

**National Defense Industrial Association (NDIA)
Command, Control, Communications & Computers Division (C4)
&
U.S. Defense Information System Agency (DISA)
Office of Secretary of Defense, Network Information & Integration (OSD-NII)
Washington DC
C4 Enterprise Study**

**Terms of Reference
BACKGROUND**

Planning and managing the provision of capabilities and services supporting net-centric operations is different than anything the Department of Defense (DoD) has previously undertaken. Previously, warfare components were optimized within a specific operating plan with boundaries around how a component would operate. Network-centric capabilities and services, on the other hand, are specifically tailored to meet a particular mission, place, time. This distinction is important: acquiring capabilities and services meant to be used in unexpected ways will require a different enterprise governance and acquisitions philosophy. Existing practices for design and testing of networked systems are not fixing the problem. In fact, they may be making it worse. Furthermore, if these issues are not solved in concert, the costs of developing new systems will escalate, as will risk to the war-fighter, resulting in 'brittle' systems and technology incompatibilities. DoD is concerned because as these systems become more interconnected and complex, the ability to understand (and control or influence) their behavior with traditional methods is limited. These new network-centric systems need to be designed to allow evolving uses.

Today's Defense information systems are on interlinked (hardware, software and communications components) to gain advantage over adversaries. This interlinkage creates interdependencies among applications, components and systems which can lead to non-intuitive failures, expensive to maintain interfaces, and potentially undesirable systems behaviors. These second, third or nth order effects are not predictable under current system design and management practices. If network centric warfare is the goal, current methods for design, testing, validation and verification, and deploying must change from a group of stand alone tasks to an integrated enterprise marketplace of technologies and processes that change and self-correct as a system grows and evolves.

Transforming US forces is a critical component of our national security strategy. Information superiority, as enabled through ease of access to data, knowledge management, collaboration within and across disparate networks, and shared situational understanding, is a key to winning the war on terrorism.

"The essence of net-centricity is placing all information – intelligence, command and control, logistics and business information – in the hands of users, allowing them to plug in to the "network" from wherever they are and pull the information they need for their particular mission. We view the network as one including communications, computing, and storage, all provided and managed in a coherent, dynamically

scalable and secure manner. Net-centricity will facilitate powerful, immediate decision making based upon machine-to-machine interaction wherever possible"

- *Lt Gen Croom, Director Defense Information Systems Agency*

DISA has a crucial role in moving the Department toward net-centricity. We imagine and envision a world in which information is virtual and on demand with global reach. Information is protected by identity-based capabilities that allow users to connect, be identified, and access needed information in a trusted manner. It is a world in which United States military forces can deploy and connect no matter where they are located, pull information needed for their missions, and be given timely, accurate information on any threats they may face. It is a world with well-developed and available standards and no seams between the sustaining base and the tactical edge. It is enabled by an equally well-developed and available set of standards facilitating the exchange of data. It is a world in which information services, such as voice, data, and video are converged on a mature, technology-fresh, and available Internet Protocol (IP) network. It is a world in which the past differentiation between the network and computing or data processing no longer exists since computing will be done virtually across the entire network. It is a world in which the United States military can freely exchange information routinely with coalition partners and others responsible for the security and defense of the United States. The technology employed is agile, adaptive, and capabilities-based. It uses machine-to-machine communication and wireless connectivity, allowing connection regardless of location. And, we imagine and envision a world in which our soldiers, sailors, airmen, and marines are equipped with Information Technologies capabilities and services that are state-of-the-art.

To achieve net-centricity, the Global Information Grid must be a www-like enterprise in which people can discover information, orchestrate their own operational picture based on the situation at hand, and operate securely in a trusted manner. We must bring people together efficiently, help them do their jobs in ways never anticipated, and enable them to compose services to do things never envisioned.

The NDIA C4 Division is offering to perform a study that provides an industry perspective on current DoD C4 capabilities and gaps, with the goal of recommending areas of improvement in technologies, processes and services that offer "off-the-industry" enhancement to current operations. The study's scope will address in priority order key DISA/OSD C4 mission areas that follow:

- Compare/contrast DISA's Federated Development Certification Environment (FDCE) with industry's methods.
- Look at agility and parallelism in testing and certification and accreditation to gain speed and enable introduction of small service and capability modules. How should DISA balance risk management, innovation and testing?

- Look at commercially managed services: focus on the successes and lessons learned of collaboration.
- What is the role of enterprise-wide systems engineering in this highly dynamic age of web services?
- SOA and web services acquisitions, governance and service level management models. How are companies able to adapt more quickly using them and how did they create their internal models?
- Does SOA impact doctrine, and if so how does it change? How would you build tasking orders differently? Look at the intersection of doctrine and enablers.
- What should be the criteria for RFP/RFQ's when operating in this new SOA/Services world?

The NDIA C4 Division will work closely with the DISA staff and its key mission partners (see *Proposal*) to refine the scope of the study effort as necessary. The C4 Committee will form a team of Industry and DoD experts who will bring to bear a wide range of deep technical and functional C4 domain knowledge and experience to underwrite a composite understanding of both emerging Industry products, practices and services, critical C4 asset capabilities and limitations, as well as infrastructure components necessary for addressing the compelling operational requirements associated with DISA/DoD-CIO mission. The output of this study will be a written report with summarization in tabular and graphical format, and formal panel briefing that will present the findings of the team.

PROPOSAL

The NDIA C4 Division, for and on behalf of the DISA/DoD-CIO and *at no cost to the Government* will undertake a study to accomplish the following:

- Conduct an expert-based analysis of the current and projected FDCE approach, concept and requirements in support of the key programs NECC, NCES, and Service contributed capabilities focused on the mission areas outlined above.
- Produce a prioritized set of recommendations based on industry experiences that would enable near and mid-term high payoff to DISA in its efforts to increase the speed of delivery of capabilities to support the warfighters.
- The study team will explore all appropriate areas for potential enhancements to include technology, people and processes to ensure that recommended findings are comprehensive and able to be implemented.
- It will also address impediments, such as policy, legal, and liability issues that may inhibit the DoD's success to embrace SOA capabilities.
- All study team members will have valid US Secret clearances.

ASSUMPTIONS

The following assumptions are provided as guidance to the study team in the execution of this effort:

- The study team will have access to and coordinate with the appropriate standards bodies within both industry and DoD to ensure interoperability with current or targeted programs (i.e. DCGS, DoDIIS).
- This Terms of Reference (TOR) may be modified at any time in writing by mutual agreement of all parties.

STUDY SCHEDULE

The NDIA Operational C4 Gap Industry Study Team will execute this TOR document from July through December 2007. The form of the final deliverable – The Report - will be mutually agreed to by both parties. It is envisioned that there will be mid-term status briefings and progress reports. At a minimum, the NDIA study lead will provide a monthly status report of progress to C4. Key dates are as follows--

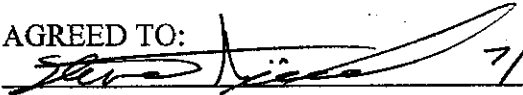
- TOR approved on/before 18 July 2007
- Status Reports – Monthly
- Mid-Term status update October 2007
- Draft Report delivery to DISA/OSD-NII

POINTS of CONTACT

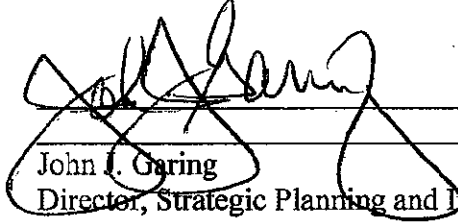
The following points of contact are listed as:

- NDIA C4 Division Lead for the study is: Mr. John M. Scott, 240-401-6574
- DISA Point of Contact for the study is: Mrs. Roberta Stempfley 703-607-6406
- The NDIA C4 Division member companies will provide up to 10 people to the Study Team.

AGREED TO:

 7/23/07

Steve Kimmel
C4ISR Chairman

 7/18/07

John J. Garing
Director, Strategic Planning and Information