Service Oriented Acquisition: Harmonizing Horizontal Requirements with a Traditionally Vertical Process

Chris Gunderson
NPS, JITC & W2COG
Chris.Gunderson@w2cog.org

Abstract

The Department of Defense has adopted the concept of Netcentric Operations and Warfare, i.e., effective, distributed, collaboration over a network to gain asymmetric advantage, especially with respect to information superiority. To enable NCO/W, the DoD has issued transformational policy mandating change from a vertical (stovepiped), serial, system-centric requirement model to a horizontal, capability-based, adaptive, requirement model. This policy specifically calls for using the service oriented architecture (SOA) paradigm as a change agent, and a means to accelerate delivery of information processing capability. However, the intent of this SOA-enabled netcentric requirements policy is at odds with the implementation detail mandated by Acquisition policy. That is, Acquisition policy does not offer tools to enable, let alone encourage, cross program development of enterprise capability or to de-couple software development from the rigid, serial, timelines associated with developing sensors, weapons, and platforms. This paper suggests a way to subtly nudge two aspects of the existing policy regime to provide those tools. In particular, the Net-Ready Key Performance Parameter (NR-KPP) should be based on a minimal matrix of measurable and testable criteria that can be observed on the ground, written into enforceable contract language, and rolled up into executive dashboards. The Tailored Information Support Plan (T-ISP) concept should be expanded to include the notion of a network service stack (NSS) to address enterprise-level information processing capability. The intent of a NSS T-ISP would be to provide a plan, enforceable through contract language, that will maintain NR-KPP service level objectives throughout a capability lifecycle.

1. A service oriented paradigm for IT interoperability testing: Net-Ready Assessment.

The Department of Defense has issued policy explaining its desire to become a “netcentric” [1] enterprise enabled by a Global Information Grid (GIG). To enforce this policy in the DoD Acquisition process, DoD has created the “Net-Ready Key Performance Parameter (NR-KPP). Traditionally, KPP’s are rigid, mandatory, engineering specifications associated with major DoD programs. The NR-KPP is intended to ensure that artifacts fielded on the GIG contribute and conform to the objectives of a netcentric enterprise. “Netcentric” implies an adaptive and collaborative approach to information processing, a concept at odds with the traditional rigidity of KPPs. Hence, net-ready assessment, i.e. validation and verification (V&V), test and evaluation (T&E), and/or certification and accreditation (C&A) of “net-readiness”, should be an adaptive and collaborative process. Adaptive and collaborative assessment is a profoundly new concept for DoD. Net-ready assessment should therefore not be hidebound to the bureaucracy of the status quo. Rather, net-ready assessment should be a useful engineering service embedded throughout the software development and deployment process, based on measurable and testable parameters that will accomplish the following:

Reduce Acquisition policy and requirements documents into measurable and testable attributes that can be coded in machine readable formats for testing and used as the basis for contract enforcement language.

Decrease the time and money developers spend on testing by consolidating various aspects of testing (e.g. C&A, Interoperability), sharing best practices across programs, and standardizing assessment methods across certification authorities.

Focus assessment on software architecture rather than software build, so that “most current COTS/GOTS component” can be a test criteria.

Bundle candidate information processing capabilities into reference implementations of
net-ready architecture that can be tested independently for compliance, and then used as a universally validated component instead of testing thousands of services for compliance with hundreds of often vague standards.

Assess both adequacy of service oriented infrastructure (e.g. enterprise security and semantic interoperability) and value added to business objectives (i.e. targeted improvements in mission outcomes.)

Weigh risk and reward to scale the rigor of assessment as appropriate to address the spectrum from small and/or generic COTS or GOTS software modules (e.g. Google Earth) to large and/or specialized “systems” (e.g. Future Combat System.)

Assist developers of large complex systems to deploy their capability continuously and incrementally as a “system of services” composed largely of COTS and GOTS modules.

Rapidly assess information processing capability prior to its operational deployment by heavily leveraging modeling and simulation. Follow up with operational V&V that holds developers responsible for delivering targeted service levels of mission performance improvements.

Create an on-line digital feedback loop to capture lessons learned and assist in the tasks described above.

Reduce the barrier to entry for IT vendors and developers that don’t traditionally support the DoD by hiding the complexity of DoD policy and process behind recognizable, comfortable, e-market interfaces.

1.1 Net-ready assessment’s three broad categories.

1.1.1 Do no harm (assurance and performance).

The GIG will be a network of interactive software and hardware services that propagate and evolve quickly and without central control, by design. This federated design requires discipline across the federation to ensure that a candidate new service does not negatively impact the existing ecosystem. Net-ready assessment should address software assurance (SwA) with respect to how the assessed software architecture affects overall network vulnerability, latency, lifecycle cost, and reliability. Current methods for testing SwA are immature, and although the net-ready assessment process will deliberately evaluate and incrementally improve those methods, they will never be perfect. Therefore, the task is to manage risk rather than eliminate it. Some risk and/or service degradation is acceptable if tradeoffs warrant. For example it may be acceptable to gain higher assurance at the cost of greater latency, more functionality at the cost of lower reliability, or greater speed to better capability at the risk of introducing some vulnerability. Operational customers will be the final arbiter of the acceptability of these tradeoffs during operational V&V.

1.1.2 Bind to Trustworthy Service Oriented Architecture (SOA) infrastructure (reusable and composable).

“Bind-ability,” i.e. the ability to quickly compose new capability from distributed components, is a key aspect of netcentricity. SOA is a technological approach that can be used to compose capability (i.e. “mash up”) across a network. (The idea of “composability” applies to both on-line operational use of the capability, and engineering re-use of the technology.) “Enterprise Service Bus” (ESB) is a generic term used in industry to represent the interfaces, protocols, and objects that form the framework for a particular SOA. We can define SOA IA infrastructure as enterprise IA services plus the ESB (or other framework) that governs their use. If an SOA IA infrastructure achieves DIACAP (Defense Information Assurance Certification and Accreditation Process) certification, it will have been deemed “trustworthy” to the level of assurance associated with its C&A. (Note that the IA infrastructure for any particular network operation includes more than SOA IA infrastructure. DIACAP accreditation of operational environments will include traditional vulnerability assessment of basic IA infrastructure that includes things like firewalls, packet sniffers, encryption, and physical security. Certainly nothing about SOA mitigates vulnerabilities imbedded in applications deployed on local computing platforms. However, it is possible and useful to decouple consideration of the vulnerability associated with SOA activity governed by an ESB or other SOA framework.) Consequently we can “compose” trustworthy information operations by binding various Community of Interest (COI) services to the trustworthy infrastructure and invoking enterprise IA services each time data is exchanged. By metering the ESB, we can assess data transactions that occur from a particular COI service across the ESB. If all assessed transactions invoke IA services properly we can (1) “certify” the data
transactions as “assured”, and (2) assess the associated COI service as “net ready” to deploy in any similarly configured trustworthy SOA infrastructure.

The elements that define a “service” in a SOA designed for composability (e.g. Web-SOA) are: (a) self-describing; (b) discoverable; (c) executable via open standard interfaces. Assessing those elements requires a test environment that provides a realistic representation, i.e. a “reference implementation,” of the target SOA infrastructure.

Per NSA’s GIG IA policy [3], key elements that define “IA services” are: (a) developed by the U.S. Government at high assurance levels defined by the “Common Criteria”; (b) authenticate identity of people and machines that join the network including their current level of access and mission role; (b) authorize access to data and services according to dynamic modular policy that governs Risk-adaptive Access Control (RADAC); (c) provide Multi-Level Security (MLS); (d) audit all data transactions that occur on the network. Reference implementations composed of combinations of these IA services, properly governed by an ESB, or other SOA IA Infrastructure, will be certified and accredited via DIACAP.

Components of trustworthy SOA infrastructure will be incrementally improved, tested, and fielded to increasingly automate a process that dynamically authorizes or denies access to data and services on the basis of identity, current role, and emergent operational conditions. The level of certified and accredited assurance, i.e. the degree of trustworthiness, of a SOA infrastructure will increase as IA services and governing IA framework are incrementally improved, validated, and verified.

The test of whether or not a candidate net-ready artifact is self-described, discoverable, and executable via open standards is to require that artifact to bind effectively with a reference implementation of certified trustworthy SOA infrastructure. When a tested software component binds to a trustworthy SOA infrastructure, data transactions that include interaction with that component can be trusted to the level of the SOA IA Infrastructure’s accreditation, by definition. Hence, the tested artifact need not “come with” or establish its own IA accreditation. Rather, through duly diligent SwA assessment per paragraph 2. a., and by demonstrating ability to conduct trusted transactions across an ESB (or similar framework), a component can be certified as net-ready to deploy across any similarly accredited trusted SOA infrastructure.

1.1.3 Add value.

Candidate artifact should actually demonstrate improved capability. Accordingly, testers and developers should work with operational customers to define objective, testable, measures of effectiveness (MOEs) based on objective mission performance improvement goals. Testable MOEs might include mission planning cycle time reduction, “kill chain” compression, reduction of the amount of inventory at rest in a supply chain, etc. The operational customer will be the final arbiter of the acceptability of objectively demonstrated service levels during an objective operational audit of the deployed capability.

1.2. Net-ready attributes.

DoD NR-KPP Policy [4] describes four “pillars” of the NR-KPP, the Netcentric Operations and Warfare Reference Model (NCO/WRM), IA Policy, Enterprise Architectural Framework, and Key Interface Profiles (KIPS). With respect to information processing across an Internet Protocol network, the four pillars can be summarized as a requirement to demonstrate and document operational value added via IA, SOA, and data strategy.

A useful definition of “netcentric value added” is “enables rapid ad hoc discovery and collaborative application of distributed capability to achieve an asymmetric advantage.” Note that interoperability is a necessary, but not sufficient condition for netcentricity. Netcentric = Discoverable + Interoperable + Collaborative + Effective

Netcentric value added applies to engineering, acquisition, logistics, and training as much as it does to operations. All these disciplines should collaboratively enable asymmetric advantage with respect to mission outcome and acquisition efficiency.

Hence, a net-ready assessment must perform rapid, adaptive, and collaborative V&V with respect to IA, SOA, and data strategy. It should employ objective MOEs in context with operations, engineering, acquisition, logistics, and training. Assessment should include due diligence in pre-deployment simulations and verification in post deployment operational scenarios. Per discussion above, and as summarized in Figure 1, the netcentric performance attributes are as follows:

“Discoverable” means that data, services and technology can be easily found and used by previously unassociated entities. Collaboration among unknown providers and consumers of data, services and technology requires a pragmatic strategy to put data, services and technology in context
with critical conditions of interest. Producers must create and register metadata with respect to content, context and administrative detail. Consumers must create and register their critical conditions of interest. Data owners must define dynamic discretionary access policy rules that describe objective criteria for weighing the need to protect vs. the need to share information. An agreed intellectual property rights (IPR) model must support discovery and re-use of useful, information, services, and technology and information.

“Interoperable” means that a capability will bind with another previously unknown capability usefully and ad hoc. Therefore interoperability requires use of open standard interfaces. However, compliance with any contemporary set of software “standards” does not guarantee interoperability; reference implementation is required. Note that capability must be deployable under an intellectual property rights (IPR) model that supports binding with other modules.

“Collaborative” means that information value is enhanced as a result of interaction. It takes energy to interact with unfamiliar entities. Merely enabling exchange of bits among disparate players does not enhance productivity. (E.g., providing unlimited email access to soldiers in a hot zone is unlikely to enhance productivity.) Effective netcentric collaboration requires a disciplined approach to ensuring a high value-per-bit-of-data-exchanged ratio.

Testers will assist developers and customers define critical conditions of interest, and discretionary access rules, for the anticipated family of information exchanges. The assessment process can thereby inform communities that share critical conditions of interest and help them develop pragmatic semantic strategies for productive collaboration.

“Effective” means objectively demonstrated value added. The artifact must enable information to be shared more usefully. The net-ready assessment will include a post deployment operational audit to verify that a tested artifact actually improves service levels with respect to objective MOE. Delivering more bits is not the goal; the goal is to deliver more value per bit. Value added can be operational, engineering, and/or acquisition. Any latencies, unreliability, or vulnerabilities must be offset by benefits. Any useful capability developed by the government should be reusable.

Traditionally, network architectural views focus on the OSI “link” layer of data bit exchange. Web services make it practical to conduct information exchange without concern for the detail of the bit flow. It is this more abstract information exchange architecture that facilitates netcentricity. So, in an netcentric, i.e. service oriented, architecture the DoD Architectural Framework (DODAF) views should be represented at or above the OSI “session” layer. Further, the “system view” in an SOA should represent a “service view.”[7]
Artifacts should be assessed as modules in an enterprise rather than as stand alone systems. If a module is net-ready it will be expected to interact across multiple programs, and therefore across multiple supporting requirements, (e.g. JCIDS), acquisition (e.g. DoDI 5000.2), and DODAF documents.) It doesn’t make sense to force a one-to-one relationship between an enterprise capability and a particular program. The net-ready assessment process will therefore map tested capability modules to capability requirements in support of multiple programs.

The net-ready assessment should be largely runtime activity and minimize paperwork. As discussed in reference (e), the mere existence of architectural design artifacts, e.g. DoDAD view, does not guarantee, or even imply, netcentricity. A net-ready assessment will demonstrate that a capability module actually does interact netcentrically with the other components of a SOA infrastructure and thereby feed the net-ready software standard development process. Rather than require pre-created prognostic DODAF views, the net-ready assessment will use mission simulations to diagnose the actual netcentric architectural functionality. The operational “view” (OV) will illustrate the collection of simulated operational information exchanges, i.e. the mission threads. The technical view (TV) will illustrate the collection of invoked interfaces. The system (or service) view (SV) will illustrate the collection of invoked service interactions. In a web SOA all these interactions occur at or above the OSI session level, and can be observed at the OSI application layer. Hence, web tools can generate graphic representations of these different netcentric architectural abstractions as necessary for net-ready assessment documentation as a by product of, rather than a requirement for, testing. Any paper documentation required should be automatically generated as a by product of demonstrated capability, not as a pre-condition to the test.

The NR-KPP assessment matrix (figures 2-4) provides objective assessment guidance per discussion above. The net-ready assessment process will automate, streamline, and share best practices to
help developers map their artifacts to the NR-KPP assessment matrix.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Assessment Criteria</th>
<th>Data Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Documentation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Submit Netcentric Service Stack TISP Request</td>
<td>N/A</td>
<td>Provide TISP N/A</td>
</tr>
<tr>
<td>Register mission models (S) to be used for V&amp;V (Submit modeling language (e.g., BPEL) mission model(s) and mission level objectives (MLOs), identify SLAs and/or performance standards, identify operational sponsor(s) and CDIs)</td>
<td>N/A</td>
<td>Provide NESS TISP Register sponsors, CDIs, scenarios, MLOs, SLAs, and use cases</td>
</tr>
<tr>
<td>Describe net-ready strategy</td>
<td>Provide C&amp;A roadmap</td>
<td>Provide SV4B Provide data strategy</td>
</tr>
<tr>
<td>Describe re-used GFE netcentric architectural components</td>
<td>ID authorized components (NCES or certified alternative)</td>
<td>ID GFE SOA</td>
</tr>
<tr>
<td>What is the existing software maturity and functionality pedigree? (CMMI maturity model or similar) Consumer report? Developer's internal process?</td>
<td>ID C&amp;A status</td>
<td>ID software architecture pedigree (CMMI, standard stack, code print, etc) N/A</td>
</tr>
<tr>
<td>Is the intellectual property rights (IPR) model compatible with netcentric reusability? (Register all IPR license agreements. Determine whether IPR issues may help or hinder reuse from both operational and engineering perspective)</td>
<td>N/A</td>
<td>Register IPR model N/A</td>
</tr>
<tr>
<td>Illustrate the netcentric architecture involved by information exchanges demonstrated during runtime simulations (Configure the suite of services. Execute mission simulations. Generate DoD views as necessary)</td>
<td>N/A</td>
<td>Generate diagnostic views, SV4B, TV in runtime N/A</td>
</tr>
</tbody>
</table>

**Figure 2**: Proposes NR-KPP Assessment Matrix Assessment Criteria
## NR-KPP Assessment Matrix

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Assessment Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NETCENTRIC Functionality (SOA Functionality)</strong></td>
<td></td>
</tr>
<tr>
<td>Assurance and Performance</td>
<td>Test for S/W assurance and performance</td>
</tr>
<tr>
<td>Does the assessed artifact impact reliability? MOE = % of time operational?</td>
<td>N/A Reliability in simulation ≠? N/A</td>
</tr>
<tr>
<td>Does the assessed artifact impact transactional latency? MOE = time per information transaction?</td>
<td>N/A Transaction latency in simulation? N/A</td>
</tr>
<tr>
<td>Does the assessed artifact introduce IA vulnerability? MOE = SW Assurance Vulnerability score; % of time service denied; # unintended disclosures; PL #? Does assessed artifact perform adequately with industry best-of-bread?</td>
<td>SW Assurance vulnerability score? SW Performance score? Assured transactions across ESE or similar framework accredited at PL =? Network downtime in simulation =? Disclosures in simulation?</td>
</tr>
<tr>
<td>Does lifecycle model address re-capitalization via tech refresh? MOE = COTS currency?</td>
<td>N/A Current build? Yes/no? N/A</td>
</tr>
<tr>
<td>Is the artifact discoverable? Is artifact self described and employ open interfaces? MOE = yes/no GIG SOA reference model?</td>
<td>Does artifact discover bind to IA services? Does capability module map to current commercial standard SOA RM (e.g. OMG, GADS, etc)? Does artifact discover bind to is Trusted SOA in run time? Does trusted SOA services discover and bind to artifact in run time? Is metadata registered for context, context, and admin? Does artifact auto-register new metadata? What percent of on-line data is discoverable in context?</td>
</tr>
</tbody>
</table>
**2. A service oriented paradigm for IT network integration and life cycle support: Network Service Stack Tailored Integration Support Plan (NSS T-ISP).**

2.1 The issue is a “horizontal” information-centric requirement addressed by a vertical system-centric acquisition model.

DoD policy for Acquiring, integrating, and maintaining capability on the Global Information Grid mandates addressing supportability and cross-program interoperability early in the development process via an “Information Support Plan” (ISP)[6], and emphasizes an intent to leverage Commercial Off the Shelf (COTS) software; employ rapid incremental development techniques; re-use successful engineering components across programs.[7] This policy acknowledges that acquiring information processing capability should be handled differently than acquiring platforms, sensors, or weapons. Nevertheless, the policy enforcing directives invoke the formal requirements process across the full acquisition spectrum. They cite the need for formal artifacts, in addition to ISP, such as Joint Capability Integrated Design System (JCIDS) Analysis of Alternatives (AoA) documents, Integrated Capability Document (ICD), Capability Design Document (CDD), and Capability Planning Documents (CPD). These artifacts are expensive and take years to generate. They typically govern large “systems” funded by single “vertical” domain sponsors.

Other DoD policy [8][9][10][11][12][13] mandates service oriented architecture (SOA), information assurance, and data interoperability to enable “Netcentric Operations and Warfare” (NCO/W). This policy requires network software infrastructure that can be shared across programs in both build time and run time. It describes how the SOA paradigm can be used to achieve that objective faster, better and cheaper than previous approaches to interoperability through agile, continuous, improvement to network enabled capability. For example, typical SOA-enabled COTS software builds are delivered annually with quarterly updates. This rapid, incremental software development cycle can support AoA, Engineering Design Modeling (EDM), Development, or Life Cycle Maintenance (LCM), as

---

**NR-KPP Assessment Matrix**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Assessment Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value Added</strong></td>
<td>Test for dynamic accesses control</td>
</tr>
<tr>
<td>Is the artifact sponsored by multiple operational activities and/or cost codes? NOE = # of sponsors; %S leveraged against other programs</td>
<td>N/A</td>
</tr>
<tr>
<td>Does FRP model encourage re-use? NOE = cost of enterprise license; open source development model years?</td>
<td>Are intellectual property rights protected?</td>
</tr>
<tr>
<td>Does life cycle model increase relative percentage of resources available for tech refresh and retiring legacy capability vs. sustainment? NOE = % for re-capitalization</td>
<td>N/A</td>
</tr>
<tr>
<td>Does the artifact enhance value per bit exchanged? i.e., does the artifact achieve “mission level objectives” (MLO)? NOE = time, # of cycles, casualties, probability of kill, units of issue, etc.; yes/no</td>
<td>Are dynamic rules to address authorization re-use need to know vs. need to share registered?</td>
</tr>
<tr>
<td>OPTEST</td>
<td>SLA’s achieved? Is operational community satisfied with service levels delivered?</td>
</tr>
</tbody>
</table>

---

Figure: 4 Proposed NR-KPP Assessment Criteria
defined in DoD Acquisition policy, equally well. Further, many information processing requirements are identical across programs and SOA theoretically makes it easy to share, re-use, and/or improve software components developed by others.

Clearly, DoD specifically intends to apply the inherent modularity and composability of SOA to support its Acquisition objectives. However, JCIDS AoA, ISP, ICD, CDD, and CPD, are typically vertical (i.e. describing specialized systems), monolithic (i.e. a lot of money and time spent to deliver quantum improvement in capability), and serial (i.e. non-iterative progression from developing formal requirements, through engineering milestones, to deployment, through life cycle support.) Hence these artifacts, designed to field major systems, are at odds with the SOA approach to deploying information processing capability, i.e. horizontal (i.e. generic flat infrastructure), incremental (i.e. capabilities deployed rapidly in small pieces with options to try alternative vectors), and parallel (i.e. iterative continuous feedback among requirements, engineering, deploying, and lifecycle support).

In fact, these directives call for Test and Evaluation Master Plans (TEMPS) that proceed from Development Testing (DT), to Operational Testing (OT), to Interoperability Testing (IOT), to Certification and Accreditation (C&A). In this model, software is tested in the same serial fashion as platforms, weapons, or sensors. For example, a program’s software build is frozen at DT until it undergoes OT at least eighteen months later. This approach guarantees that software will be out of date by the time a system is deployed. Further, there is no standard Acquisition artifact that enables, let alone encourages, managers from different programs to mutually develop requirements, find investment partners, or identify existing solutions.

The Deputy Undersecretary of Defense for Acquisition, Technology and Logistics (DUSD AT&L) recognizes a need for less onerous approach, and has created an option for a Tailored Information Support Plan (T-ISP). The T-ISP allows small programs, legacy systems, and/or rapid technology insertion projects to develop and demonstrate supportability and cross-program interoperability with minimal supporting documentation. However, T-ISP is still program-centric and system-centric. It does not provide a means for programs (large or small) to leverage SOA as a means to deliver or consume shared network capability.

A Joint Staff Instruction defines the Net-Ready Key Performance Parameter (NR-KPP). It explains that NR-KPP should address network IA, SOA-enablement, data strategy, and mission enhancement in parallel, and that NR-KPP assessment should begin early in the development cycle. JITC is developing a process and measurable and testable criteria toward those ends. If the NR-KPP defines the necessary and sufficient criteria for supportability, interoperability, and security; then it follows that an ISP should simply be a roadmap to achieve, demonstrate, and maintain NR-KPP compliance. A tailored TEMP (T-TEMP) could facilitate the process by using early and continuing NR-KPP assessment to validate that a particular software architecture is net-ready. In that case there would be no need to freeze a program’s software build. DT, OT, IOT, and C&A would simply test and evaluate the deploying system with the current build of its software architecture installed.

Many leaders in DoD recognize the issues and opportunities described above. Accordingly, they have chartered various projects aimed to create federated development and test and evaluation (D, T&E) platforms. DISA in fact is working toward two variants of a Federated Development and Certification Environment (FDCE). The idea is that resources like FDCE would provide a means for autonomous domains to conveniently and effectively collaborate, especially with respect to network enabled, and network enabling software.

2.2 The solution is to create a complementary “horizontal” information-centric process servicing the verticals.

To bridge the gap between the stated need for cross program collaboration and the lack of an enabling process, DoD should make a subtle adjustment to an existing tool. That is, DoD should add a new eligibility category for T-ISP. Call this category “Network Service Stack” (NSS) to be cited in lieu of “program” or “system” on the current T-ISP standard documentation. Define NSS to include software services, framework, resources and/or applications associated with a well defined, service architecture. Use the T-ISP process to continuously collect, document, and advertise successful “SOA reference implementations” of network service stacks. Use these certified SOA reference implementations as test artifacts.

DoD should adopt the net-ready assessment criteria outlined in figures 1-4 as the basis for defining the NR-KPP for any particular capability. Define NSS T-ISP as “a roadmap for designing, refining, and complying with a tailored NR-KPP assessment matrix for a given network service architecture.” Define an NSS that is successfully assessed against NR-KPP criteria as “architecturally net-ready”. Define a Tailored TEMP (T-TEMP) to ensure that the current build of the net-ready software
architecture is assessed during DT, OT, IOT, and C&A of deploying systems. In other words, T-TEMP will both enable and require government program managers to consume “architecturally net-ready” COTS and GOTS software at the same rate it is updated.

NSS T-ISP-eligibility (currently ACAT II, II, & Non-ACAT) should expand to include the SOA-enabled information processing aspects of ACAT I programs. Federated D, T&E platforms (e.g. FDCE) can serve as resources to develop and execute NSS T-ISPs. In this way, software engineering gets decoupled from the slower moving aspects of system development, and major programs can perform agile, incremental, software engineering (AoA, EDM, production, and life cycle maintenance) on COTS-like time scales. Further, program managers can conveniently leverage each others’ investments in information processing infrastructure.

Vendors should pay a fee for service to use the NSS T-ISP process and get “pre-approval” for their architecturally net-ready NSS COTS offerings. This will help government program managers to more readily leverage COTS software for AoA, EDM, development, and life cycle maintenance.

The beauty of this service-oriented approach to analysis of alternatives is that it can be applied to validate itself. DoD can quickly learn if it works by investing in a handful of short duration, low cost pilot projects spirals designed around well known requirements for network services that provide assured Quality of Service for things like security, privacy, and priority delivery of valued information.