Mission Thread Market: A Faster, Better, Cheaper Path to Net-enabled Capability

Chris Gunderson
Naval Postgraduate School, Joint Interoperability Test Command, World Wide Consortium for the Grid (W2COG)
Chris.Gunderson@w2cog.org

David Minton
Planning Systems Incorporated, QinetiQ North America, W2COG
Dminton@plansys.com

Abstract

Joint Interoperability Test Command (JITC) employs the W2COG Institute (WI), a government and industry expert body established by OSD, to serve as a computer network-enabling "Capability Broker." Accordingly, the WI has designed a "Mission Thread Market" (MTM) process to incentivize sustained COTS software competition around government use case requirements in 90 day production cycles. In particular, Government seeks to incentivize industry to bind innovative SOA solutions to government-furnished high assurance services, e.g. for authentication and authorization. WI executed a case study that compares a typical government-managed pilot project to a pilot managed by a Capability Broker. The Capability Brokered project employs the MTM process. Both eighteen-month pilots, executed simultaneously, aimed to deliver the same SOA enabled C2 and high assurance security capabilities. Both used the same baseline GFE software. The MTM process will deliver an open standard COTS/GOTS architecture that addresses ~80% of government requirements; government cost was ~$100K; COTS (e.g. SAML 2.0) is up to date; availability is 2Q FY09 via COTS procurement. The government pilot has not identified any functional architectures or use cases; government cost was $1.5M; COTS (e.g. SAML 1.1.) is eighteen months out of date; availability TBD, but greater than eighteen months. JITC's capability broker has mapped the MTM process to standard DoD procurement methods. It takes about 90 days to establish an MTM from scratch, and an additional 30 days to deliver MTM-based acquisition documents. Establishing an MTM from scratch costs about $2.4M

1. JITC Capability Broker for Netcentric Acquisitions

A request for information (RFI) from the Defense Information Systems Agency (DISA) to support the "Net Enabled Command Capability" (NECC) program, dated 28 June 2007, describes a need for a "Capability Broker", i.e. "… a third party capability broker…to identify and nominate specific technologies and capabilities from the public sector outside DoD, the private sector, or other organizations/activities. NECC may acquire some computing capabilities as a managed service or buy easy-to-implement commercial solutions, and subdivide large projects into smaller components that can be combined using service-oriented architecture (SOA) specifications and standards."

Serendipitously an initiative called "Netcentric Certification Office" (NCO), launched in July 2006 by the Joint Interoperability Command's (JITC) Chief Engineer's office, addresses the requirements of the NECC Capability Broker RFI. That is, NCO specifically focuses on enabling NECC via Service Oriented Architecture (SOA). Further, the NCO project is chartered to use the DISA Federated Development and Certification Environment (FDCE) concept as means to do that. The JITC NCO project employs an organization called the "World Wide Consortium for the Grid (W2COG) Institute (WI)" to be its capability broker.

The Office of the Secretary of Defense (OSD) sponsored creation of the WI (www.w2cog.org) to accelerate fielding netcentric capability. The concept

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
20 MAY 2008	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Mission Thread Market: A Faster, Better, Cheaper Path to Netenabled Capability	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School, Joint Interoperability Test Command, World Wide Consortium for the Grid (W2COG)**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES
AFCEA-GMU C4I Center Symposium "Critical Issues In C4I" 20-21 May 2008, George Mason University, Fairfax, Virginia Campus, The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**28**	

is to create an independent not-for-profit collaborative of government and industry experts to apply best Internet collaborative and e-Business practices (e.g. open standards, open source software (OSS), service oriented architecture, IPv6, etc.) in rapid, agile, discovery spirals. WI members represent international government, industry, and academic organizations and are recognized by their peers as experts in operational, technical, and business aspects of information science and technology. WI created and manages its "GIGlite" (www.giglite.org) on line suite of distributed laboratories to facilitate rapid developing, testing, and certification of network-enabling software bundles.

A key aspect of the WI process is its "openness". WI maintains a low barrier to entry so that contributors from any domain, especially those traditionally outside the defense industry, can join the innovative process. One need not be a member of the WI to participate in WI projects or to use the GIGlite laboratory. Further, WI has established an intellectual property rights (IPR) regime to facilitate collaborative development by: 1. "Open sourcing" Government Purpose Rights to government off the shelf (GOTS) software; 2. Protecting the commercial interests of contributors; 3. Maintaining community ownership of intellectual property created to establish open interfaces and frameworks.

Because WI is a tax exempt not for profit scientific organization (501(c)3), its activity is orthogonal to the Federal Acquisition Regulations (FAR). That is, WI activities are around network science "discovery" not procurement. Hence government and industry participants are free to mutually invest resources without concern over conflict of interest. Should prototype bundles be validated by government participants, any participating vendor is free to "shrink wrap" a productized offering. Government consumers are free to procure the COTS offering per applicable regulations. No promises. Using this model, the WI can help project sponsors apply their own use cases, existing acquisition policies, and regulations to establish and manage "Mission Thread Markets" (MTM) designed to incentivize industrial competition around their requirements.

2. General observations about government computer network Acquisitions

The specifications provided in government requests for information (RFI) or proposals (RFP) often drive specific engineering solutions, to include specific software versions and builds. Development cycles associated with these procurements typically last at least eighteen months. Competing vendors make proposals, but once the procurement contract is awarded the competition stops.

The government development team, i.e. government overseers plus newly contracted vendor(s), generally has no incentive, or legal requirement, to update COTS software builds or versions during post award developmental increments. Because the competition dries up, there is no inherent or natural incentive to maintain the COTS currency. Likewise, this team has no obligation or tendency to adopt an alternative software technology that might appear on the market in the middle of the development cycle. For a notional example lets say the program specifies a thick client like Microsoft Office for desk top administrative applications. Meanwhile, let's say a network service alternative like Google Docs appeared on the COTS market. The team would have no motivation to examine whether Google Docs might satisfy use case requirements better, cheaper, and/or open up access to a broader customer base. If for some reason the government team did happen to reach that conclusion, they would have no freedom to adopt it during the contracted developmental period. However, let's say that after the eighteen month development cycle the PM decides to add Google Docs to the program specifications in the next contract. He will not delete the superseded technology from the spec for fear he may stop satisfying unknown legacy requirements. Hence, the future builds will include both the new and the superseded legacy technology. These builds will almost certainly have incompatible software architectures and spread limited maintenance resources to sub-optimally sustain both the legacy tail and the new COTS.

When confronted with this observation, the government PM might protest that engineering discipline demands developing and complying with rigorous static requirement statements for a build-time increment. The counter argument is that PMs developing software systems for industry don't give their software engineers: 1. Luxury of eighteen months to get to a deliverable; or 2. Freedom to ignore facts of life in a competitive market. Through the use of lightweight, agile and incremental System Engineering practices, successful PMs on commercial projects employ 90 day or shorter software development cycles. They recognize the diminishing return and simply stop supporting customers of obsolete technology vectors (e.g. more than two or three generations superseded).

Frequently, government seeks to avoid these issues by avoiding "development" altogether and use some form of rapid COTS insertion instead. Often "COTS insertion" means taking an existing commercial technology literally off the shelf and deploying it to fill a requirements gap. This approach often works well in the short term. However, the government's long term solution is through traditional acquisition. It will therefore not leverage the COTS insertion technology vector, and will typically take five to seven years to deliver its alternative. Operators in the field are left with inadequate legacy tools, aging COTS alternatives, and a long wait for the promised permanent capability.

Government leaders increasingly recognize the problems described above. In response, they have issued enlightened new policies mandating that government software developers leverage the ultra competitive commercial market by applying, for example, SOA, managed services, and Open Technology Development (OTD). [1][2]

A few early adopters across the government have embraced his policy and are working to adapt COTS market methods to field information processing capability faster, better, and cheaper. Concepts like FDCE intend to provide resources and process models to share and propagate these best practices across the myriad government "verticals." Concepts like "capability broker" intend to jump start the process.

3. Mission Thread Market

JITC is using its *capability broker* (W2COG Institute) to flesh out implementation detail by analyzing e-Biz and e-Gov successes. That is, JITC is studying the way successful commercial enterprises and government activities leverage COTS software, SOA, and OTD to rapidly and continuously improve. (Note that industrial success in this space varies widely. Many companies suffer from issues similar to those that plague most government programs. Further some new-think government acquisition initiatives have been quite successful.) Best practices and common patterns of failure have emerged from the study. In sum, these lessons learned point to the Mission Thread Market model: a broadly scalable and repeatable process based on best COTS software market practices; aimed at government-specific use cases; including embedded, adaptive, objective, risk/reward based "net-ready" validation and verification; and executed via standard DoD acquisition artifacts and development cycles. Note that COTS tools can be used either on a live network or via simulation to verify and validate according to objectively defined "net-ready" criteria.

The first lesson is to *beware the fatal error of expecting SOA, OTD, COTS competition, Open Source Software (OSS), or other e-Gov methods to decrease over all network costs!* Rather these e-Biz methods can *avoid excessive IT sustainment costs*, and therefore free funds for *re-capitalizing* via innovative COTS & GOTS software deployment. Arguments promoting overall IT cost savings through e-Gov initiatives will inevitably cause those "savings" to be redirected from IT support to pay bills in other areas. That said, *deliberately fueling and leveraging commercial competition over government requirements can achieve more over all value per dollar spent.* Achieving that increased value/dollar ratio is the over all objective of the MTM model. Some specific goals and associated metrics are described below:

Improve currency of embedded COTS software, intercept new COTS vectors, and sunset archaic software: As previously explained, government development process almost inevitably leads to sub optimal, expensive legacy software issues. We can objectively determine the currency of any embedded COTS product and hence use "currency" as the basis of contract service level agreements (SLA).

Satisfy larger percentages of government requirements with relatively cheap generic COTS software: Government contractors working on different programs with the same generic information processing requirements, continually and repeatedly develop proprietary software to satisfy to satisfy them. We can objectively measure what percentage of the overall requirement is satisfied by COTS/GOTS investment. (Note that COTS tools can measure and report the detailed content of any software stack in terms of percentages of code under various licenses.) If that number increases, it indicates that our COTS market strategy is working.

Identify COTS capability gaps to address with government research investments: Having captured a greater percentage of the COTS potential per the previous bullets, and by comparing the COTS gaps identified across multiple programs, we can objectively define and prioritize research investments aimed at the missing capability. When government research delivers promising technology, government

sponsors will furnish it as "open source" GFE. Vendors can then improve it and bundle it in COTS vectors. A lead metric of success will be increasing percentages of "government open source" appearing in COTS products.

Analysis of government and industry success stories indicate that the following approach will deliver the goals described above:

Procurement strategy: 1. Oversee a continually spiraling Agile "bake off" wherein vendors bundle their products (at their expense) in Federal SOA compliant packages, demonstrate them against published use cases in a Federal SOA community laboratory; undergo Federally approved validation and verification. (Note that approaches like MITRE's Mission Level Modeling (MLM) can use intuitive user interfaces to convert descriptions of mission threads into objective, machine readable, design and test criteria.); receive pre-approved certification based on objective net-ready assessment criteria. 2. Buy or lease best value pre-approved service bundles on a rapid refresh cycle.

Requirement statement: Broadly announce information processing use cases for Federal business/mission outcomes, critical processes, and IT architectures in lieu of detailed requests for information (RFI) and/or requests for proposals (RFP). Do not constrain the vendor engineering solution. Announce also the size and schedule of intended service-based procurements.

Government Furnished Equipment (GFE): Exercise government purposes rights to the software the government pays to devlop: provide reference implementations of, including open license to, government-developed SOA; Establish a government-brokered network laboratory; Provide government approved "net-ready" T&E, V&V, and C&A services @ fee for service.

Source selection criteria: Objectively-defined mission-based measures of effectiveness; Quality of Service (QOS) targets; compliance with objective NR-KPP criteria; legacy COTS issues; viability of technology vector; off the shelf availability vs. specialty offering; Certification and Accreditation strategy; service orientation; etc.

Source selection board: Include operational customer, and representative from independent industry expert body, in addition to usual representatives from agency program office.

Procurement method: Employ "free and open competition" and "COTS procurement" (buy or lease) options. Establish pre-approval for successfully "certified net ready" COTS SOA bundles.

4. Case Study

JITC is using the W2COG GIGlite distributed lab to demonstrate the validity of the mission thread market (MTM) hypothesis. The control case is a government program that aims to field military command and control (C2) capability via SOA and is in the piloting phase. Call it Program X to avoid parochial issues. Program X devised a series of limited technical experiments (LTE) to address a variety of issues associated with brokering, federating, and managing SOA security services. Two particular services are authentication (AuthN) and authorization (AuthZ). Program X wants to leverage as much COTS and GOTS as possible (especially SOA enabled GOTS like NCES) and comply with GIG policy regarding NR-KPP. Information Assurance (IA), including certification and accreditation, is a particular concern. Accordingly, Program X intends to pioneer the Defense IA C&A Process (DIACAP) and deliver a SOA reference implementation with a secret and below interoperability (SABI) certification. This is consistent with W2COG project goals to incentivize industry to bundle SOA solutions with government furnished high assurance services for security. From a business perspective, Program X wants to field adequate, accredited (i.e. system assured), affordable capability faster than typical DoD acquisition pipelines.

The Program X demonstration use case is only loosely defined at the moment, but it aims to create private coalition enclaves on a secret network, enable effective data discovery and sharing, and add value to C2 objectives such as coalition planning.

Program X and W2COG intend to deliver SOA reference implementations that addresses these requirements and constraints. Program X is using a traditional acquisition approach and has identified an engineering team that includes contract and

government employees. Program X is also evaluating the MTM approach. Accordingly, WI has assembled a self selected engineering team that includes representatives from government and industry. One industrial team member is common to both projects. This case study compares and contrasts the two approaches.

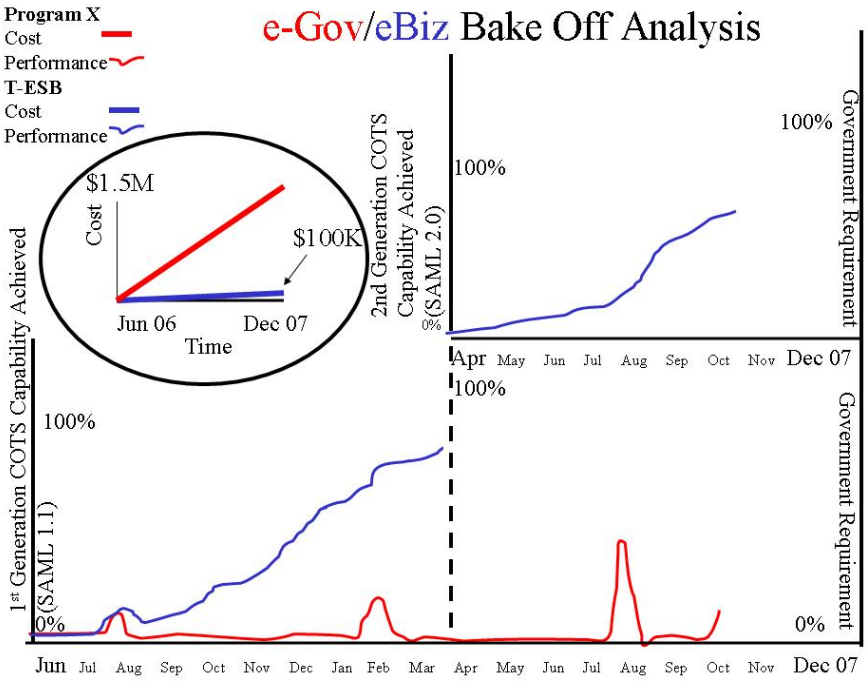


Figure 1: Case study "bake off" results. Red lines are government project; Blue lines are M-T-M project. Note that achieving 100% of any COTS generation capability still generally falls short of the total government requirements. In this case the T-ESB team applied most of the potential COTS capability to achieve about 80% of the government requirements for high assurance authorization and authentication. Note also that commercially motivated T-ESB team necessarily adopted the 2nd generation COTS capability regardless of impact on cost or schedule, while without competitive pressure, the government team did not. The majority of the T-ESB development costs were borne by the commercial participants in anticipation of competitive advantage in specifically foreseen Government procurements.

See Figure 1. Program X conducted three LTEs. In each case the contract vendors were tasked to bundle the GOTS IA services for AuthN and Auth Z in different configurations at a government laboratory. In each case the technology functioned properly within the government specified configuration and narrow constraints of the experiment. The government collected data and gained useful insight into COTS/GOTS technology performance and limitations. The COTS limitations were of particular concern.

Define "use case" as a narrowly described set of mission outcomes, technology architectures, and process models associated with a targeted capability. In each LTE, the experimental configuration changed because as of this writing, the Program X use cases are evolving. This is not a pejorative statement. Program X is using the LTE series to help define the use case. However, this comparative analysis is presented from the industrial perspective. Clearly industry does not yet have visibility into Program X's targets. Therefore, the government's industrial partners can't help solve the government's COTS implementations problem. Certainly, industry at large can not. Accordingly, shortly after each LTE the Program X COTS capability returned to near zero.

Meanwhile, the MTM vendor team members each joined the project because they have customers in mind. The members believe that bundling their companies' capabilities with the GFE IA services will give them a competitive edge. To do that bundling, the MTM team built software service architecture around the concept of a trustworthy, "open", Enterprise Service Bus (ESB). They chose a standard called Java Business Integration (JBI) because it is open source, very modular, composable, and adaptable. They had previously built extensions from a JBI ESB to DISA's Netcentric Enterprise Services (NCES). Therefore, it was relatively easy for them to build similar extensions to AuthN and AuthZ, which they received as GFE. The MTM team

has applied lessons learned at each of the Program-X LTE, and are using Agile methods to continually add and subtract C2 services and resources to the T-ESB "stack". Hence, their COTS capability curve climbed steadily.

The MTM team developed the use-cases sub-optimally because their all-volunteer experimental effort lacked operational customers until very late in the project. Finally however, target operational use cases have emerged as follows:

Technical use case: T-ESB (includes AuthN+AuthZ) + High Assurance Platform (HAP) (HP NetTop Client as proxy) + ESRI GIS Client + C/JMTK Geospatial Appliance (CGA) + JBISoft intelligent agents + Raytheon Tactical Service Bus and UAV Sensor Services + HP Mercury/Systinet Audit Services. Because each information transaction across the ESB is forced to invoke the IA services, the *MTM Team calls its architecture Trusted-ESB (T-ESB).*

Operational use cases:

1. EUCOM will use UAVs for counter drug maritime patrols. The UAVs will monitor Automated Information System (AIS) VHF ship-to-ship squawks. Merchants not squawking are likely to be smugglers and will trigger an alert. UAV's will use T-ESB to feed various COTS versions of the "User Defined Operational Picture (UDOP)". UDOPs will have different content in different coalition operational centers based on each coalition's membership.

2. US Navy Meteorology and Oceanography (METOC) centers have general access to data from all NATO nations. Certain NATO nations do not share weather data freely with each other for commercial reasons. There are exceptions for certain emergent military situations. The sharing is governed by bilateral agreements that can be coded into rule based access criteria. The US Navy will use T-ESB to populate US only and NATO UDOPs with METOC data. Authorization criteria will be NATO rule-based access according to emergent operational considerations.

Requirements	Program X (Gov't Pilot) Delivered	T-ESB Team (MTM Pilot)
Demonstrated value re: operational use case	Unknown	1.Enables EUCOM ISR tipper for coalition drug interdiction. 2.Enables multi-version coalition C2 (METOC) COP
High assurance identity service (PL5)	Unknown	SABI PL4
Multi-Level Security	Multi-level viewing of GENSER + SCI data at rest + Guard	Multi-level viewing of GENSER + SCI data at rest + Guard
Viable Technology Refresh	Superseded version of COTS s/w e.g. SAML 1.1	Current version of COTS s/w e.g. SAML 2.0
Affordable	Unknown	Commodity pricing
Deployable off the shelf and Interoperable	Unknown	Open Standard ESB (JBI) + COTS/GOTS

Figure 2: Bake Off deliverables. T-ESB does not fully support government requirements, but will deliver a COTS commodity product that is a substantial step in the right direction. By "open sourcing" GFE GOTS, and incentivizing industry to follow its preferred approach to net-work assurance, the government ensures that the next COTS generation will address more of its requirements. Program X is organized as a tech demo and will not deliver a deployable product until follow on developmental spirals.

See Figure 2. Note that the T-ESB will satisfy approximately 80% of the government use case requirements for C2 + IA services. However, for example, it will not allow automatic access back and forth across security domains. T-ESB will use a GOTS "guard" (e.g. Radiant Mercury) or COTS high assurance VM ware (e.g. NetTop) as a work around. To achieve true Multi-Level-Security, the government will need to invest in continued research in high assurance web services that can leverage new COTS vectors for high assurance silicon chips and operating systems. Further, COTS discovery services are not adequate to support the ad-hoc collaborations envisioned by the EUCOM use case. Government, again, must invest in the research necessary to enhance the state of the art in semantic technology. However, this low cost, interoperable, 80% solution is ready to demo and certify within the next several months.

The original specification for the Program X LTE series called for SAML 1.1. Security Assertion Markup Language (SAML) is an XML standard for exchanging authentication and authorization data between security domains. SAML is an essential component of the AuthN/AuthZ service stack. A new SAML version was released in early 2007. The MTM team reacted to that fact-of-life by re-coding the T-ESB to include the latest version. They did this automatically because they realized that nobody will buy a COTS stack that is built on outdated software. Accordingly, after a brief re-configuration period, the T-ESB capability continued to improve.

Per Figure 1, the Program X team has not reacted to any of the SAML updates. Keeping SAML current is one example of several that demonstrate the inherent difficulty Program X had in keeping up with COTS. Re-coding for SAML 2.0 would require adjusting the original specification documents and re-allocating resources from tasks perceived as higher priorities. Certainly there is no competitive pressure that would drive the Program X government team to consider the configuration change as a normal part of its development process. As a result, the product the government proposes to deliver will become more and more out of date. Implementing the inevitable down stream change to the newer and better COTS capability will become ever more complex and expensive.

The Program X LTE series is funded at $500K per six month build time interval. By the end of CY07 it cost the government $1.5M. By contrast, the MTM demo, which used by Program X for some small studies, will have cost the government about $100K. The time and material investment associated with both projects is similar. However the vendors in the MTM demo used internal R&D funding (IRaD) to develop the capability in pursuit of competitive advantage for their COTS offerings. They are targeting several specific DoD procurements.

5. Results Summary

To summarize the case study results, Both Program X and the MTM team started with the same baseline GFE code. The Program X engineering approach was to align the GFE with legacy system technology. Program X demonstrated its capability in March 08. There is no stated expectation of an operational availability. Presumably, since Program X is not creating a COTS bundle, it will depend on the standard DoD RDT&E pipeline to deliver capability to the field. That means it will take at least another eighteen months. Government contract costs were about $1.5M. COTS in the Program X software stack (e.g. per SAML 1.1 specification) is about 18 months out of date.

The MTM team engineering approach was to bind the GFE to an open COTS architecture from the start. The MTM team is on a path to demonstrate its capability against government requirements by June 08. They expect to achieve a SABI ticket as an outcome of that demonstration. The shrink wrapped, "certified net-ready" COTS T-ESB bundle will be available for procurement by mid FY09. The up front development cost the government about $100K in contract costs. COTS in the T-ESB bundle will be up to date (e.g. compliant with SAML 2.0).

While this outcome may come across as damning to Program X, it should not. Virtually all DoD software development efforts have similar results. Program X, to its credit, executed a narrowly focused, low cost pilot series that leverage their previous investments. Further, it has supported the MTM concept development and is studying options to leverage the MTM methods in its next AoA phase. Major government programs (we all know who they are from the bad press they receive) often get identically disappointing outcomes after investments of $100M's and many years of work. This is the phenomena Dr Barry Boehm and Jo Ann Lane compare in a recent *Cross Talk* article[3] to playing Roulette where you bet all your acquisition money on one spin and hope for the best. He describes an alternative "incremental commitment model" (ICM) and compares it to Texas Hold 'em – a game that allows you bet a little bit, learn a little bit, and then bet more if things are going your way. *MTM is simply a practical way for federal*

programs to use vendor competition to apply ICM to their software acquisitions.

6. Competition

The necessary catalyst for MTM success is competition. Observe figure 3. The key is for the government to find ways, such as those suggested in the MTM hypothesis, to incentivize COTS developers to continue to compete re: government use cases after initial contracts are awarded. If government can do that, the cost/capability will begin to fall, and the speed to capability will increase. That is a well documented aspect of software markets that support other enterprises. As in those other markets, at some point the government will reach a point of maximum efficiency. At that point the government program-of-record will deliver COTS information processing capability at about the same speed and costs as it is being produced and consumed in industry - rather than five to seven years later at premium price points.

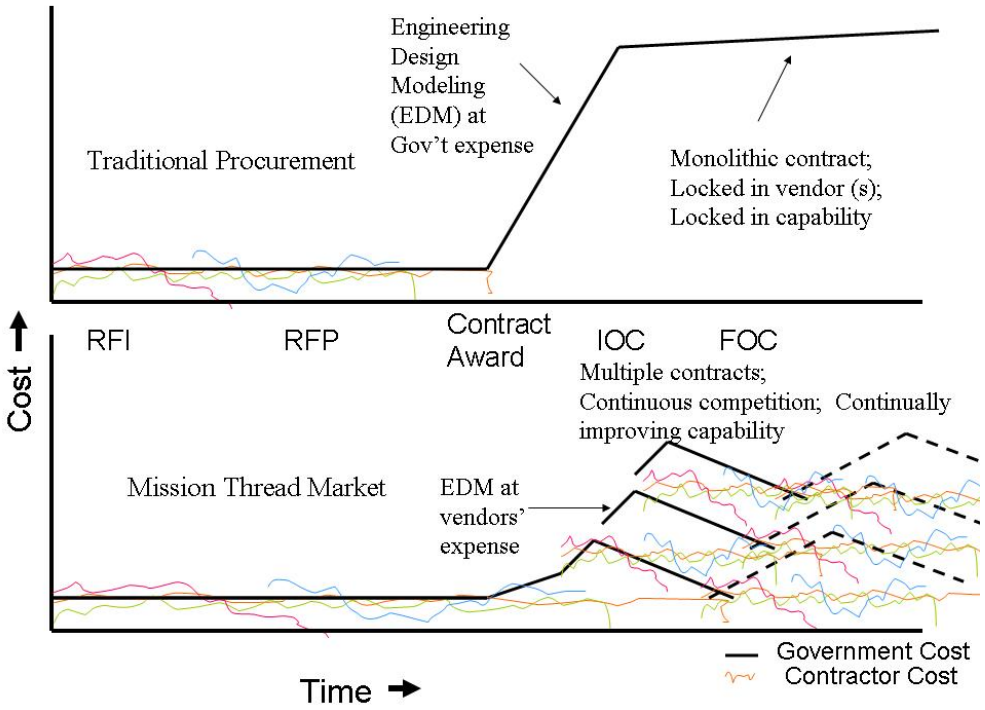


Figure 3: In traditional procurement vendors compete for big bang procurement and then stop at contract award. Capability delivered remains virtually stagnant for program life cycle. In MTM procurement, vendors continuously compete for sub contracts that are re-evaluated, e.g., biannually. Prime contractors are incented to refresh COTS via SLAs requiring continuous re-capitalization.

On one hand, government officials frequently point out the inadequacy of COTS to satisfy rigorous government operational requirements. That thinking leads to government investment in large monolithic proprietary systems, hard-wired to specific, gigantic government requirements. On the other hand, the government, with no influence over the COTS software market, simply buys whatever Microsoft, Oracle, IBM, etc. sells when it comes to satisfying smaller or more mundane requirements. For example, is PowerPoint or Excel really optimal for Pentagon requirements? Who knows? By expanding the Mission Thread Market across the universe of government software procurement, MTM mitigates both issues. That is, COTS venders will increasingly develop and bundle their offerings in competition for specific government sales opportunities.

Clearly it is good for the government to have industry compete over government capability requirements. However, there is a less desirable aspect of competition in play. The various government authorities compete with one another over "who's in charge?" Said another way, government advocates for one approach to policy compete continuously with advocates for alternative

approaches. This *administrative competition* is based on speculation. That is, policy writers theorize that if they require certain behaviors, then certain capabilities will result. Policy competition *winners* issue directives based on their theories. For example, policy writers have speculated that if government IT system procurements specify "industry standards"; then resultant information systems will be interoperable. Administrative competition has led to various iterations of "use industry standards" policy for decades, and has yet to achieve widespread interoperability across government information systems.

In point of fact, IT changes so fast that it is impossible for policy created via any bureaucratic process to keep up. Businesses that successfully leverage information systems don't even try to write company policy about it. They just incentivize their IT service providers to *do it*, where "it" is defined in terms of outcomes to enable. A Mission Thread Market gives government policy owners similar hands-on leverage. By converting desired policy outcomes into published use cases, performance metrics, and source selection criteria, policy makers can use study money to leverage Vendor IRaD. The policy-based use cases will allow vendors to build various COTS/GOTS stacks that either do or don't achieve the outcomes. When a bundle satisfies the requirement, it becomes easy and profitable for developers to satisfy the policy makers' intent: they simply build on top of the documented policy-based *reference implementation*. Lessons learned in this market process then inform the next iteration of use cases and policy-based performance and selection criteria.

Another aspect of administrative competition occurs among government sponsors who are incentivized by the acquisition process to compete with each other for resources. Many information processing requirements are the same for multiple programs. Yet, the current hierarchal acquisition process results in repetitive, but incompatible, capability delivered. After all, the various sponsors are not incentivized to, nor is there a process that allows them to, leverage mutual investment to deliver shared capability. The MTM provides both incentives and process by encouraging competition among the competing approaches to solutions, regardless of who develops them.

7. Acquisition Strategy

Virtually all technical acquisitions require some type of acquisition basis, e.g. in industry "venture capital", "IRaD", or "follow-on development" are common approaches. Government addresses this issue in FAR Part 7 and DODI 5000.2 by requiring an "Acquisition Plan" and "Acquisition Strategy."

An artifact embedded in the "Acquisition Strategy" is "Source Selection Criteria". The government may use "Qualified COTS" as a source selection guide. Note that DoD 5000 series traditionally defines Commercial Off the Shelf (COTS) as "Non-Developed Item" (NDI) Commercially produced software, i.e. NDI, is not necessarily "off the shelf". As previously discussed, often the government pays its developers to develop software capability that is already available as COTS. MTM defines COTS software as "software available either shrink wrapped, or as a managed service, straight from a commercial catalog." The government may use "Catalog offering" as source selection criteria.

COTS software that was never officially "required" and/or tested and/or certified per acquisition regulations nevertheless is ubiquitous in government computer networks. For example, IPv6 is embedded in virtually all COTS office products. For that matter, COTS office products themselves (e.g. MS Office) were not generally required, tested, or certified prior to deployment. Traditional acquisition strategy tends to ignore that reality, but certainly Government may specify "leveraged GFE COTS legacy" as a selection criterion. The advantages are two fold: First, "legacy COTS" means that pricing and licensing models are pre-approved. This pre-approval allows the government to avoid the long expensive "earned value" analysis generally required to purchase NDI [1]; Second, government can benefit from vendor innovation around the inherent capabilities of the new technologies, like IPv6, that will inevitably ship with current versions of COTS software.

MTM enables life cycle maintenance via re-capitalization, as compared to continuously repairing a legacy network. Such recapitalization requires that selected COTS vectors be sustainable on the market place. Therefore "viable technical trajectory" is a legitimate source selection criterion.

NR-KPP should define a pragmatic set of measurable and testable parameters. These should

[1] "Non-developed items" (NDI) is the traditional term used in DoD acquisition language for commercial products. However, NDI does not necessarily mean "off-the-shelf", i.e. available from a catalog. Often NDI means that the government pays a vendor premium prices, per "earned value analysis" to develop a proprietary solution for what is likely to be a generic requirement. Theoretically the government can then execute "government purpose rights" to enable other vendors to re-use this software for different programs. However, it has historically been very difficult for the government to actually execute these rights.

address level of service, information assurance, network assurance/performance, software assurance/performance, data interoperability/assurance, and mission enhancement. *NR-KPP assessment should validate that a particular software architecture is net-ready*. *One assessment criteria should be that all the COTS components of that architecture must be current.* This means that any particular *software architecture must have an associated lifecycle maintenance model that can credibly keep embedded COTS up to date*. W2COG can assist MTM sponsors to define these NR-KPP criteria, which can then be set as source selection criteria.

Mission Thread Market Estimated 1st Year Cost and Schedule

Cost		Schedule in Days After Contract (DAC)	
• Develop/maintain acquisition documents	$445K	• Establish Use cases:	70 DAC
• Establish & run marketplace 1st year	$325K	• Establish lab :	80 DAC
• Set up lab ($150K ODC)	$323K	• COTS jamboree:	100 DAC
• Establish C&A/test docs	$425K	• First vendor lab demo:	120 DAC
• Jamboree	$289K	• Revise acquisition documents:	120 DAC
• 3 X 90 day tests (2, 5 days ea)	$750K	• Second vendor lab demo	180 DAC
• Final lab demo (TRR)	$142K	• Second documents revision	195 DAC
• Update and transfer lab for IOC	$55K	• Third vendor lab demo (TRR)	270 DAC
• **TOTAL**	**$2754K**	• Final documents revision	290 DAC
		• COTS Evaluation (SS)	330 DAC
		• Installation ready products	360 DAC

Figure 4: This estimate assumes use of existing infrastructure, 90 days ramp up, 3 X quarterly development cycle to deliver multiple installation-ready products.

Certification and accreditation (C&A) is a very difficult, long, and expensive process required by various government agencies before a "system" may deploy on a government network. Recent NSA GIG IA policy introduces the concept of "quality of assurance" (QOA), aiming at an assurance model analogous to the QOS model. To achieve that objective, NSA mandates that C&A evolve into a component-based, rather than system-based, process. NSA desires that SOA enabled systems of systems be composed of certified components and achieve accreditation relatively quickly and cheaply. Therefore, net-enabled or net-enabling products require a C&A roadmap. The roadmap must indicate the direction and level of assurance possible, as well as the incremental (high assurance component-enabled) steps planned to get there. WI is pioneering this new approach to C&A by offering it as a vendor incentive. By including "C&A roadmap?" as a selection criterion, government can use vendor innovation to help improve the C&A process.

"Full and Open Competition" is a preferred method of government procurement. Clearly the government wants to get more value per investment dollar by encouraging industrial competition. The MTM improves on typical acquisition strategy with respect to this government objective by: 1. Appealing to a broader industrial base; 2. Reducing constraints on vendor innovation; 3. Enabling vendors internal R&D (IRaD) funds to be spent on government's developmental requirements; 4. Sustaining broad vendor competition beyond contract award.

8. Acquisition Plan

"COTS Procurement" is a legitimate basis for planning acquisition. MTM is simply an approach to COTS Procurement specifically tailored to a sponsor's use cases. Note that the MTM COTS Procurement method is especially applicable when multiple sponsors seek to leverage each others' investments in shared infrastructure. Further MTM COTS Procurement can support government investment in Analysis of Alternatives (AoA) (e.g. JCIDS); RDT&E engineering prototyping (e.g. Pre-milestone down-select); development; and/or life cycle maintenance. The general plan is as follows:

The WI is a tax exempt, independent, not-for-profit capability broker. WI can receive government or industry funds to rapidly establish a government-approved development and test environment, at cost, for participants. The environment will scale on top of existing infrastructure and be configured either inside or outside government firewalls using .mil, .gov, or .org environments according to sponsor desires.

Sponsors and/or their supported operational communities will specify use cases, i.e. narrowly defined set of mission outcomes, technology architectures, and process models (e.g. mission level models) associated with a targeted capability. Use cases will provide the basis of demonstration, testing, V&V, and certification. Note that modeling and simulation will be used for much of the V&V. Very short and simple BAAs, RFI's, and RFPs will describe use cases, GFE, and anticipated procurement schedules. Contracts will include incentives and penalties re: SLA's and MLA's (mission level agreements) around the use cases. SLA's will include the need for decreasing infrastructure sustainment costs in order to free resources for both refreshing GFE software technology, and retiring superseded software technology.

The capability broker, in this case WI, will distribute use cases broadly and solicit MTM participants. The solicitation will respect any specified sponsor constraints, e.g. ITAR. The capability broker will then manage quarterly demonstration cycles.

The government (e.g. JITC) will perform risk/reward based adaptive V&V and net-ready assessment of the COTS/GOTS software architecture, per objective NR-KPP criteria, as an included aspect of the COTS/GOTS bundling cycles. Note that NR-KPP includes IA considerations such as C&A – not necessarily a certification or accreditation, but at minimum, a specified path to C&A. "Adaptive" means the tester will assess capability against government policy and sponsor's use cases and will referee risk/reward based acceptability thresholds. Assessing the software *architecture* for net-readiness, rather than a particular build, allows a program's Tailored Test and Evaluation Master Plan *(T-TEMP) to require the current COTS software build at each evaluation phase* (DT, OT, IOT, C&A). The fee for this NR-KPP assessment service can be borne either by the sponsor or the vendors according to sponsor preference.

The government will assign pre-approved status to bundles that are successfully validated against sponsor use cases, and have been assessed as generally net-ready.

The MTM Source Selection Board should include the usual representation from the sponsoring program or project office. Additionally it should include a representative from the supported operational community, and a representative from the capability broker. The capability broker is both independent and expert regarding the state of the art of the COTS software market. ***If multiple sponsors with similar requirements choose to collaborate, they can use the MTM source selection process a ready-made approach to federated governance.***

---

[1]Gallagher, Sean. (Mar 24 2008). Croom: Acquisition done better, faster, cheaper. *Federal Computer Weeky.* Retrieved Apr 29, 2008 from http://www.fcw.com/print/22_6/features/151969-1.html

[2] Scott, John, Lucas Mark, Herz, JC. Prepared for Ms Sue Payton (April 2006). Open Technology Development Roadmap. Retrieved April 29 2008 from http://www.oss-institute.org/NCOSPR/OTDRoadmap_v3_Final.pdf

[3] Boem, Barry and Lane Jo Ann; Using the Incremental Commitment Model to Integrate System Acquisition, Systems Engineering, and Software Engineering; STSC Cross Talk, Oct 2007.

World Wide Consortium for the Grid (W2COG)
Institute: *Assured* Value-of-Information-Service (V*oIS*) *across a networked enterprise*

"Better networked capability - faster, and cheaper - through adaptive collaborative, value-focused, architecture, engineering, and acquisition

Chris.Gunderson@W2COG.org
(o) 703 262 5332
(m) 831 224 5182
www.w2cog.org

1

Mission Thread Market (MTM): A Faster, Cheaper, Better Path to Netcentricity (A JITC - W2GOG Project)

Chris Gunderson
Chris.gunderson@w2cog.org
David H. Minton
Dminton@plansys.com

2

W2COG “GIGlite”

- Independent (501(c)3) government-industry net-enabling research project partnered with JITC; not a program
- Hands dirty in real commercial and government engineering and procurement activity; not a standards body
- Brokers government and industry experts for consultation, demos, and prototypes at cost; i.e., a “capability broker”

3

Observations

- COTS software in government systems is generally out of date at IOC and falls farther behind throughout life cycle.
- Government requirements process does not intercept new COTS s/w vectors or sunset archaic s/w requirements.
- Government rapid technology insertion methods generally lack sustainment tail.
- IRT the above, enlightened *e-Gov* policy *mandates* COTS, SOA, OSS, and “best” industrial practice (e.g., ABC, FDCE, OTD, etc.)

➢ ***e-Biz unwritten “policy” is to <u>leverage competition</u> in the marketplace…***

4

Problem

- At home, a warfighter can text message his children and trade photos with them using his cell phone. At war he can use a stovepipe circuit to send e-mails without attachments
- At home and at war, a terrorist can and does text his associates using Google earth.

5

Solution

- Get *sustainable* COTS information processing capabilities into the war fighting kit faster
  - Often tried, never very successful
  - Success is prevented by an archaic legacy acquisition method designed to build embedded computer systems
  - Given modern SOA and distributed services, the success of the archaic method can only decrease
  - Success requires a modern acquisition method

6

What New Modern Method?

- "Mission thread marketplace" (MTM) for acquiring information processing tools for warfighters
- Federate GIG COTS/GOTS development and certification through a "NetCert Logo" qualification process
- How is this method different?
  1. Increases and sustains competition
  2. Decomposes traditional acquisition risk into four manageable components and makes managing risk factors basis of competition

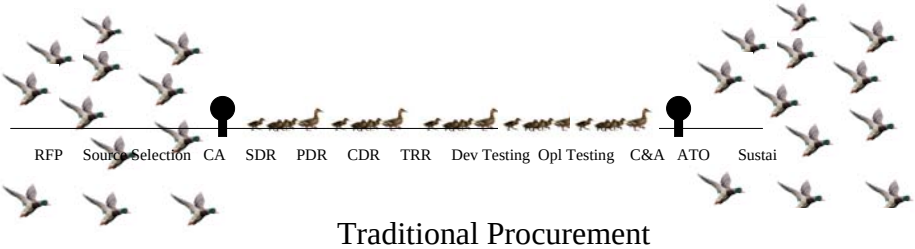
7

Traditional S/W Acquisition Risks

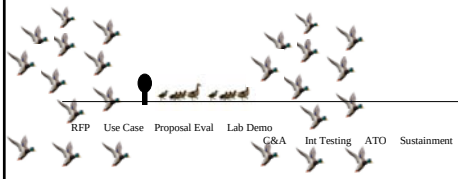
- Cost and Schedule
  - Risk managed by continuous competition and frequent deliveries
- Interoperability
  - Risk managed by measurable/testable net-ready criteria
- Performance
  - Risk managed by Mission Threads
- Assurance
  - Risk managed by certified, reusable, high assurance GOTS components

NetCert Logo Program = "NR-KPP + C&A inside"

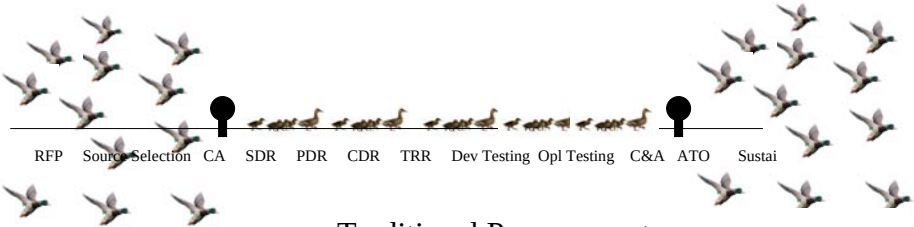
8



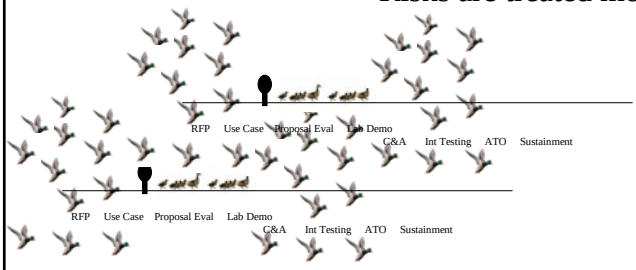
Traditional Procurement
Risks are treated monolithically and serially



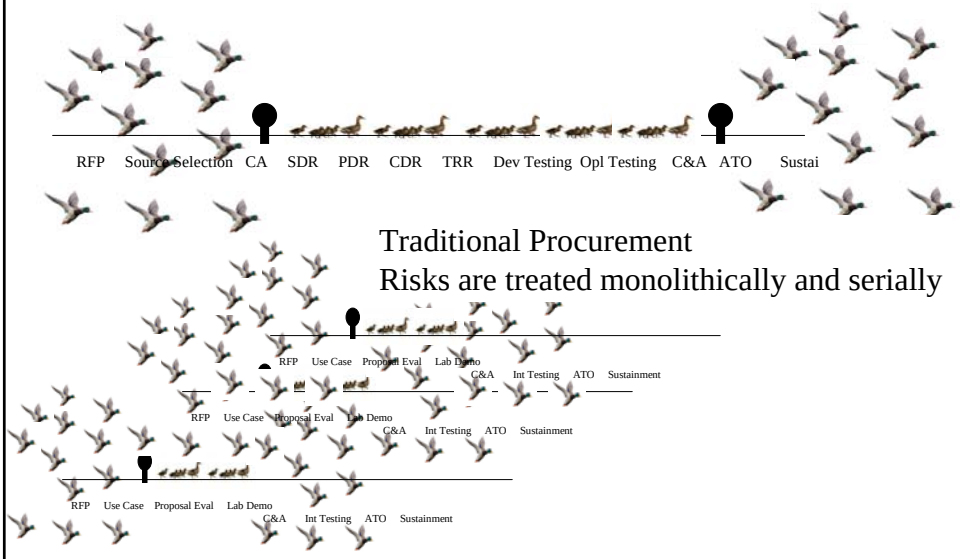
Mission Thread Market Procurement
Risks are treated iteratively and in parallel 9



Traditional Procurement
Risks are treated monolithically and serially



Mission Thread Market Procurement
Risks are treated iteratively and in parallel 10



Traditional Procurement
Risks are treated monolithically and serially

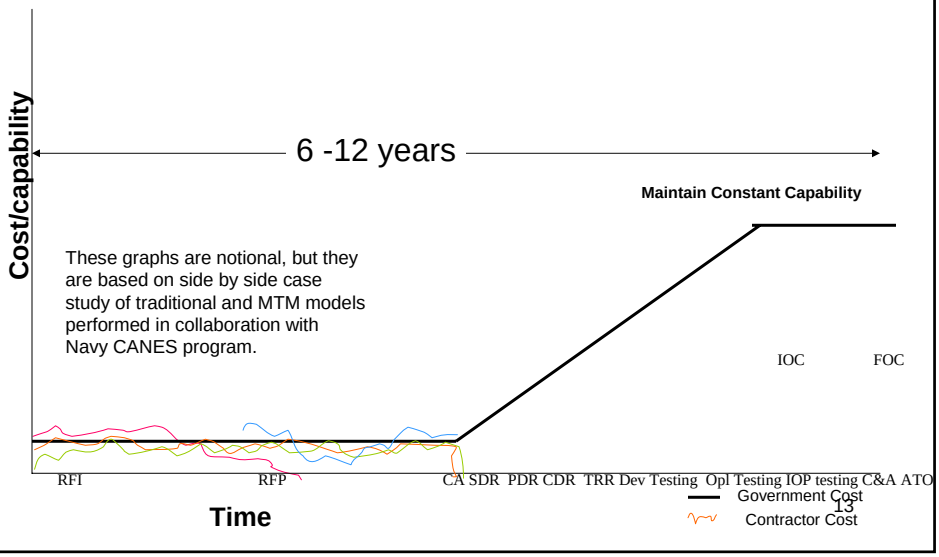
Mission Thread Market Procurement
Risks are treated iteratively and in parallel 11

Market Competition

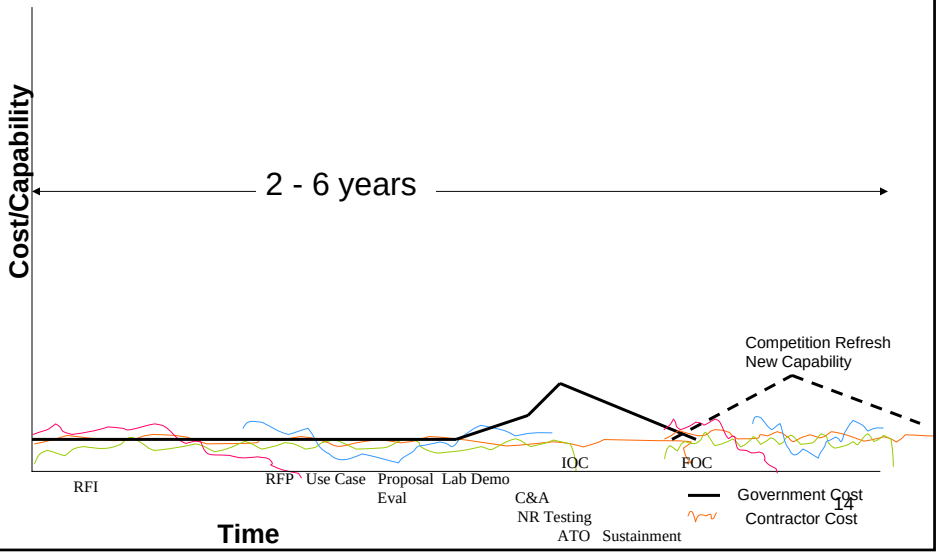
- Treats the four main Acquisition risks in parallel
- Adds and sustains competition past traditional contract award, decreasing cost, and risk

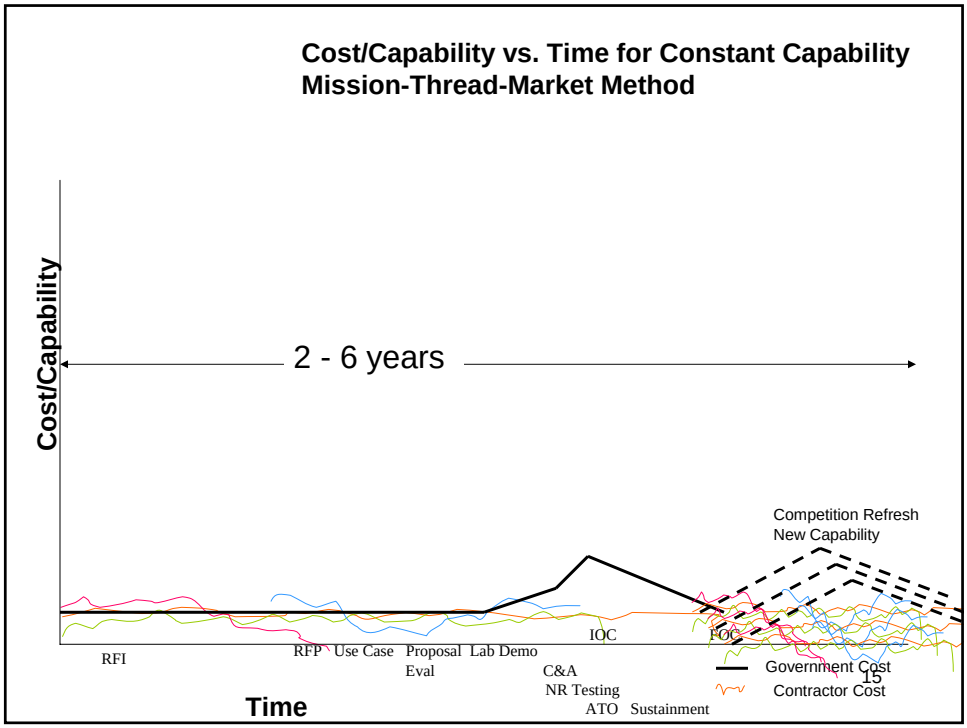
12

Cost/Capability vs. Time for Constant Capability Traditional Procurement Method



Cost/Capability vs. Time for Constant Capability Mission-Thread-Market Method





Market Model Acquisition Strategy

- Identify and manage components of acquisition that can reduce risk and make it possible to deliver better information processing capability faster
  - Exploit new NDI/COTS DoD/IC GIG Acquisition policies
  - Extend and expand pure COTS competition for DoD/IC information processing capabilities
  - Require prototypes over paper studies for decision support
  - Shorten delivery cycles
  - Incentivize PMs and COTS vendors to participate
    - Furnish pre-approved GOTS components
    - Streamline C&A
    - Furnish V&V to put COTS on approved products list
  - Create boiler plate process and artifacts to achieve all the above via “NetCert Logo” program

Good Housekeeping NetCert Logo

6

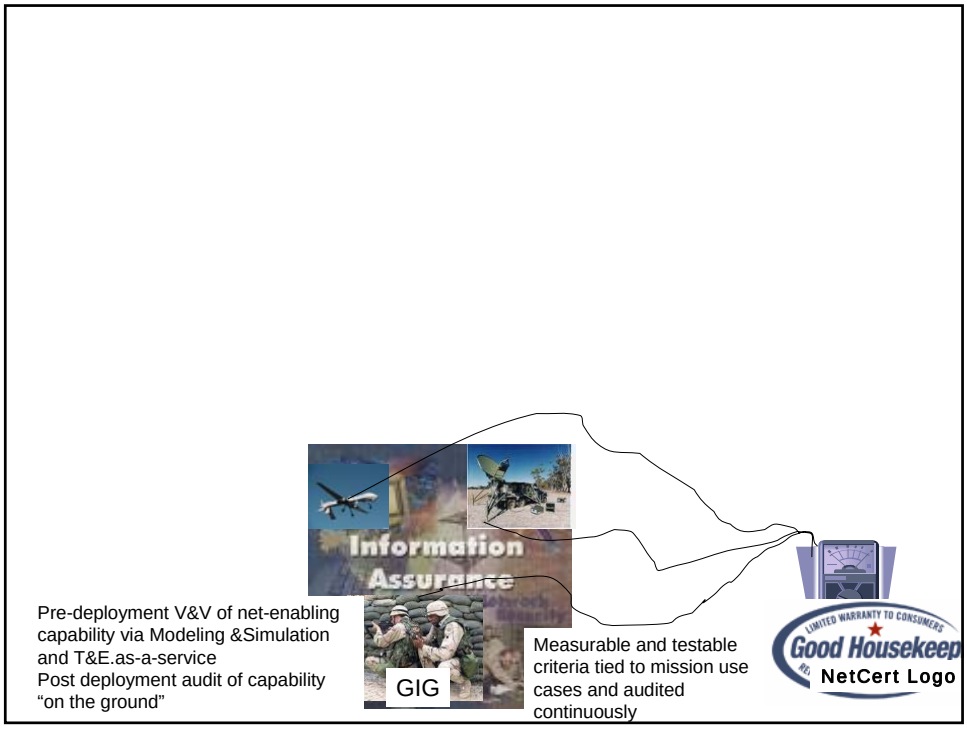
NetCert Logo Concept

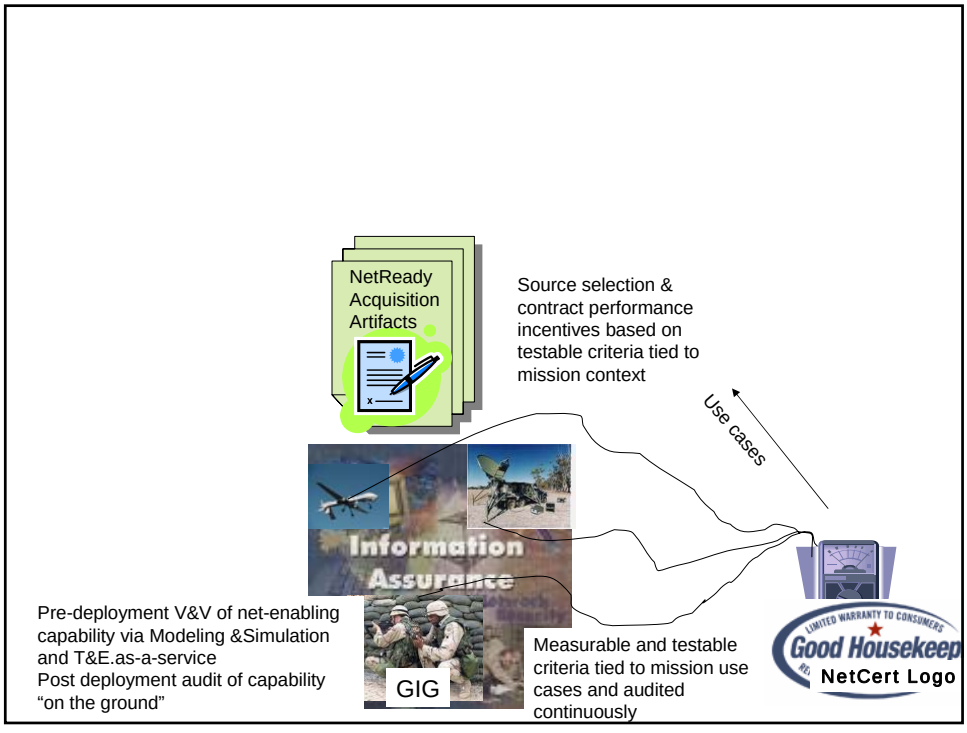
- Implementation strategy for federated development, T&E, and C&A of GIG capability
- Create a literal federation of independent government, industry, and academic “net-ready” certification labs
- Define minimal federation membership requirements re: standard net-ready criteria, methods, and tools
- Certify compliant labs with a JITC “NetCert Logo”
- Maintain “living” and continuously improving NetCert master template lab at JITC
- Place COTS & GOTS products certified by logo’d labs on GIG approved products list

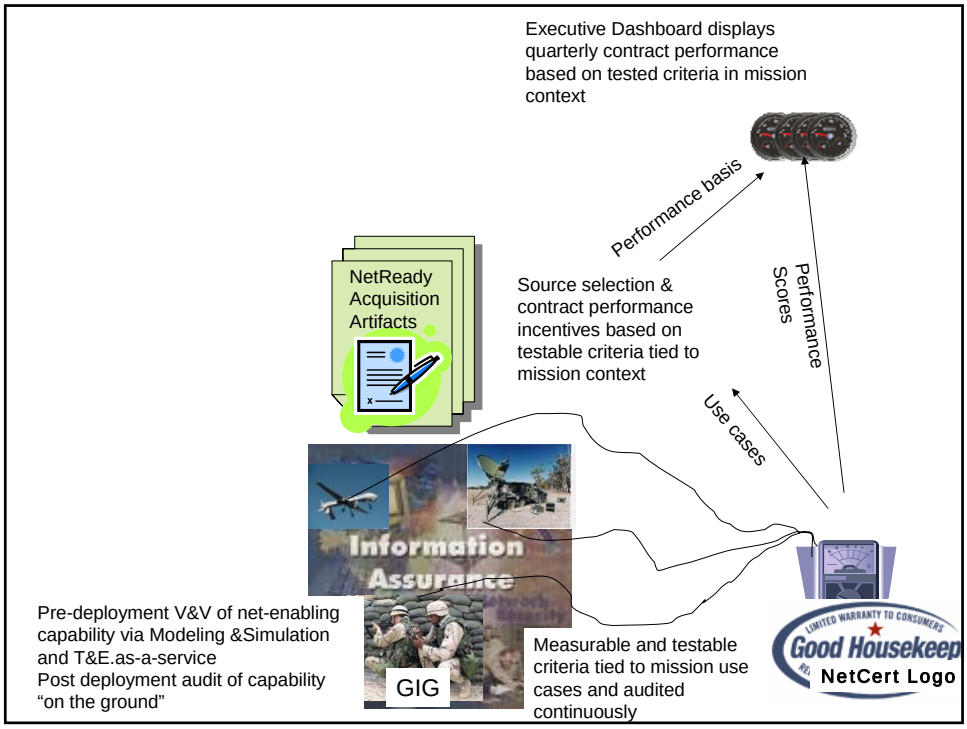
17

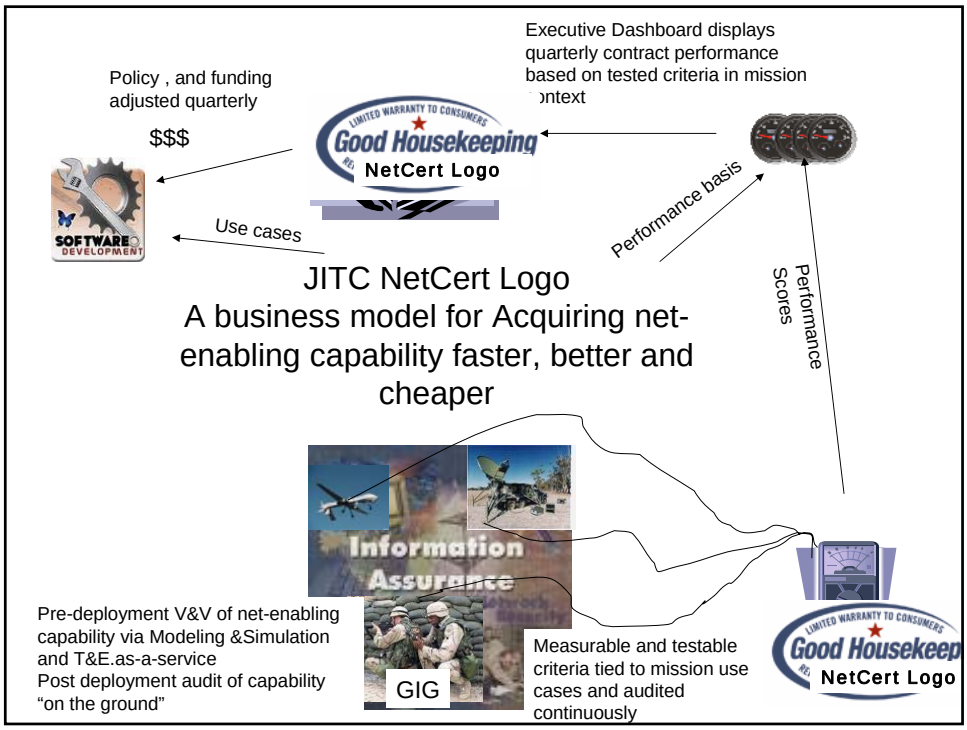
JITC NetCert Logo
A business model for Acquiring net-enabling capability faster, better and cheaper

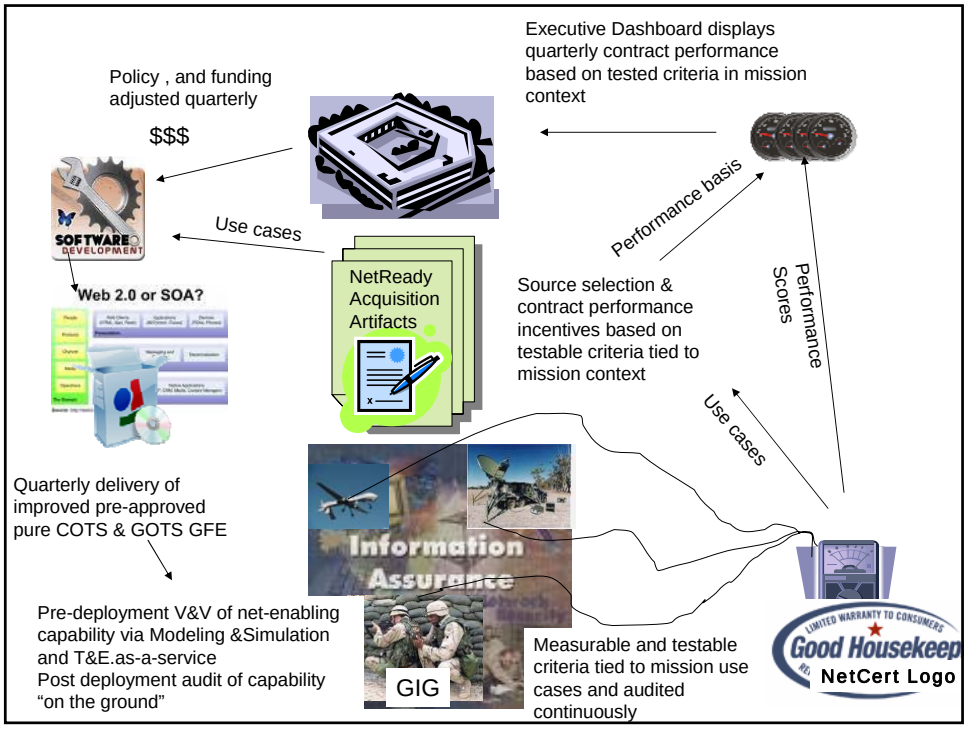
18


Information Assurance
GIG
Pre-deployment V&V of net-enabling capability via Modeling &Simulation and T&E.as-a-service
Post deployment audit of capability "on the ground"
Measurable and testable criteria tied to mission use cases and audited continuously
LIMITED WARRANTY TO CONSUMERS
Good Housekeep
NetCert Logo


NetReady Acquisition Artifacts
Source selection & contract performance incentives based on testable criteria tied to mission context
Use cases
Information Assurance
GIG
Pre-deployment V&V of net-enabling capability via Modeling &Simulation and T&E.as-a-service
Post deployment audit of capability "on the ground"
Measurable and testable criteria tied to mission use cases and audited continuously
LIMITED WARRANTY TO CONSUMERS
Good Housekeep
NetCert Logo


Executive Dashboard displays quarterly contract performance based on tested criteria in mission context
Performance basis
Performance Scores
NetReady Acquisition Artifacts
Source selection & contract performance incentives based on testable criteria tied to mission context
Use cases
Information Assurance
GIG
Pre-deployment V&V of net-enabling capability via Modeling &Simulation and T&E.as-a-service
Post deployment audit of capability "on the ground"
Measurable and testable criteria tied to mission use cases and audited continuously
Good Housekeeping
NetCert Logo


Executive Dashboard displays quarterly contract performance based on tested criteria in mission context
Policy , and funding adjusted quarterly
$$$
Use cases
Performance basis
Performance Scores
Good Housekeeping
NetCert Logo
SOFTWARE DEVELOPMENT
JITC NetCert Logo
A business model for Acquiring net-enabling capability faster, better and cheaper
Information Assurance
GIG
Pre-deployment V&V of net-enabling capability via Modeling &Simulation and T&E.as-a-service
Post deployment audit of capability "on the ground"
Measurable and testable criteria tied to mission use cases and audited continuously



NetCert Logo Strategy

- **Born Netcentric**
  - Partner with JITC re: NR-KPP
  - Partner with NSA re: C&A
  - Partner with W2COG re: eBiz & collaborative best practice
  - Focus on "open" architecture for security (e.g. MILS*) and data strategy (e.g.CIEF**)
- **Learn by doing**
  - Use existing GIGlite infrastructure as ramp up "training wheels"
  - Build infrastructure iteratively per feedback from "training wheels"
  - Certify testing-as-a-service capability as first use-case
    - Certify ~1 X net-ready test case per month thereafter
- **Feedback & continuous improvement**
  - Regular customer visits
  - Teach new functionality
  - Collect new use cases
  - Audit performance

*Multiple Independent Layers of Security
** Cross-domain Information Exchange Framework

24

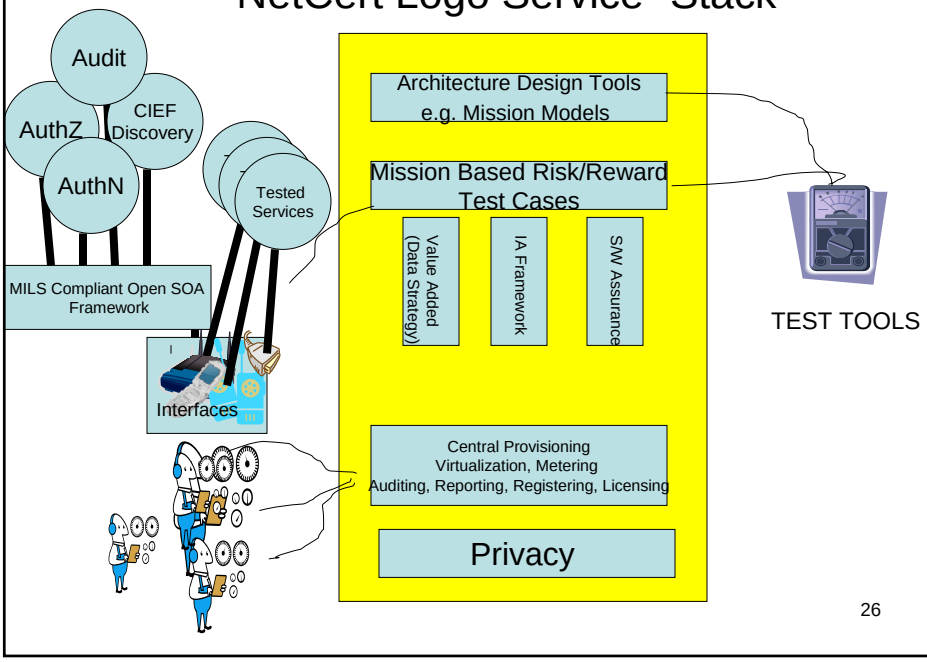
NetCert Logo Lab Requirements

- Reference Implementation of Net-Ready Service Oriented Architecture:
  - Routable network backbone
  - Open standard, self described, discoverable interfaces.
  - Assured Security (MILS* compliant)
  - Assured Data Strategy (CIEF** compliant)
- Mission-model based measures of effectiveness (e.g. NECC Mission Level Model BPMN graphic to BPEL executable)
- Software Assurance & Performance test tools and trained operators (e.g. OMG Software Assurance Eco-system methodology)
- SOA functional *and performance* test tools and trained operators.
- "Architecturally Net-ready" Acquisition artifact boiler plate (e.g. Net-Ready COTS Acquisition Strategy, C&A plan, NR-KPP, T-ISP, TEMP, etc.)
- Government purpose rights to software enforced. (Standard license model for GFE s/w re-use across programs)

*Multiple Independent Levels of Security
**Cross-domain Information Exchange Framework

25

NetCert Logo Service "Stack"



26

Early Adopter "NetCert Logo" Candidate's 1st year Objectives

- Certified by JITC as qualified to perform Net-Ready s/w assessment per GIG policy stack
- Interim Authority to Operate (ATO) SOA Test Lab per DIACAP and appropriate DAA
- Multiple Independent Levels of Security (MILS) Reference Architecture Implementation (IA control)
- Cross-domain Information Exchange Framework (CIEF) Reference Architecture Implementation (GIG Data Strategy control)
- Open Standard SOA Infrastructure
  - Cadre of professional s/w developers trained to maintain Open Standard SOA Infrastructure
- Suite of SOA design and test tools
  - Cadre of professional testers trained to maintain and operate SOA design and test tools
- Three net-ready test cases leads to one certified net-ready service = testing-as-a-service capability
- Prepared to perform one net-ready test case per month going forward

27

NetCert Logo Candidate's POA&M

- Establish use cases & test cases: 60 Days
- 1st lab demonstration : 120 Days
- 1st draft lab design & docs*: 130 Days
- Training complete: 130 Days
- 2nd lab demo: 180 Days
- 2nd draft lab design & docs: 190 Days
- 3rd lab demo: 270 Days
- Final documents revision: 290 Days
- Lab Certification & IATO: 360 Days

*e.g. Net Ready COTS Acquisition Strategy, T-ISP, NR-KPP, TEMP, Diagnostic DoDAF artifacts, Government Purpose Rights (GPR) license model

28

ROM* NetCert Logo Ramp UP Costs

- Expert consultants (IA, C&A, Acquisition, Data Strategy): ~1.5 FTE @$300K = ~$450K
- Open Standard SOA infrastructure & SOA test tools: $250K - $1.2M (varies based on desired scale and internal FTE available.)
- 3 X Tests @ $125K = $375K
- Documentation ~ $440K

29

*Highly variable based on internal resources available

Deliverable

- Create and implement a self-sustaining Mission-Thread-Market of certified “architecturally net-ready” off-the-shelf offerings
  - Provide for continuous and/or opportunistic competition across a broad spectrum of information processing capabilities
  - Level the playing field among vendors by reducing cost of entry
  - Reduce certification timeline by certifying concurrent with developing
  - Reduce delivery time by making more pre-approved COTS available faster

30

Investment and RoI

- Invest AoA and/or development funds from program to stand-up MTM and “NetCert logo” process.
- Achieve self sustainment by requiring vendors to obtain, at their cost, NetCert logo to “qualify” their COTS for GIG deployment

31

Acquisition Strategy

- Incremental improvements
  - COTS based on market
    - Source selection and contract performance based on life cycle re-capitalization
    - Sustained competition provides improvements
      - » Also reduces cost and time to deploy
  - Mission Threads provide specs
  - Lab environment provides early testing
    - For certification and accreditation
    - For interoperability
  - Product support team provides continuous customer feedback

32

MTM via NetCert Logo Schedule

- Establish Use cases: 70 DAC*
- Establish lab under JITC/NPS: 80 DAC
- COTS jamboree: 100 DAC
- First vendor lab demo: 120 DAC
- Revise acquisition documents: 120 DAC
- Second vendor lab demo 180 DAC
- Second documents revision 195 DAC
- Third vendor lab demo (TRR) 270 DAC
- Final documents revision 290 DAC
- COTS Evaluation (SS) 330 DAC
- Installation ready products 360 DAC

* DAC = Days After Contract

33