CWID08 Demonstrates Rapid Evolutionary Acquisition Model of Coalition C2

AFCEA-GMU C4I CENTER SYMPOSIUM
Critical Issues in C4I
19-20 May 2009
National Conference Center
Lansdowne, Virginia

Coalition Warrior Interoperability Demonstration (CWID) 08 Interoperability Trial #5.64 “Trusted Enterprise Service Bus” (T-ESB)

A service-oriented approach to “flattening” coalition networks… and delivering Valued Information at the Right Time (VIRT) via evolutionary, value-based, service-oriented acquisition.
Coalition stovepipe “air gapped” network enclaves:

Redundant physical infrastructure is expensive and clumsy.
Agile, responsive information exchange is impossible

A framework to deploy High Assurance Tactical SOA (HATS) faster, cheaper, and better via a “Mission Thread Market” (MTM) of pre-approved net-ready Off-the-Shelf (OTS) components.
High Assurance Government Furnished Services for:
Authentication (AuthN)
Authorization (AuthZ)
COTS “Discovery” Services to deliver Valued Information at the Right Time (VIRT)

- Same physical network with logical enclaving decreases maintenance costs & enables continuous re-capitalization
- Smart push of critical information + dynamic security policy enables agile information exchange
TESB
Dynamic Security Policy + High Assurance AuthN & AuthZ services = Access to C4ISR Picture via Browser

BLUE FORCE TRACKS

AIS Tracks

C2 + GIS service

PL4 AuthN/ AuthZ services

RELEASABLE

NOFORN

Dynamic Security Policy + High Assurance AuthN & AuthZ services = Access to C4ISR Picture via Browser

PL4 Service Based Authorization and Authentication

Workstation

Server

Policy Decision Point (PDP)

Identity Provider (IdP)

PL4 SABI

E.g. Join Track Manager

PL4 TSABI underway

E.g. Google Earth
### NORMAL Policy

<table>
<thead>
<tr>
<th></th>
<th>CA</th>
<th>NZ</th>
<th>OC</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>METOC (NOFORN)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>METOC (REL)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AIS (NOFORN)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIS (REL)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SENSOR (NOFORN)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

### EMERGENCY Policy

<table>
<thead>
<tr>
<th></th>
<th>CA</th>
<th>NZ</th>
<th>OC</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>METOC (NOFORN)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>METOC (REL)</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AIS (NOFORN)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIS (REL)</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>SENSOR (NOFORN)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

### SELF DEFENSE Policy

<table>
<thead>
<tr>
<th></th>
<th>CA</th>
<th>NZ</th>
<th>OC</th>
<th>US</th>
</tr>
</thead>
<tbody>
<tr>
<td>METOC (NOFORN)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>METOC (REL)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>AIS (NOFORN)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIS (REL)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SENSOR (NOFORN)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CA = CANADA  
NZ = NEW ZEALAND  
US = UNITED STATES  
OC = OTHER COALITION

Detail of national security policy is set by nations. Policy is presented as “black box” based on pre-agreed states of urgency. These matrices show US national policy “under the hood” per CWID IT 5.64 scenario.

Sysadmin set policy by clicking on appropriate button:
- NORMAL Policy
- EMERGENCY Policy
- SELF DEFENSE Policy
Open std web service bus (TSB) aboard sensor platform, e.g. UAV, provides sensor service

C4ISR Services
Occasionally connected UAV’s post SIGINT web-services at the tactical edge of the GIG

AIS Tracks
Blue Force Tracks

C2 + GIS service

VIRT* Services
Intelligent agents monitor pre-defined critical conditions of interest. When threshold criteria exceeded. Exception to security policy is enabled.

UNK Track inside 3 mile limit = Alert Criteria. Change release policy

* VIRT = Valued Information at the Right Time. A VIRT Service is an intelligent agent that provides a “smart push” or an alert when emergent conditions satisfy a client’s pre-defined critical conditions of interest profile.
VIRT* Services

VIRT service issues alert to opportune coalition interdiction platform.

C2 + GIS service

UNK Track inside 3 mile limit = Alert Criteria. Change release policy

VIRT* Service

Issue alert to Interdiction asset

Coalition platform requests targeting service via AuthN/AuthZ

National sensor service allows coalition platform to view UNK Track targeting data

ISR sensor "sees" contact of interest

TESB
Emergent operational situation drives need to release NOFORN data to coalition asset
Netcentric “Business” Driver

• At home, a US 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.

• How can we apply our vastly superior resources to overcome this asymmetrical disadvantage w/rt information processing?
Evolutionary Acquisition via NetCert Logo and Mission Thread Market

- Problem:
  - Operators, dispersed worldwide, need networked IT resources.
  - The IT network must deliver just the right information in the right mission context.

- Solution:
  - Create an enterprise IT experimentation infrastructure for rapid, low cost, mission-tailored demonstration, validation, verification & certification per "NetCert Logo".
  - Transition validated/certified capability via COTS "Mission Thread Market" (MTM).

GIG acquisition objective: Reuse and continually improve shared infrastructure, i.e. routable networks + SOA, to enable netcentric operations

- Invest to develop valuable content
- Minimize time & cost by reusing and continuously improving valuable community infrastructure
- Invest to exploit valuable content
But....

- After many years and $B’s spent the promise of SOA remains largely unfilled across DoD....

Observations....

- COTS s/w 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.
- PMs use COTS as gap fillers that generally lack sustainment tails.
- IRT the above, DoD top-down policy mandates SOA and “best” e-Biz practice (e.g., NESI, DoDAF 2.0, Open Technology Development, NR-KPP, etc.)

- YET.... e-Biz un-mandated “best-policy” is to leverage competition in the marketplace... No one is in charge....
DoD Inst 5000.02

- Single sponsor
- Massive monolithic requirements
- Expensive, repetitive, paper documentation
- Long serial process

Program IOC ~ 10 years

JCIDS Says to define "Capability Based Rqmts"...
GIG Policy Says to field "Netcentric Capability..."
But….follow the money

So....

• How can DoD leverage the SOA e-Biz value proposition within the constraints of the Federal Acquisition Regulations (FAR)?
Bottom Line

- Establish GIG business model = e-Portal for consumable off-the-shelf (OTS) = COTS, GOTS & Open Source Software (OSS) certified net-ready components

- Define generic and objective net-ready assessment categories and methods (not universal specifications!) per enterprise business objectives

- Use a NR-KPP "logo" to create a federation of qualified, motivated, independent government, industry, and academic net-ready providers

- Base GIG Acquisition on components that can reduce risk re: cost, performance, and schedule and deliver capability faster.
  - Require logo as "responsive" to GIG procurements
  - Bake evolutionary COTS process into FAR boilerplate
  - Hardwire cross-program collaborative work flow

NR-KPP Architecture and Engineering Principles

- Objective is Value of Service (VoS), not just Quality of Service (QoS)
  - QoS = reliability
  - VoS = reliable, trusted, significant, content + continuous improvement

- "Information Assurance" (IA) is not just "Security"
  - "Assurance" means increased predictability
  - "Security" is one value attribute, others are "supportability" and "availability."

- Assurance is necessary to make informed risk/reward tradeoffs

- Modularity, measurability, and accountability are key.
If one of my component fails, Ao decreases. How do I get the “9”s I need for my box?

- More spares?
- More redundancy?
- More technicians?
- Better technology?

Any number of factors beyond my control affect network performance. How do I get the “9”s I need at my node of interest?

- Topology?
- SOA vs. Thick Client?
- C&A, IOP, DT, OT?
- COTS vs. GOTS vs. OSS?
- Build vs. Buy vs. Lease?
- Enterprise vs. Seat License?
- FFP vs. LoE, Long vs. Short Term Contract?
A_o of a Network = QoS, i.e. Operational Availability of SLA-compliant data stream at node of interest

A_u = Availability of useful data. Reliable data flow is necessary, but not sufficient. Objective is “valued” data flow:

\[ A_u = f (\text{Trust, Significance, Cost, etc..}) \times IPE \]

IPE = Valued Bits/Total Bits Processed = \[ w1 \times (RB) + w2 \times (AB) + w3 \times (IB) \]

\[ RB + AB + IB \]

IPE = Information Processing Efficiency

w1, w2, w3 = Weighting Function

RB = Useful Relevant Bits

AB = Actionable Bits

IB = Irrelevant Bits

A_{nr} = Availability of Net-Ready Capability – a build time/buy time process level Measure of Effectiveness (MOE).

\[ A_{nr} = \frac{D_{ti}}{C_{DT} = D_{Tc} + T_{Tc} + C_{Tc}} \]

e.g. \( C_{DT} \leq \) Moore’s Law Cycle = 18 months

\[ A_{nr} \geq 0.66 \]

A_{nr} = Net-Ready Availability: a unit-less index that maps the obsolescence rate of the technology to the acquisition timeline, including development, test and certification.

C_{DT} = Capability Deployment Time

D_{ti} = Initial estimated Development Time: calendar time required, in consideration of testing and certification timelines, to field an increment of IT capability prior to its obsolescence.

D_{Tc} = Current, or revised estimate of Development Time at the time of evaluation

T_{Tc} = Current or revised estimate of Test Time: calendar time required post development to complete any additional required testing.

C_{Tc} = Current or revised estimate of Certification Time: calendar time required post testing to achieve any necessary certifications.
CDT = Capability Deployment Time

DT = Development Time.

ITi = Invention Time: calendar time (calendar days, not necessarily billable man hours) it takes to develop new intellectual property.

RT = Reinvention Time: calendar time it takes to re-develop capability that someone else has already developed as a government, commercial, or open source off-the-shelf component.

BT = Bundling Time: calendar time it takes to compose existing capability components into a coherent, stable, and robust package.

OT = Overhead Time: billable hours spent doing things other than directly developing capability.

TT = (Post-Development) Test Time.

CT = (Post-Test) Certification Time.

w = weighting factor

\[ A_{iv} = \frac{DTi}{(CDT = DTi + ITi + RT + BT + OT) + TT + CTc} \]

\[ w = w1 \cdot w2 \cdot \ldots \cdot wn \]

\[ A_{mr} = \frac{DTi}{(CDT = DTi + ITi + RT + BT + OT) + TT + CTc} \]

\[ A_{iv} = (Ao)(Au) \]

It follows that the Value of Service (VoS) of a system is equal to the sum of the run-time value of each of the composite capabilities:

\[ VoS_{System} = \sum_{n=1}^{n=k} (Ao)(Au) \]

where \( k = \) # of capabilities

VoA is the total value of the acquisition. An objective means to manage risk and optimize opportunity.

\[ VoA_{System} = A_{w} \sum_{n=1}^{n=k} (Ao)(Au) \]

Scorecard 2

Ao = Information Value Availability
Ao = Operational Availability
Au = Utility Availability
VoS = Value of Service
High Assurance Tactical SOA Acquisition Plan

<table>
<thead>
<tr>
<th>Service</th>
<th>3 Mos</th>
<th>6 Mos</th>
<th>9 Mos</th>
<th>12 Mos</th>
<th>15 Mos</th>
<th>18 Mos</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAV Sensor Service</td>
<td>Demo</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IOC</td>
</tr>
<tr>
<td>AuthZ Service</td>
<td>Demo</td>
<td>Demo</td>
<td>Demo</td>
<td>IOC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOTS AuthN Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOTS METOC Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COTS AIS Track Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COTS VIRT Alert Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSS OTS Geospatial Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certification and Accreditation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NR KPP Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPTEST</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper work</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**HATS Acquisition Value Analysis**

\[ w_{m1} = 1.2 = 20\% \text{ improvement in probability of detection.} \]

\[ w_{m2} = 2.0 = 100\% \text{ improvement in detect to engage time.} \]

\[ \text{IPE} = 1.18 - 4.0 \text{ per 2X vs 10X weighting factor for actionable information} \]

\[ A_u = (1.2)(2.0)(1.18)(U_{BL} = 1\text{uu}) = 2.83 \text{ uu} \]

\[ A_v = 0.9999 (\text{Internet}) \]

\[ A_r = 12\text{Mos} / 18 \text{Mos} = 0.66 \]

\[ \text{VoA} = (0.66)(0.9999)(2.83)\text{uu} \times 4 \text{ Capabilities} = 7.5\text{uu} \]

**VoA**

\[ \text{VoA}_{\text{Baseline}} = 1.7\text{uu} \]

**HATS value added**

\[ 7.5 / 1.7 = 4.41X \]

* Determined by assigning \( A_u = 1 \) to current network capabilities and calculating their IPE in the same operational demonstration case.
Can we build it …?

YES WE CAN!

Backup Detail
Acquisition Strategy

- Base IT procurement on acquisition components that can reduce risk re: cost, performance, and schedule
  - Exploit new GIG Acquisition policies
  - Extend and expand pure COTS competition
  - Issue simple use cases in lieu of traditional RFI/RFP
  - Require mission context prototypes vice paper studies
  - Shorten delivery cycles and contract review periods
  - Exercise government purpose rights to software licenses
- Incentivize PMs and COTS vendors to participate
  - Furnish pre-approved GOTS components
  - Streamline Certification and Accreditation (C&A)
  - Furnish V&V to put COTS on approved products list
- Create evolutionary systems engineering tools and FAR-compliant boiler plate to achieve all the above

\[ A_u(X) = (w_m)(w_s)(w_c)(w_p)(IPE)(U_{BL}) \]

\( A_u(X) \) = Utility Availably function of data stream X

\( w_m \) = Weighting factor associated with consideration x

\( w_m \) = Mission performance factor = fraction of baseline performance improvement enabled by new capability. E.g., if mission performance metric increases by 10%, \( w_m = 1.1 \).

\( w_s \) = Safety factor = fraction of baseline performance enabled by new capability. E.g., if safety metrics improve by 10%, \( w_s = 1.1 \).

\( w_c \) = Cost avoidance factor = fraction of baseline performance enabled by new capability. E.g., if cost avoidance improves by 10%, \( w_c = 1.1 \).

\( w_p \) = Preferred data source factor. If preferred source used, \( w_p = 1.0 \). If non-preferred source used \( w_p < 1 \) per sliding scale.

\( \text{IPE} \) = Information Processing Efficiency = (Valued Bits)/(Total Bits Processed).

\( U_{BL} \) = Utility Baseline Value in utility units
Software Currency = "1" if current or previous standard or build is used; Software Currency = .1 if standard or builds are older than one previous generation.

Lines of Code = f(excess or superseded code), i.e. the number of lines of code tends to increase as new software architectures are added, including unnecessary features, and as legacy architectures remain in the "stack".

$$W = \frac{Software\ Currency}{Lines\ of\ Code(LoC)/Baseline\ LoC)}$$

$$w = \text{weighting factor}$$
Notional Example
C2 Program X Operational Availability (A_o) and Net-Ready Availability (A_{nr})

Demonstration of how relationship between A_{nr} and A_o improves Reliability Maintenance and Availability (RMA) while reducing cost

Chris Gunderson
David H. Minton
9 March 2009

Assumptions

A_o = \frac{MTBF}{MTBF + MTTR + MLDT} = 0.99999

and

A_{nr} = \frac{DT_i}{DT_r + TT + CT} = 0.66

where DT_r <= DT_i and DT+TT+CC <= 18 mos (to simplify notional example)
At PDR, MTTR is xxxx hrs given:

\[ A_o = 0.99999, A_{nr} = 0.66, \text{ Cost} = \$\$\$\$\$ \]

At IOC, (IOC = PDR + 18months) MTTR is xxxx hrs, given:

Where, MTTR_{1I} < MTTR_{1P}, MTTR_{2I} < MTTR_{2P}, etc., and
\[ A_o = 0.99999, A_{nr} = 0.66, \text{ Cost} = \$\$$, or…
\[ A_o = 0.9XXXX, A_{nr} = 0.66, \text{ Cost} = \$ \]
At Lifecycle Support Contract
Performance Review (IOC + 18months)
MTTR is xxxx hrs, given:

Where, MTTR\textsubscript{1LC} < MTTR\textsubscript{1I}, MTTR\textsubscript{2LC} < MTTR\textsubscript{2I}, etc.,
over each improvement cycle and, A\textsubscript{o} = 0.99999, A\textsubscript{nr} = 0.66, Cost = $$$$ ....
or A\textsubscript{o} = 0.99XXX, A\textsubscript{nr} = 0.66, Cost = $$. ....

Draft Executive Brief for C2
Program X Management
Reliability, Availability, and Maintenance Issue

• Program X aims to deliver C2 capability via new “open system” paradigm: leverage SOA and COTS to deliver continuous evolutionary improvement.

• Program X inherited KPP, Ao=0.99999, designed for legacy “closed system” paradigm.

• Issue is that Program X aims to provide software-enabled “Information Availability”, but traditional Ao is a H/W-centric metric.

SOA Program Scoring Conference (SC)

• Typical SC recognizes the issue:
  – Uses Business Process Modeling (BPM) to define Fully Mission Capable (FMC) and “Available, Degraded” (Deg)
  – Considers both h/w & s/w

• However, SC analysis finds most failures as h/w issues because:
  – H/w failures are material and s/w failures are not.
  – H/w fails after thousands of hours, s/w fails in tens or hundreds of thousands of hours.

• Suggests increasing overall system availability by providing h/w spares…. an expensive approach!
Consider

• Historically, s/w improvements continuously reduce the amount of h/w required to enable capability.
• E.g., the TCP/IP capability in the early ARPANET nodes, which required two to four PDP-10/11 then, is now handled by a few thousand lines of code in a Windows or MAC machine.

Objective

• Do not dilute the strong h/w availability we’ve already captured
• Capture a similar process for software.
  – Employ objective measures like we already have for h/w
  – Use objective measures as thresholds and objectives for deliverables.
Proposed Methodology

- Base RAM metrics on “supportability” per CJCSI 6212 NR-KPP.
- Use Moore’s Law 18 month technology refresh time line as the delivery cycle for transferring increments of FoS functionality (and other) to NECC Enterprise Capability (EC).
- Establish Business Process Model (BPM) as the requirement set.
- Set the threshold and objective RAM targets inside the 18 month delivery cycle.
- Adjust RAM targets for each successively delivered COTS s/w bundle to anticipate inevitable reduction in h/w redundancy requirements.
Engineering Tasks

• Isolate the BPM against the EC
• Establish the COTS s/w trajectory for this technical capability (COTS supportability).
• Establish threshold and objective RAM targets for the bundled s/w.
• Make RAM targets part of the IOC deliverables.

GIGlite Federation… open technology development across the stovepipes

- Single point of contact for Gov’t, industry, & academic members
- Title 10 compliant, Non-FAR < ~90 day S&T & engineering spirals
- Open source/Open Standards IPR model
- Rolodex of experts

- Distributed major net-ready test range
- Single POC for Gov’t labs and sponsors
- Distributed, Adaptive, Collaborative, net-ready V&V and certification
- Convenient process for reuse of off-the-shelf components

GIGlite Federation
Best Net-centric Practice
$ & IP
Net-Ready Certification
NetCert.gov

Umbrella Cooperative Legal Agreement

e-Portal for Gov’t certified, off-the-shelf, bundles and components of net-ready capability
### Evaluation Criteria: Net-Ready

#### Measurable & Testable Parameters

<table>
<thead>
<tr>
<th>Net-Ready Parameters and Business Objectives</th>
<th>IA =&gt; Share &amp; Protect</th>
<th>SOA =&gt; Reuse &amp; Mash Up</th>
<th>Data Strategy =&gt; Trusted Discovery in Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net-Ready Parameters and Business Objectives</td>
<td>✓ Assurance and Performance</td>
<td>✓ Reuseable/Composable*</td>
<td>✓ Value/Bit Exchanged</td>
</tr>
<tr>
<td></td>
<td>✓ Software Assurance OK?</td>
<td>✓ Discoverable?</td>
<td>✓ COI approved mission thread?</td>
</tr>
<tr>
<td></td>
<td>✓ Network Assurance OK?</td>
<td>✓ Self describing?</td>
<td>✓ Register critical conditions of interest</td>
</tr>
<tr>
<td></td>
<td>✓ Register dynamic discretionary access policy?</td>
<td>✓ Open standard interfaces?</td>
<td>✓ Meta data registered in context?</td>
</tr>
<tr>
<td></td>
<td>✓ Latencies OK?</td>
<td>✓ Cross program investment?</td>
<td>✓ Mission based MOE OK (i.e., compress time line, and/or improve mission outcome)? **</td>
</tr>
</tbody>
</table>

*Bind to Trustworthy SOA Framework, e.g. T-ESB

** Confirm with operational audit

---

### GIGlite Strategy

- **Born Netcentric**
  - Partner with JTC re: NR-KPP
  - Partner with NSA re: C&A
  - Partner with DOT&E re: DT, OT
  - Partner with W2COG re: eBiz & collaborative best practice
  - Objectively define “open” reference architecture for security and semantic interoperability
- **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
“GIGlite” Virtual Lab

- Reference implementation of net-ready SOA
  - Routable network backbone
  - Open standard, self described, discoverable interfaces.
  - High assurance GOTS security components (e.g. MILS)
  - Value-based information sharing /communication /management framework (e.g. NPS VIRT**, SPAWAR CIEF***)
- Mission-model based measures of effectiveness
  - (e.g. MITRE Mission Level Model)
- Software assurance & performance test tools and trained operators
  - (e.g. NIAP-lite, MDA “CDTS simplifier” and OMG “SwA Ecosystem”)
- Network (SOA) functional and performance test tools and trained operators
  - (e.g. OPNET, Teledyne)
- Net-ready Acquisition artifact boiler plate
  - (e.g. MTM Acquisition Strategy, Spec, SOW, WBS, C&A plan, NR-KPP, T-IISP, TEMP, etc.)
- Open IPR model to exercise government purpose rights

*Multiple Independent Levels of Security
**Valued Information at the Right Time
***Cross-domain Information Exchange Framework

GIGlite 1st Year Objectives

- Reference implementation of high-assurance SOA infrastructure
  - Discoverable, open standard, self describing interfaces
  - High assurance GFE security services
  - Value-based information/communication/management framework
- Interim Authority to Operate (ATO) SOA test lab
- Certified by JITC as qualified to perform net-ready s/w assessment
  - Cadre of qualified designers, testers, and developers
  - Suite of SOA design and test tools
  - Demonstrated three net-ready test cases leading to one certified net-ready service
  - Prepared to perform one net-ready test case per month going forward
MTM Inside DoD Inst 5000.2

Vendor Jamborees; published use cases; government furnished GOTS s/w reference implementations; government refereed network T&E lab; M&S; embedded net-ready assessment; ~Analysis of Alternatives (AoA) via 90 day s/w bundling demos in lieu of JCIDS paper artifacts

These are pre-approved “qualified net-ready” COTS/GOTS s/w bundles

Existing GIG policy sufficiently defines requirements for SOA information processing. Policy is enforced by objective NR-KPP criteria, using M&S and other automated test tools

EDM via 90 day Agile COTS/GOTS bundling demos, or “sprints”. These can be used as down selects or simply net-ready qualifying opportunities

GFE COTS/GOTS software build every ~360 days
Program IOC ~ 10 years
## W2COG DoD Acquisition Artifacts Consistent with MTM

<table>
<thead>
<tr>
<th>Process</th>
<th>Directive</th>
<th>Capability Broker Deliverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>JCIDS</td>
<td>CJCSI 3170.01, DODI 4630.8</td>
<td>Tailored ISP</td>
</tr>
<tr>
<td>FAR/DFAR</td>
<td>DODI 5000 series</td>
<td>DODINST 5000.2 compliant artifacts, e.g. BAA, RFI, RFP, Source Selection Plan, Risk Mitigation Plan, SOA COTS Acquisition Strategy, Contract SLAs</td>
</tr>
<tr>
<td>IA Compliance, e.g. DIACAP</td>
<td>DODI 8500 series</td>
<td>Enterprise &quot;Type Accreditation&quot; (Trusted SOA DIACAP certification plan)</td>
</tr>
<tr>
<td>NR-KPP= (NCOW = IA+ SOA+ Data Strategy) + KIPS + DoDAF</td>
<td>CJCSINST 6212.01, NCO/W Ref Model, KIPS, NSA GIG IA policy, DoDAF v1.5</td>
<td>Measurable and Testable Net-Ready Parameters, diagnostic DoDAF views</td>
</tr>
<tr>
<td>T&amp;E</td>
<td>DODI 5010.4, 4630.8</td>
<td>Tailored TEMP (latest COTS GFE is tested at DT and goes to QT)</td>
</tr>
</tbody>
</table>