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 environments, 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 resourcing 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

Continued on Page 16

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

1. Can be accessed at <https://gesportal.dod.mil/sites/JITCIPv6/tewg/default.aspx?RootFolder=%2fsites%2fJITCIPv6%2ftewg%2fDocument%20Library%2f1%2fJoint%20Staff%20IPv6%20Operational%20Criteria&View=%7bA84A1771%2d0AC1%2d4003%2dB341%2dC6D8EF28FA40%7d>, but a DoD Common Access Card is required.

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

Continued From Page 10

those attributes critical to the realization of interoperable shared services throughout the DoD.

Way Ahead. A common infrastructure enables force capabilities to be readily networked in support of joint warfighting and operations. Interoperability of capabilities is improved when military services, agencies, and mission partners create reusable *building blocks* through the use of services. NCES is a key provider of building block services as part of the common infrastructure to be leveraged across the DoD and its mission partners in the development of information sharing capabilities.

The NCES program needs to continue working collaboratively with the DoD community to expedite the delivery of its common infrastructure services, related standards, and guidance for using its services.◆

References

1. DoD CIO. "Department of Defense Net-Centric Services Strategy." Washington: DoD CIO May 2007.
2. DoD CIO. "Implementing the Net-Centric Data Strategy, Progress and Compliance Report." Washington: DoD CIO Aug. 2006.
3. DoD CIO. "PDM III Core Enterprise Services." Washington: DoD CIO Sept. 2006.

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