| 1. REPORT DATE | JUL 2007 |
| 2. REPORT TYPE |
| 3. DATES COVERED | 00-00-2007 to 00-00-2007 |
| 4. TITLE AND SUBTITLE | Providing the Tools for Information Sharing: Net-Centric Enterprise Services |
| 5a. CONTRACT NUMBER |
| 5b. GRANT NUMBER |
| 5c. PROGRAM ELEMENT NUMBER |
| 5d. PROJECT NUMBER |
| 5e. TASK NUMBER |
| 5f. WORK UNIT NUMBER |
| 6. AUTHOR(S) |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | OASD (NII), DoD CIO, 1851 S Bell ST STE 7000, Arlington, VA, 22202 |
| 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 |
| 14. ABSTRACT |
| 15. SUBJECT TERMS |
| 16. SECURITY CLASSIFICATION OF: | a. REPORT unclassified | b. ABSTRACT unclassified | c. THIS PAGE unclassified |
| 17. LIMITATION OF ABSTRACT |
| 18. NUMBER OF PAGES | 2 |
| 19a. NAME OF RESPONSIBLE PERSON |

*Standard Form 298 (Rev. 8-98) Prescribed by ANSI Std Z39-18*
Providing the Tools for Information Sharing:
Net-Centric Enterprise Services

Ann H. Kim and Carol Macha
Department of Defense Chief Information Officer Information Policy Directorate

The Department of Defense (DoD) is establishing a net-centric environment that increasingly leverages shared services and Service Oriented Architecture (SOA) that, among other things, is supported by the required use of a common and shared infrastructure. A common infrastructure enables force capabilities to be readily networked in support of joint warfighting and operations. The Net-Centric Enterprise Services (NCES) program is a transformational program that delivers a set of shared services as part of the DoD’s common infrastructure to enable networked joint force capabilities, improved interoperability, and increased information sharing across mission area services.

As the DoD continues to face new and evolving threats, it must be poised to quickly respond to those threats with an increased level of agility. The DoD recognizes that this level of agility requires a fundamental change in the way information technology is provided and managed by the DoD. With the publication of the Net-Centric Services Strategy [1] the DoD has established a vision for achieving this agility through the use of shared services and SOAs.

The DoD Net-Centric Services Strategy outlines an approach in which the DoD’s wide range of information and functional capabilities – provided by our many systems – are made available through software-based services on enterprise networks. These software-based services deliver reusable business functionality as standardized building blocks that can be quickly adapted into capabilities that meet rapidly changing mission needs.

To achieve this vision of a services-based environment, the DoD must establish a common infrastructure that will enable networked joint force capabilities, improved interoperability, and increased information sharing across mission area services. The objective of the NCES program is to deliver a set of shared services as part of this common infrastructure.

The NCES is a Defense Information Services Agency acquisition program to adopt, buy, or create essential information sharing services needed by the DoD. As part of the common infrastructure, it will enable seamless information sharing by providing enterprise-wide services for characterizing, cataloging, locating, and accessing information on the Global Information Grid (GIG). NCES is the only program specifically tasked with providing enterprise-wide information sharing capabilities to enable information superiority, accelerated decision-making, and effective operations.

This groundbreaking program faces the following significant challenges:

**Establishing Trust.** As a provider of shared enterprise services, NCES has a vested interest in facilitating the cultural shift within the DoD to establish trust in the availability of services provided outside of one’s own organization. A secure, agile, and interoperable services-based environment in which information is much more readily visible and accessible to the DoD, as well as other authorized federal, state, local, and coalition partners requires the establishment of trust on multiple levels. The success of NCES depends on the establishment of mechanisms to enable trust in the capabilities (availability), trust in the information (assurance), and trust in the participants (identity).

NCES’ services must be made available across the DoD. Its user community spans strategic, operational, and tactical networks. To facilitate trust in NCES’ services, the NCES program must be able to define service level agreements (SLAs) that describe the reliability and performance of its services for its many users across the different networks. It needs to publish those SLAs and instrument its services such that they can be monitored against the SLAs. As a result of two recent DoD Chief Information Officer (CIO) reports [2, 3], the NCES program is actively working with the Joint Task Force-Global Network Operations (JTF-GNO) to identify needed capabilities for operating and monitoring information sharing capabilities offered as services on the GIG.

To establish trust in NCES as a service provider, the program has established the Early Capabilities Baseline through which users and organizations have an early opportunity to use NCES’ services and provide feedback to the program. This early interaction allows NCES to develop relationships with its user community, to demonstrate utility across their environ-

ments, and to continuously involve its stakeholders in the refinement of its enterprise services.

**Scaling to the DoD Enterprise.** NCES’ services are currently being developed to support an estimated number of users. However, as the DoD’s implementation of services and SOAs mature, the value of information reuse and readily found capabilities will be recognized. The program must plan for its services being leveraged in the development of information sharing capabilities by unanticipated but authorized users across the DoD and its mission partners. Any initial load balancing and scalability thresholds could very quickly be exceeded.

Through NCES’ collaboration with the JTF-GNO to identify capabilities for operating and monitoring shared enterprise services, the program is proactively developing long-term solutions to this challenge. The technical solution must be augmented by an appropriate resource model that enables the program to continue providing services according to published SLAs and accommodate growth in demand.

**Governance.** Widespread adoption of NCES’ services into business/mission processes requires the establishment of governance around their provisioning, security, use, and operation. NCES’ services must be based on common standards and rules to ensure interoperability and consistent implementation throughout the DoD. The DoD must establish a governance framework that ensures that the common standards and rules are consistently applied and enforced.

The NCES program, in collaboration with the DoD community, has been developing an enterprise services governance framework that addresses this challenge. This framework should provide limited, lightweight enterprise governance for
Get Your Free Subscription

Fill out and send us this form.

517 SMXS/MXDEA
6022 Fir Ave
BLDG 1238
HILL AFB, UT 84056-5820
FAX: (801) 777-8069 DSN: 777-8069
PHONE: (801) 775-5555 DSN: 775-5555
Or request online at www.stsc.hill.af.mil

NAME: ____________________________
RANK/GRADE: ____________________
POSITION/TITLE: __________________
ORGANIZATION: __________________
ADDRESS: _________________________
__________________________________
__________________________________
BASE/CITY: _________________________
STATE: __________ ZIP: ____________
PHONE:(____)____________________
FAX:(____)_______________________
E-MAIL: __________________________

CHECK BOX(es) To Request Back Issues:
Mar2006  □  PSP/TSP
Apr2006  □  CMMI
May2006  □  TRANSFORMING
June2006  □  WHY PROJECTS FAIL
July2006  □  NET-CENTRICITY
Aug2006  □  ADA 2005
Sept2006  □  SOFTWARE ASSURANCE
Oct2006  □  STAR WARS TO STAR TREK
Nov2006  □  MANAGEMENT BASICS
Dec2006  □  REQUIREMENTS ENG.
Jan2007  □  PUBLISHER’S CHOICE
Feb2007  □  CMMI
Mar2007  □  SOFTWARE SECURITY
Apr2007  □  AGILE DEVELOPMENT
May2007  □  SOFTWARE ACQUISITION
June2007  □  COTS INTEGRATION
To Request Back Issues on Topics Not Listed Above, Please Contact <stsc.customerservice@hill.af.mil>.

Note
   but a DoD Common Access Card is required.

Continued From Page 10

...into the enterprise networks transition plans. We have developed a DoD IPv6 master test plan to coordinate all IPv6 related testing activities across the DoD and promote efficient use of DoD test and evaluation resources. The DoD has acquired IPv6 address space and is developing a DoD IPv6 addressing plan. We recognize that DoD IPv6 transition progress depends, to a great degree, on industry’s transition to IPv6. The DoD continues to collaborate with industry standard’s bodies to ensure DoD requirements are reflected in evolving IPv6 standards.

Effective implementation of IPv6, through synchronized planning and comprehensive testing, in concert with other aspects of GIG architecture development, will enable the DoD to achieve the net-centric vision.

Note

About the Author
Kristopher L. Strance currently serves as a senior IT analyst in the Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration (NII)/DoD CIO. He is responsible for development of DoD policy for IT and National Security Strategy (NSS) interoperability, IP convergence, VoIP, and IPv6 transition. Strance has more than 30 years of experience in IT and NSS, including policy, planning, development, programming, and operational employment. His technical and management experience includes key policy and planning positions working directly for senior government executives. Strance has a bachelor’s degree in biology and chemistry from the University of New Mexico. He received his commission as an Ensign in the U.S. Navy in 1975 and was designated as a Naval Flight Officer in 1976.

OASD (NII)
DoD CIO
1851 S Bell ST STE 7000
Arlington, VA 22202
Phone: (703) 607-0249
E-mail: kris.strance@osd.mil

Author Contact
Ann H. Kim
DoD CIO
Information Policy Directorate
1851 S Bell ST STE 600
Arlington, VA 22202
Phone: (703) 602-0940
E-mail: ann.kim@osd.mil

Carol Macha
DoD CIO
Information Policy Directorate
1851 S Bell ST STE 600
Arlington, VA 22202
Phone: (703) 602-2720 ext. 145
E-mail: carol.macha@osd.mil

...and promote efficient use of DoD test and evaluation resources. The DoD has acquired IPv6 address space and is developing a DoD IPv6 addressing plan. We recognize that DoD IPv6 transition progress depends, to a great degree, on industry’s transition to IPv6. The DoD continues to collaborate with industry standard’s bodies to ensure DoD requirements are reflected in evolving IPv6 standards.

Effective implementation of IPv6, through synchronized planning and comprehensive testing, in concert with other aspects of GIG architecture development, will enable the DoD to achieve the net-centric vision.

Note

About the Author
Kristopher L. Strance currently serves as a senior IT analyst in the Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration (NII)/DoD CIO. He is responsible for development of DoD policy for IT and National Security Strategy (NSS) interoperability, IP convergence, VoIP, and IPv6 transition. Strance has more than 30 years of experience in IT and NSS, including policy, planning, development, programming, and operational employment. His technical and management experience includes key policy and planning positions working directly for senior government executives. Strance has a bachelor’s degree in biology and chemistry from the University of New Mexico. He received his commission as an Ensign in the U.S. Navy in 1975 and was designated as a Naval Flight Officer in 1976.

OASD (NII)
DoD CIO
1851 S Bell ST STE 7000
Arlington, VA 22202
Phone: (703) 607-0249
E-mail: kris.strance@osd.mil

Author Contact
Ann H. Kim
DoD CIO
Information Policy Directorate
1851 S Bell ST STE 600
Arlington, VA 22202
Phone: (703) 602-0940
E-mail: ann.kim@osd.mil

Carol Macha
DoD CIO
Information Policy Directorate
1851 S Bell ST STE 600
Arlington, VA 22202
Phone: (703) 602-2720 ext. 145
E-mail: carol.macha@osd.mil