government furnished authentication and authorization services, together with dynamic and granular security policy, provide mechanism for balancing need-to-protect vs. need-to-share. Capability is assured at Protection Level 4.

    d. Assured data strategy to prevent information overload in a coalition Command and Control environment

IT 5.64 M&S analysis shows that T-ESB/TC2P provides at least 60%, and as much as two orders of magnitude, greater Information Processing Efficiency as compared to the baseline capability. That analysis proves how VIRT services guarantee increased IPE and frees processing time to allow for better informed searches for information.

2. Credible "net-ready" assessment timeline including:

    a. PL4 Secret and Below Interoperability (SABI) Certification
    b. (At least) Interim Authority to Operate (IATO)

The WI team is working with NSA and an operational activity, Fleet Numerical METOC Center (FNMOC), and its Designated Approval Authority (DAA) to deploy the T-ESB (at SABI PL4) in FNMOC's accredited environment under an existing ATO. The team is developing components of the T-ESB in context with the "Multiple Independent Levels of Security" (MILS) architecture and the Defense Information Assurance C&A Process (DIACAP) methodology[16]. An objective is to streamline the C&A process through, re-useable "type-certified" medium and high assurance web service component. This partnership delivered a PL4 SABI certification for an authentication component of the T-ESB in eighteen months. Thirty-six months is more typical. Target is C&A and updated ATO complete by 3rdQ FY09. MNIS DAA can leverage this on-going investment to accredit T-ESB in his/her chosen environment(s).

    c. Interoperability certification
    d. NR-KPP assessment
    e. Operational Test

The WI team has engaged with JITC and DISA regarding items 2.c. - 2 .e. The WI team is performing as an early adopter in the Federated Development and Certification Environment Pilot (FDCE) project. That project aims to perform "net-ready assessment" in parallel with development. CWID 08 IT 5.64 was designed specifically to enable the FDCE concept. The Target to place T-ESB/TC2P on approved DISA approved products list by 4th Q F09.

3. Lifecycle maintenance model including:

    a. Continuing currency of IT architecture

WI team bid includes quarterly software upgrades and a guarantee to install all applicable new standards within three months of their release. Using the methodology demonstrated in CWID 08 IT 5.64, the WI team will continuously evaluate new technology in context with government requirements. WI will propose timelines for intercepting new vectors and divesting legacy architecture -- and associated cost benefit analysis -- for government consideration.

    b. Continuing customer connection.

WI team bid includes a continuing customer outreach program, i.e., one three day visit per month to a site designated by the government. Visits will inform customers of detailed functionality and collect potential new use cases. WI team will also recruit and nurture a distributed "beta community" among the government customers. Input from the outreach and beta efforts will inform quarterly the software update cycle. WI team will maintain a 24 X 7 trouble desk and provide on-site technicians to resolve any trouble tickets still open after 72 hours.

    c. Cost

WI team (hypothetically) bids $10M/yr, renewable annually, to manage T-ESB/TC2P as a network service suite. Bid includes unlimited software licenses, all server-side hardware, and lifecycle support required to deliver capability described herein. Bid includes processing data flows from all discoverable sensor web services. Bid does not include delivery or maintenance of UAV or other sensor platforms.

Alternatively, WI team will negotiate professional services contract required to install and maintain this network service suite at designated government sites.

Alternatively, WI team will negotiate pricing for COTS T-ESB/TC2P appliance (pre-loaded server blades and shrink-wrapped client-side software) including lifecycle support as described here-in.

    d. Cross-program re-usability of IT architecture

WI team will maintain all information technology delivered under this procurement as purely generic "off-the-shelf" commercial standard catalog offerings. WI will offer all capability under unlimited enterprise software licenses. WI team will maintain all furnished GOTS components, and any software developed at government expense, under Open Source Software (OSS) General Purpose License (GPL). WI team will honor any caveats or modifications to GPL required by the government.

Appendix F: Value-Based Acquisition: an Objective, Success-Oriented, Evolutionary Approach

Chris Gunderson
David Minton
Rick Hayes Roth

Value-Based Acquisition: An Objective, Success-Centric, Evolutionary Approach

Executive Summary

Rather than dwell on well-documented information system acquisition issues, we analyze government success stories. We capture best practice in a suite of tools whose familiar look and feel will resonate with acquisition professionals. We demonstrate how those tools can enable rapid, evolutionary information system development. After all, government policies mandate acquiring information systems rapidly & adaptively. DoD in particular has taken a visionary approach that adopts cutting edge paradigms like Service Oriented Architecture and Open Technology Development. Despite overall slow progress, the government has succeeded impressively in some cases. Success stories include continuous technology refresh of deployed systems; government investment in some COTS markets; inserting true COTS as a quick fix; and consuming state-of-the art COTS hardware. Typical government acquisition behavior contrasts sharply with this best practice. Training and tools can solve that issue. Our strategy is to leverage the enduring value of traditional approaches, the lessons learned from success stories, and the innate innovative tendencies of the best employees. We apply the successful continuous re-capitalization model to govern incremental "development" through a suite of objective measures of effectiveness (MOE) and associated algorithms. These tools are based on the concept of "Quality of Service" but address the higher abstraction "Value of Service." "Value" depends on reliability, speed-to-capability, utility, and cost. The algorithms reward modularity, interoperability, and currency. They include a profoundly new concept for government acquisition – that the front end requirements and procurement activity should be governed with process-level systems engineering MOE. The algorithms provide a framework to optimize choices around bundling options, intellectual property, test & certification, and billable hours. They provide an objective means to enforce policy, and a dashboard to monitor policy impact in near real time. We demonstrate the viability of value-based acquisition in a simple commercial use case, and in context with a real on-going military acquisition. Programs can, may, and should leverage the success of the best of their peers, and begin value-based acquisition immediately. The World Wide Consortium for the Grid (W2COG) Institute (WI) can assist.

Government policies mandate acquiring information systems rapidly & adaptively.

A common perception of government "acquisition" bureaucracy as stogy is at odds with much of the actual policy. In particular the general public might be surprised at the enlightened language in the Federal Acquisition Regulations (FAR) about developing information systems. This policy obviously wants government acquisition professionals to be creative and adaptive. The DOD's vision of "Netcentric Operations" (NCO) enabled by a "Global Information Grid" (GIG)[1] is especially ambitious. DoD has spawned various FAR-compliant directives to implement cutting edge paradigms like Service Oriented Architecture (SOA)[2], Open Technology Development (OTD)[3], and "Agile"[4] methods.

Serious issues notwithstanding, the government has succeeded impressively in some cases.

Nevertheless, myriad GAO reports and media articles document horrendous difficulties delivering large information systems like the GIG[5]. In this paper we take a different tack. We notice that many dedicated innovative government employees, and their industry partners, have in fact achieved great success. We think we can generalize and share their successes. We introduce tools and methods that will resonate with the acquisition community.

If we define "success" of an information-system acquisition as "rapidly deployed, continuously improved, capability that demonstrably delights consumers", then, government information-system success stories tend to follow one of four general patterns. See sidebars for elaboration, but we summarize the successful patterns and their associated takeaways as follows:

1. **Technology refresh of deployed systems.** [6] The best government practitioners do life-cycle maintenance on their operational[a] information systems just like the best commercial "e-businesses". That is, they perform continuous "technology refresh", i.e. "recapitalization." They leverage continuous vendor competition in close partnership with their operational customers.

2. **Government investment in COTS markets.** [7] When it does three things well, government drives Commercial-off-the-Shelf (COTS) markets in directions that address critical government requirements. The three critical activities are:
    a. Investing in research to address COTS technology gaps.
    b. Furnishing the resultant intellectual property to the industrial base
    c. Certifying COTS in ways that provide competitive commercial advantage to vendors of compliant offerings. .

3. **COTS "insertion".**[8] Major acquisition programs, working closely with operational customers, often "buy down" a large percentage of their requirements with true[b] COTS purchases. Program offices deploy the COTS capability before the official system deploys, i.e., before "Initial Operational Capability" (IOC). They field it quickly and at relatively low cost.

4. **Rapidly evolving, COTS precludes pre-defining specifications.** Rather than specifying IT architectures years in advance of deploying it, good acquisition professionals now purchase and integrate state-of-the-art true COTS hardware. They negotiate excellent price points, and deploy

[a] "Operational systems" are associated with programs past "Initial Operating Capability" (IOC). That means they are no longer in "development" but are in a lifecycle maintenance status.

[b] "True COTS" is a vendor offering that is not modified to suit specialized customer requirements. It might ship straight from a catalog order. Shrink wrapped software is an example of true COTS. Contracting with a COTS vendor to develop a specialized capability based on "commercial standards" is not true COTS.

hardware in phase with program fiscal execution. [c] If follows that we can teach them to do the same thing with true COTS software.

Information-system failure stories (per myriad GAO reports[9]) tend to follow just one pattern: legacy monolithic system-centric serial processes applied unsuccessfully to develop next-generation federated information-centric systems-of-systems. The takeaways from the failure pattern, contrasted with points 1-4 above, are as follows:

1. **Long serial development of new system.** Serial development process takes many years to deliver initial capability. Program spends money continuously, but no capability is fielded until "Flag Day".[d] Meanwhile, operational customers spend their maintenance budget fixing broken legacy capability.

2. **Government as an uninformed retail customer of commercial technology.** Typical analysis of alternatives and solicitations take years to process. The basis for competition is white papers, PowerPoint, and "who you know". Winning vendor teams are locked in for years. Customer input is formal and time-late.

3. **Government develops large proprietary systems aimed at 100% of the requirements.** Program managers recognize that government requirements are more stringent than commercial requirements. This is especially true regarding security and interoperability. Programs contract with commercial providers to develop specialized capability based on "commercial standards." Specialized capability is more expensive than true COTS. Cross-program security and interoperability remain elusive.

4. **Government "chases" industry standards.** Programs embrace the concept of "open" commercial standards. Their strategy is to specify a particular "stack" of standards to ensure interoperability. Inevitably standards evolve much faster than bureaucratic process can keep up.

Continuous Recapitalization = Good e-Business

Fielded government information systems require lifecycle maintenance. Typically "maintenance" means fixing broken legacy capability. However, "maintenance" may legally mean "refreshing technology". When it comes to IT, the technical difference between "Research and Development" and "Technology Refresh" is arbitrary. The practical difference is the nature of the funds involved, and the associated time line to spend them. Tech Refresh requires operational funds available in the current year. R&D requires "developmental" funds in "programmed" out years. Savvy managers of operational systems use their operational maintenance budgets to incentivize competition among IT service vendors. They work with their customers to achieve continuous capability improvement, i.e., recapitalization.

The success stories prove that the governing directives, per se, do not absolutely mandate the failure pattern. After all, the government employees engaged in the acquisition activity described in the sidebars have managed to succeed under the auspices of those directives. The issue may simply be that governing directives do not translate best innovative practice into formats familiar to rank-and-file acquisition professionals. Tools and training in their use can solve that issue. However, there are some critical tools absent in the current stack of acquisition policy artifacts. The missing tools are "controls"[e] on the acquisition process itself that are as objective and rigorous as the disciplined controls program managers use to make system-level engineering tradeoffs.

---

[c] This assertion is based on personal observation and anecdotal evidence such as proliferation of government-sponsored Indefinite Delivery Indefinite Quantity (IDIQ) contracts with COTS hardware vendors.

[d] "Flag Day" is the date of "Initial Operating Capability" (IOC) of a large system deployed en masse. The Flag Day comes after many years of serial development effort. A flag day contrasts starkly with continuous incremental development and deployment.

[e] In DoD these system-level "controls" are called "Key Performance Parameters" (KPP). KPPS are measures of effectiveness (MOE) computed from algorithms that define engineering trade space.

Government success cases illustrate "best practice".

Government can convert the lessons from success cases into universal "best practice" per the following actions.

1. **Leverage the enduring value of the traditional system-centric approaches.** In particular, traditional "Key Performance Parameters" (KPP) such as "Operational Availability" (A_o)[10] have been very useful to define trade space for program mangers and engineers. A_o is also known as "Reliability". Engineers use the A_o algorithm to objectively calculate the "Quality of Service" (QoS) of a network. Acquisition professionals need abstractions of the A_o concept appropriate for modern system-of-system paradigms such as SOA. Those new abstractions should preserve the following attributes that make A_o a good Measure of Effectiveness (MOE):

    a. Objective, testable, enforceable
    b. Measures critical functionality
    c. Clearly defines options

2. **Leverage lessons learned through early successes in fielding information-centric systems-of-systems.** Analysis of the success stories reveals the following wining behaviors:

    a. Include operational "beta"[f] users in development process
    b. Focus on specific critical transactions per voice-of-the customer
    c. Leverage economy of scale

        i. Incentivize broad competition in the COTS market
        ii. Deliver small increments of improved capability continuously
        iii. Government invests to develop critical shared infrastructure
        iv. COTS products leverage government-furnished infrastructure
        v. Government certification translates to commercial competitive edge

3. **Leverage the innate innovative tendencies of the best-and-brightest employees.** Every good military leader and industrial executive recognizes that human capital is the most precious resource. The best leaders and executives empower their people to innovate. The following actions empower acquisition professionals:

    a. Provide objective guidelines with real, and clear alternatives
    b. Require risk/benefit analysis
    c. Reward risk management
    d. Punish risk avoidance

Government Investment in COTS

The Internal Revenue Service (IRS) provides its tax algorithms freely to industry. The IRS also "governs" electronic tax return legal and ethical standards. The IRS influenced but did not dictate commercial IT standards associated with e-tax returns. An on-line tax return marketplace, supported by robust SOA, now flourishes. Average tax preparation time, and the time it takes to receive refunds has decreased. Numbers of IRS audits has decreased. Profitability of the e-tax accounting firms endorsed by the IRS has increased. The public image of the IRS has improved.

[f] "Beta" refers to the debugging stage of software development. Successful Internet portals use huge numbers of tech-oriented volunteers from their customer communities to help with this process. This approach has proven to be an outstanding way to collect and act on customer input.

Clear, objective, and scalable MOE translate "best practice" into repeatable process.

As Peter Drucker, the quintessential management consultant emphasized "You get what you measure." A critical task for mangers and engineers is to convert desired best practices into measurable and testable parameters. Clearly, the single most compelling "best practice" associated with successful information system is "continuous incremental improvement".[11] Hence, MOE for information systems should consider "continuous incremental improvement" as an essential design specification. This is a profoundly new paradigm for the government! It requires managers to expand the notional information system boundary to include the end-to-end acquisition process. Accordingly, MOE should not only measure run-time system performance. They should also measure "performance" in design-time and build-time.

Per the preceding discussion, the value attributes of an information system are reliability-of-capability, time-to-capability, utility-of-capability, and cost-of-capability. Therefore value-based MOE should define each of those attributes objectively.

Arguably, MOE regarding reliability, time, and cost functions can be universally defined. Different consumers will have different requirements, but they can use the same measurements to make their tradeoffs. However, "utility-of-capability" depends on any given customer's perspective. MOE for "utility-of-capability" must address that need for customization. The customization process will require consumers to define and continuously validate their perceived "utility-of-capability". That feedback loop must span design-time, build-time, and run-time.[12] They may use similar techniques, but the measured parameters may vary considerably.

Algorithms that calculate MOE should enforce acquisition policy. That is, they should pragmatically parameterize policy objectives such the following:

> "…use common sense and sound business process," "…avoid imposing government-unique restrictions", "…include performance-based specification", "…monitor and assess Modular Open Systems Approach… that emphasizes modularity and use of commercially supported practices, products, performance specifications, and performance-based standards," "…Ensure access to the latest technologies" [13]; "…provide for full and open competition", "…a trade off process is appropriate", "… all evaluation factors and their relative importance should be clearly stated", "… Address complex information technology objectives incrementally," "…Facilitate acquisition of subsequent increments", "…comply with commercially acceptable standards," "….Reduce risk by avoiding custom designed components," *"… release long-range acquisition estimates."* [14]

COTS Buys Down the Total Requirement

Acquisition programs that fall behind schedule will frequently take a strategic pause to address urgent requests from their customers. During this period they purchase true COTS capabilities. The COTS ships quickly and satisfies many, perhaps most, immediate requirements. Since COTS products tend to be easy to use formal training is not a big issue. Customers tend to be delighted…. at least until lack of lifecycle maintenance becomes an issue. Program offices are likewise happy. Not only are their customers happy, but the true COTS is also inevitably cheaper than an equivalent increment of "developed" capability.

The algorithms should also provide a framework to optimize choices with respect to program priorities, resource allocation, technologies, architectures, bundling options, intellectual property rights (IPR), testing, and certification. That is, algorithms should help program managers manage continuing competition in ways that minimize emergent risk to specific program priorities.

Modularity, interoperability and portability enable re-usability of valued components. Re-useable, interchangeable components contribute to rapid continuous improvement. Hence historic policies have mandated "compliance" with a particular group of "open" industrial standards. Those policies have not delivered the desired interoperability or re-usability.[g] Value-based MOE approach the issue by treating interoperability and modularity as means to an end. Value-based MOE, measure the end, not the means. If a component is rapidly deployed at low cost, is reliable, and delivers valued information at the right time, it will earn a high score. In that case, the component must have been sufficiently modular and interoperable. Developers are thereby self-incentivized to re-use these "certified successful" artifacts.

Consume State-of-the-Art COTS as a Commodity

Two decades ago, despite a robust COTS market, DoD programs still developed IT hardware per Military Specification Standards (MILSPEC). Until recently, even after adopting COTS hardware, DoD program offices specified the details for future builds (e.g. processor speed, RAM, external storage formats, etc) according to current standards. When it came time to execute the build, the specified hardware was already obsolete. Obviously obsolete equipment is difficult to obtain, expensive to maintain, and suboptimal in any case. Consequently, many government programs have learned to integrate state-of-the-art COTS hardware in phase with actual fiscal execution.

Consider some objective value-based MOE.

The Joint Interoperability Test Command (JITC) has sponsored a World Wide Consortium for the Grid (W2COG) research initiative to study netcentric development, test, and certification issues. As a result, W2COG has developed a suite of algorithms based on traditional KPPs, but expanded per the discussion below.

"Operational Availability" (A_o) [15] serves as our model for a suite of MOE formulated to address various levels of abstraction. Recall that A_o is a system-level MOE equivalent to "reliability." The A_o algorithm objectively calculates the QoS of network data flow.

The A_o algorithm divides "up time" by "total time" in various formulations. In engineering terms, A_o is the level of assurance that data bits will flow at a particular place at any given time." Very reliable systems will achieve QoS scores that approach 1.000.

"Total time" includes trades pace around inherent system reliability, typical repair times, and typical logistics delay times. For example, if a system in a remote location tends to break frequently, investment in on-sight technicians and plenty of spares might bolster A_o to its specified value. Conversely, investments to develop more inherent reliability might decrease over all cost by obviating the need for spares and on-site technicians.

"Information Value Availability" (A_{iv}) is a system-level MOE. It is analogous to A_o, but at a higher level of abstraction. Netcentric engineering paradigms like SOA aim to abstract the need to understand technical details away from busy operators. Hence engineers fielding netcentric systems-of-systems need appropriately abstract MOE. Consider A_{iv} as the "reliability" that valued information will be available at the right time. The A_{iv} algorithm calculates the "Value of Service" (VoS) of a network data flow objectively. The concept of VoS recognizes that not all data, data sources, and data streams are equal in the eyes of any particular consumer. In that sense, A_{iv} is literally a design specification for avoiding "information overload". Hence, VoS is a function of the QoS of a particular data stream, but also a function of the perceived utility of that data stream. Utility depends on factors like security, relevance, timeliness, criticality, functionality, preference, etc. Individual consumers can determine utility subjectively or objectively, but perceived utility will certainly vary across different consumers. Only expert operators

[g] The various communication devices used by first responders to disasters like Katrina and 911 were all built to commercial standards. Clearly that did not enable them to talk to each other. Meanwhile commercial standards evolve so quickly it is impossible for any administrative process to keep up to date.

can define the military "utility" of any particular data flow. Hence expert operators, acting as a "beta" community, analyze critical information transactions in context with realistic mission models. They will assign higher utility scores to data flows that enable desired mission outcomes. The more objective the process, the better it is.

Conceptually, the A_{iv} algorithm divides "Available Valued Bits" by "Total Bits Processed". In engineering terms, A_{iv} is the level of assurance that useful data bits will be preferentially available over less useful data bits. Systems that deliver very reliable, very useful, data streams will achieve scores that approach 1.0000.

"Total Bits Processed" includes trade space around security policies, "discovery" tools, data strategies, and circuit discipline. For example user-defined spam filters can decrease the over-all "Total Bits Processed". "Pop-up" alert messages based on pre-defined critical conditions of interest can increase the "Available Valued Bits". Monolithic security policy might preclude "Availability of Valued Bits" to a coalition partner. Dynamic "Need-to-Share" authorization services might enable "Availability of Valued Bits" to a critical coalition partner. Geospatial services might provide context for determining a bit's "value". Search engines may enhance "Availability of Valued Bits", but will also introduce "expensive" overhead in "Total Bits Processed".

"Net-Ready Availability" (A_{nr}) is a *process-level* MOE. A_{nr} treats continuous improvement, i.e. recapitalization, as part of the "specification"[h] of an acquisition. In other words, it treats the targeted acquisition method as part of the engineered system. Accordingly, A_{nr} is the "reliability" that the acquisition process will continuously deliver valued enhancements to the information system of interest. As previously discussed, this is a new paradigm for the government. [16] The A_{nr} algorithms calculate the "Value of Enhancement" (VoE) objectively. Goals include increased speed-to-capability, and decreased cost-of-capability. One means to those ends is to reward re-use of pre-existing, pre-certified components. Another is to deploy small increments of new capability within regular maintenance cycles. Cycle times vary per level-of-effort of the maintenance action of interest, e.g. software patching vs. upgraded architecture. Modularity, interoperability, and portability all contribute to re-usability. The A_{nr} algorithm includes optional weighting functions to reward value-added attributes. "Value added" might be up-to-date COTS standards[i], use of a favored architecture, greater security, etc.

The A_{nr} algorithm normalizes a comparison of "Maintenance Cycle Time" to "Capability Deployment Time". In engineering terms A_{nr} is the level of assurance that an increment of useful capability will be delivered on cost on schedule. Providers who develop and re-use modular off-the-shelf components to deliver capability seamlessly within routine maintenance cycles will achieve scores that exceed 0.5000 and approach 1.0000.[j]

Optimizing "Capability Deployment Time" requires careful consideration of myriad choices around intellectual property rights (IPR)[k], bundling options[l], billable hours, testing options, certification options, etc. For example, bundling pre-tested and certified services developed by another program adds value and increases speed-to-capability. Contracts to develop and maintain "portable" certified security

---

[h] A "specification" is a formal description of the desired outcome of an acquisition. Good specifications identify test criteria upfront.

[i] COTS software in government systems is almost inevitably out of date. This issue illustrates the need for process-level MOE. Disciplined acquisition process can force interception of better new architectures and shedding the legacy.

[j] If a program manager needs to invent a new capability the development time investment will decrease A_{ec}. If projected values of Aec decrease below 0.5000 the PM knows he's taken on too large an increment. Reusing existing capability takes very little development time and hence enables higher values of A_{ec}.

[k] Intellectual Property Rights issues include, e.g., consideration of expensive enterprise license vs. low cost seat license, and open source vs. COTS vs. Government-off-the-Shelf (GOTs.)

[l] Bundling options include, e.g., network services vs. "thick client" applications, managed services vs. owned capability, and life cycle support options.

components under open source licenses can accelerate accreditation. Expensive enterprise licenses might be cost-effective if amortized beyond the scope of a particular program. Re-allocating billable hours from one capability to another, from one maintenance cycle to the next, mitigates risk of "busting" a critical specification.

"Measured Value" can guide evolutionary acquisition from end to end.

In a value-based acquisition, providers and consumers, together, define both critical mission requirements, and measurable verification and validation (V&V) criteria. The A_{iv} algorithm catalyzes this function by providing a clear objective framework. The A_{nr} algorithm takes input from Aiv to objectively calculate the customer-defined "value" of any particular proposal. Hence A_{nr} provides objective source selection criteria.

Accordingly, value-based solicitations are simply published descriptions of the value-based MOE together with discussion of the procurement budget and schedule. Value-based budgets and schedules include continuing vendor competitive opportunities throughout the acquisition lifecycle. Either the government directly, or a prime contractor, will manage the continuing competition. Government furnished equipment (GFE) includes mission-based test and validation cases. GFE also includes any relevant GOTS components.

Responses to value-based solicitations must include documented working products or prototypes. They may include proposed mission-based validation cases. Responses will not include white papers or PowerPoint slides. Vendors demonstrate their prototypes in accredited laboratories against operator-verified, digitally modeled, use cases. Demonstration cycles are continuous with drops at quarterly or greater frequency. Certification and accreditation authorities, together with beta community users, will validate demonstrated artifacts per value-based MOE

Value-based Work Breakout Structures (WBS)[m] and Statements of Work (SoW)[17] describe this rapid evolutionary process specifically in context with the acquisition of interest. Program manager make source selection decisions based on cost/benefit tradeoffs. Value-based MOE define "benefits" objectively. The same MOE define performance targets in contract incentive clauses. These value-based contracts include frequent review periods. Value-based contracts also include requirements for continuing, documented feedback from the operational beta community.

Throughout this process authorities place certified off-the-shelf components on pre-approved products lists. Contracting authorities award Indefinite Cost Indefinite Quantity (IDIQ) contracts to vendors of pre-approved network components. Multiple programs conduct value-based acquisitions in parallel. Many programs will have similar requirements. Pooled resources enhance economy of scale. In this way government investment fuels a "marketplace" of off-the-shelf net-enabling components.

The broadband services marketplace validates value-based acquisition.

As a conceptual proof of concept, consider an information system composed of household broadband services. In particular, consider how value-based MOE can quantify the value propositions associated with various bundling options for television, Internet, and telephone.

Options for television might include cable and satellite. Say both are immediately available and basic service costs are the same for each. QoS for cable is higher because the satellite signal suffers in strong wind and rain. On the other hand, satellite offers a sports package not available on cable. A sports fan might perceive the utility of a sports package "data stream" to be very high compared to other

[m] A Work Breakout Structure (WBS) is a traditional approach to modularizing development responsibility in appropriate functionality "bins". Modern paradigms like SOA can map to a WBS.

entertainment channel data streams. The sports fan might willingly pay more and suffer some QoS degradation in order to consume the valued data stream.

Potential "capability enhancements" might include a second antenna for the satellite system. That off-the-shelf component might boost QoS to some assured higher level for a specified additional cost. On the other hand, suppose the cable provider invests in a major infrastructure upgrade like laying optical fiber in your neighborhood. The cable provider might bundle Internet and telephone services together with the television package at some relatively small incremental cost increase. By divesting of your "legacy" Internet and telephone services, you can upgrade service and decreased cost. How important is that sports package really?

Value-based MOE quantify all these potential enhancements and bound the tradeoffs. One takeaway is that a providers' sunk cost need not hold a consumer captive. Another is that continuing competition among vendors and technologies inevitably present either an opportunity or an opportunity cost to consumers. Agility is the key to capitalizing on opportunities. *Value-based MOE parameterize agility*.

Value-based acquisition also works for real DoD C2 systems.

JITC's W2COG research initiative has demonstrated value-based acquisition in context with real world military requirements. The venue was Coalition Warrior Interoperability Demonstration 2008 (CWID 08) "Interoperability Trial" 5.64.[18] At the request of Rear Admiral Hight, Deputy Director DISA, the W2COG engaged the Multi-National Information Sharing (MNIS) program office. The MNIS mission is to consolidate and enhance multinational information sharing capability. Program requirements boil down to three objectives.

1. "Flatten" coalition networks
2. Enable data and service "discovery" via semantic interoperability
3. Decrease life cycle costs by leveraging COTS

"Flatten" means to use the same physical infrastructure to support private coalition network enclaves. "Discovery" means dynamically selecting critical bits of information from the huge pool of data available on the network. Flattening networks and enabling discovery requires balancing the "need-to-share" and the "need-to-protect" information. Hence, the demonstration assumed a basic requirement to establish multiple secure coalition enclaves on the same physical network. Central Intelligence Agency (CIA) policy[19] requires "Protection Level 4" (PL4)[n] certification for virtual separation paradigms like this one. Access to any particular enclave depended on need-to-know. Need-to-know changed dynamically per emergent events in the scenario. The scenario included a realistic mission thread around coalition Maritime Interdiction Operations (MIO) and Maritime Domain Awareness (MDA).

The government furnished PL4 GOTS security software components to a group of COTS vendors. The vendors' task was to bundle their capabilities as off-the-shelf offerings with GFE security "inside." Their hypothetical target market was a ~$10M COTS procurement in FY09. The "Utility-of-Capability" requirements were as follows:

1. Geospatial context
2. Relevant data streams
3. Alerts of pre-defined critical conditions of interest

[n] "Protection Level" PL is a graduated assurance scale managed by the National Security Agency. It loosely correlates to the Common Criteria Engineering Assurance Levels. Achieving a PL4 certification is expensive and typically takes years.

4. Dynamic authorization per emergent need-to-protect vs. need-to-share posture

The vendors' prototype included GOTS, COTS, and open source software bundled on a LINUX blade server. CWID watch standers invoked the capability as network services via Firefox or Internet Explorer browsers and point and click menus. Services included, GOTS "Single Sign On", GOTS authorization service, COTS ship tracks, COTS Unmanned Aerial Vehicle sensor data, GOTS environmental information, open source geospatial rendering, and COTS intelligent agents[o]. The government spent approximately one tenth of a man year for the prototype and documentation. Vendors can deliver "shrink wrapped" versions of the demonstrated capability within six months of a funded solicitation.

Post-CWID analysis of objectively quantified the value of this COTS/GOTS service stack. Using notional but realistic user inputs, and value-based MOE, we calculated that this capability enhancement increases the value over the current capability by at least 60% and perhaps as much as two orders of magnitude. The context of the analysis includes policy compliance, and program-specific tradeoffs.

Programs can, may, and should begin value-based acquisition immediately.

Value-based acquisition process and MOE follow from analysis of government and industry successes. Value-based acquisition not only complies with government policy, it provides the measurable means to enforce policy usefully. Further it provides an objective "dash board" for policy makers to monitor success and adjust policy accordingly. Value-based acquisition is agnostic of program owner or size. It is equally applicable at all phases of a program's lifecycle. It does not attempt to identify universal one-size-fits-all specifications. It does identify universally useful tools and methods to quantify value as perceived by any particular consumer. Value-based acquisition applied to simple commercial use cases passes the sanity check. Value-based acquisition applied to an actual DoD information system program, unlike traditional government acquisition practice, also passes the sanity check. Value-based acquisition lacks only adoption by courageous pioneers who agree with Einstein that "The same thinking that created a problem won't solve it!" Acquisition professionals, who agree with Einstein, can break the failure-cycle by taking the following action:

1. **Partner with forward leaning authorities and experts.** There are passionate individuals and offices at, e.g., JITC, NSA, DISA, and Director, Operational Test &Evaluation who are motivated to streamline and improve the C&A, T&E, and V&V processes. There are forward leaning experts in, e.g., open source software, SOA, Agile software development, industry standards, semantic technology, modeling and simulation, policy, contracting, and IA in both government and industry. No one organization or individual is expert in all requisite areas! The not-for-profit W2COG Institute (WI) exists to find forward leaning government and industry experts and to remove the barriers to effective collaborative engineering among them. Engage the WI to find partners who will help objectively define "useful", "secure", "certified", "open", "modular" architecture in your mission context, and to manage the myriad options to field it.

2. **Learn by doing.** The WI "GIGlite"[20] project has identified existing infrastructure and process aligned with value-based acquisition as described above. Use this existing GIGlite capability as "training wheels" to ramp up your own capability, or to find an appropriate outsourced provider. Target a certified value-based testing-as-a-service capability as a first value-based delivered article!

[o] Watch standers program intelligent agents with critical conditions of interest. When agents detect those conditions they send pop-up alert messages to watch stander browsers.

3. **Collect feedback & continually improve.** Actively recruit innovative, tech-savvy members of your operational customer community to serve as a beta developers. Include regular customer visits as a required condition of all contracts. Use those visits to objectively audit performance per agreed MOE, teach new functionality, explore the art-of-the-possible, and collect new use cases. Feed lessons learned into your continuing value- delivery process.

[1] (Joint Chiefs of Staff, 2001)
[2] (Federal CIO's Council, 2008)
[3] (Scott, Mark, & Herz, 2006)
[4] (Fruhling & Tarrell, 2008)
[5] (Government Accounting Office (GAO), 2006)
[6] (Haines, 2001)
[7] (Internal Revenue Service (IRS))
[8] (Boudreau, 2006)
[9] (Government Accounting Office (GAO), 2006)
[10] (Wikipedia)
[11] (Denning, Gunderson, & Hayes-Roth, 2008)
[12] (Meyerricks, Davis, Pipher, & Guthrie, 2008)
[13] (Defense Acquistion University)Defense Acquisition Guide
[14] (Code)FAR
[15] (Wikipedia)
[16] (Govenment Accounting Office (GAO), 2006)
[17] (DoD, 1996)
[18] (CWID JMO, 2008)
[19] (Director Central Intelligence, 2000)
[20] (W2COG Institute)

Boudreau, M. (2006). *Acoustic Rapid COTS Insertion: A Case Study in Spiral Development.* Monterey CA: Naval Postgraduate School.

Code, U. T. (n.d.). *Federal Acquisiton Regulations (FAR)*. Retrieved December 12, 2008, from Acquisition Central : http://www.acqnet.gov/Far

CWID JMO. (2008). *Coalition Warrior Interoperability Demonstration (CWID) 2008 Final Report.* Hampton VA: CWID Joint Management Office (JMO).

Defense Acquistion University. (n.d.). *Defense Acquisiton Guidebook*. Retrieved December 12, 2008, from Defense Acquisition Guidbook: http://akss.dau.mil

Denning, P. J., Gunderson, C., & Hayes-Roth, R. (2008, December). Evolutionary System Development. *Communications of the ACM* , p. 29.

Director Central Intelligence. (2000). *Protecting Sensitive Compartmented Information within Infomation System (DCID 6/3) Manual.* Washington DC: CIA.

DoD. (1996). *Handbook for Preparation of Statement of Work (SOW).* Washington DC: DoD.

Federal CIO's Council. (2008). *Practical Guide to Federal SOA (PGFSOA).* Washington, DC: http://smw.osera.gov/pgfsoa/index.php/Welcome.

Fruhling, A. L., & Tarrell, A. E. (2008). *Best Practices fro Implementing Agile Methods: A Guide for Department of Defense Software Developers.* IBM.

Govenment Accounting Office (GAO). (2006). *Best Practices: Stronger Practices Needed to Improve DoD Technology Transition Process.* Washington, DC: GAO.

Government Accounting Office (GAO). (2006). *Defense Acquisitions DoD Management Approach and Processes not well Suited to Support Development of Global Information Grid.* Washington DC: GAO.

Haines, L. (2001, March/April). Technology Refreshment Within DoD. *Defense ATL Magazine* , pp. 22-27.

Internal Revenue Service (IRS). (n.d.). *Information for e-file providers*. Retrieved November 25, 2008, from Internal Revenue Service: http://www.irs.gov/taxpros/providers/index.html

John Scott.

Joint Chiefs of Staff. (2001). *Global Information Grid (GIG) Capstone Requirements Document.* Washington DC: JROCM.
Meyerricks, D., Davis, S., Pipher, J., & Guthrie, P. (2008). *Independent Assessment Team Report on C2 Data.* Alexandria, VA: Institute for Defense Analysis.
Scott, J., Mark, & Herz, J. (2006). *Open Technolgoy Development Roadmap.* Washiington DC: Deputy Undersecretary of Defense Advanced Systems and Concepts.
W2COG Institute. (n.d.). *About Us/Product Offerings*. Retrieved December 10, 2008, from World Wide Consortium for the Grid: http://www.w2cog.org
Wikipedia. (n.d.). *Availability*. Retrieved November 25, 2008, from Wikipedia: http://en.wikipedia.org/wiki/Availability