



Navy Enterprise Services

By Lt. Cmdr. Danelle Barrétt, USN

The Department of the Navy has a requirement for development of an enterprise architecture that includes the management and resourcing of key enterprise services.

Currently many disparate organizations manage separate pieces of the Naval infrastructure. This results in duplication of effort and resources. A standards-based, enterprise architecture is necessary to ensure the foundation for information transfer between these four main Naval enclaves:

Integrated Shipboard Network Systems (ISNS) - under the Information Technology for the 21st Century (IT-21) Program

Marine Corps Tactical Network (MCTN)

Navy Marine Corps Intranet (NMCI) for ashore networks in the continental United States, Puerto Rico and Hawaii

Base Level Information Infrastructure (BLII) for overseas networks

Additionally, the enterprise architecture must include seamless feeds between the general service and intelligence networks, and the ability to share information between different enclaves using National Security Agency approved multilevel security solutions. This functionality needs to be engineered from the beginning and not added on at a later stage.

Recent reorganizations in the DON and the emergence of new enterprise service initiatives, such as the Navy Enterprise Portal (NEP) and the Navy Global Directory Services (NGDS), have shed light on the requirement for an organization to be assigned responsibilities for governance and resourcing on an enterprise level. In order for ForceNet concepts to become reality, governance authority and resource sponsorship for the enterprise architecture's network services across the four main Naval information systems enclaves must be identified. This governance authority should be a council of lead agents under the direction of the Deputy Chief Information Officer (Navy) and the Deputy Chief Information Officer (Marine Corps) who would make joint decisions regarding these enterprise services and coordinate their efforts through the Department of the Navy Chief Information Officer (DON CIO). The first critical function that this council should perform is the development of an enterprise architecture that addresses the pieces that tie key enterprise services together. Through the DON CIO, this group should work closely with the Defense Information Systems Agency's Net-Centric Enterprise Services group and the National Security Agency to ensure unity of effort to improve joint interoperability. They should also act in a consortium with the other Services and key agencies (e.g., De-

partment of Homeland Security) to determine which pieces of the enterprise architecture should be managed at an agency or government-wide level.

Currently, management authority and funding for enterprise services for each of these enclaves is done within these enclaves, in most cases without regard for the larger issue of building an open standards, vendor neutral, architecture. The inability to manage these services across the four enclaves has resulted in stovepipe solutions being implemented in many of these areas. These adversely impact interoperability between users in the different enclaves, limit access to information, and cause disruptions in mission critical information accessibility and continuity to operational units moving between enclaves (e.g., Marines deploying aboard Navy ships).

One of the most important tenets of a successful Naval enterprise architecture is adherence to industry standards. Standards-based products, without vendor unique proprietary add-ons and features, are essential for maintaining an environment where interoperability and product competition will thrive. Challenges created by technology vendors' products, such as proprietary elements placed on their products, can be overcome, as markets demand compliance with open standards without these elements to improve interoperability. (As in the evolution of video teleconferencing equipment from proprietary to open-based standards.)

Many of the enterprise services are interdependent, thus the importance of developing an architecture across all of the major enclaves. Additionally, the Navy's information interoperability with other Services, agencies, allied and coalition partners will be facilitated by a unified approach to these services. Critics will argue that it is too difficult and unmanageable to try and force single solutions on an enterprise as large as the Navy; that a "one-size fits all" enterprise solution is unachievable or unrealistic. However, there are certain critical functions as discussed, that Naval networks need in order to ensure that information is ubiquitously available to support the warfighter.

Enterprise services are not unprecedented in the Navy and Department of Defense (e.g., the organizational messaging system). Imagine the adverse outcome that an enclave specific approach to organizational messaging would have had on our ability to command and control Naval forces and interoperate with the other Services and coalition partners. That is not the case with many enclave specific solutions and parochial approaches to information infrastructure and services today. The changes required to implement an enterprise architecture are more cultural and political than technical and the benefits to improved knowledge management and information transfer far outweigh the costs of implementation.

Some work has already been done on several key services of the enterprise architecture. One area where the DON has had a measure of success with enterprise services is the Public Key Infrastructure. While execution of the architecture, including issuance of user hardware and software for operation has been slower than originally planned, there is a governance authority and process for implementation of this critical service across all enclaves. In other cases, efforts have not been started at all due to funding or lack of governance, or have been stalled through institutional inertia. Several key enterprise services and their status:

Navy Global Directory Services (NGDS). This effort provides the critical foundation that many of the other enterprise services rely upon to operate. The NGDS will provide an authoritative directory infrastructure across the enterprise identifying each Navy person (active duty, retired, reservist, civil servant and contractor) using a unique electronic identifier, or flat name (e.g., john.doe), referred to a Lifetime Digital Identifier. The NGDS directory should synchronize across the four enclaves and would provide support for many enterprise services such as Single Sign On, Navy Enterprise Portal, Universal E-mail, and Electronic Role-Based User Access, which all require this authoritative directory to function. An excellent architecture for NGDS and a replication process have been developed by Space and Naval Warfare Systems Command (SPAWAR) for the Navy. However, no organization has been assigned governance of this piece, it is unfunded, and does not include the Marine Corps.

Navy Enterprise Portal (NEP). The Navy Enterprise Portal effort falls under the purview of Task Force Web (TF Web). TF Web is a Vice Chief of Naval Operations special project chartered to set standards for Navy Web enablement and implement an enterprise infrastructure to support Web services. The NEP is currently the only enterprise Web services front-end solution that complies with the DON's Navy Marine Corps Portal (NMCP) Policy. Alignment of responsibility to oversee implementation of the enterprise portal solution is anticipated this year to provide continuity as Task Force Web reaches its lifecycle end in 2004. It is hoped that this new group will also be able to positively influence enterprise architecture development of other key services discussed here beyond the portal.

Single Sign On (SSO). There are many groups within Navy pursuing SSO solutions in which a user would have one login and password for all applications and services with credentials passed and authenticated behind the scenes. Unfortunately, most of these efforts are enclave or application specific solutions, and there is no group with governance and funding to implement an enterprise SSO solution for the Navy and Marine Corps. TF Web has done extensive testing on industry-standard compliant solutions and has a SSO solution implemented with the NEP. The Secure Access Markup Language (SAML) for inter-domain SSO is continuing to be refined by the standards bodies and TF Web has selected a commercial product for the enterprise solution that complies with this standard. TF Web is also working with the Fleet Numeric Meteorological Operations Center to leverage their work on an open source SAML version 1.0 compliant SSO solution that may be used at lower lifecycle cost. Imperative for the successful implementation of any SSO solution across the enterprise is the availability of the global directory services piece and an architecture to support replication of these directories between the enclaves.

Universal E-mail. Navy and Marine Corps personnel should have a universal e-mail address that they maintain "cradle to grave" so they never have loss of continuous communication as they move between duty stations. The Universal E-mail address, similar to that used within the NMCI enclave (john.doe@navy.mil) would follow the individual throughout their career and into retirement. Users would have the ability to forward their e-mail using a Web-based simple mail transfer protocol redirect service via the NEP to a local Microsoft Exchange account without ever having to

change an e-mail display address. This would not be a centralized Exchange account solution like that implemented by the Army. A centralized mailbox solution for the Navy enterprise is undesirable as all Navy ships and remote users would still need local Exchange servers to handle mail when they are disconnected from their satellite links. Currently, lack of a global directory service, governance, and funding for the enterprise are stalling this effort.

Collaborative Tools. In a policy memorandum issued November 1, 2002, the Secretary of Defense mandated that the Joint Interoperability Test Command must certify all collaborative tool solutions by October 1, 2003, or they would not be authorized for use on DoD networks. However, there is no process or governance authority in the DON that ensures that only approved collaborative tools that will work successfully across the enterprise are selected and implemented. The result is a proliferation of disparate collaborative tools being used throughout the Department of the Navy causing interoperability problems.

Document Management and Workflow Tools. There is no one group with governance or control of funding to implement an enterprise solution for these functions. Subsequently, there are many stovepiped document management and workflow tools implemented in the Navy resulting in duplication of data at various sites. This results in a loss of confidence in the fidelity and authoritativeness of data, inability to easily search and apply intelligent agents to find information across the enterprise, and high costs to the Navy for duplicative infrastructure.

Network Monitoring. Within each enclave different network monitoring hardware and software are used. There is no enterprise approach to ensure elimination of duplicative efforts, or at least increase the likelihood that these different elements will communicate.

Replication and Synchronization of Information Between Ship and Shore. While this capability exists today to some extent with Collaboration at Sea (CAS), Lotus replication tools are currently not capable of handling the large amounts of data that will be moved between ship and shore once all applications are Web enabled. What is needed is a capability to efficiently handle the replication of data between relational database management systems (RDBMS), static data, and flat files common in Naval application infrastructures. Engineering to support this requirement must include an option for robust asynchronous replication and synchronization of RDBMS, static data, and flat files required by afloat units. Additionally, enterprise architecture plans need to include identification of standards for data compression and prioritization, and a means to maximize their use so that afloat commanders can receive the information they need in the order they need it.

Shared application, content and data storage afloat. The traditional client-server architecture afloat places an enormous burden on the ship with respect to power, air conditioning, space consumption and manpower. In a Web services environment, shared infrastructure will alleviate much of this burden. Standards for Web services development have been established by TF Web in the Navy Enterprise Application Developer's Guide and the Web Enabled Navy Architecture Version 2.0. Per Vice Chief of Naval Operations directive, application owners are responsible to ensure compliance by April 2004. Enterprise architects must en-

sure sufficient capacity and capability of shared shipboard infrastructure to host these services. New systems design must comply with the enterprise architecture and this shared infrastructure as prerequisites. Program managers will be key beneficiaries of this shared infrastructure, as they will see vastly reduced cost and complexity in deploying new services for deployed forces.

Shared application, content and data storage ashore. Critical to supporting the afloat Web services environment in an enterprise architecture is a data warehousing capability for pre-staging content for afloat users. Infrastructure, connectivity, and processes need to be identified in the enterprise architecture to support pre-staging of content at the Naval Computer and Telecommunications Area Master Stations (NCTAMS) teleport sites for information to be moved afloat. Additionally, processes must be established and solutions engineered to ensure synchronization of afloat data from the teleport sites back to the authoritative sources of data throughout the shore Navy.

Today, the Navy has no enterprise solution for providing Web data services and content storage. The result is that each individual command pays for Web servers, database engines, content servers, Web server system administrators, engineers and developers. They either do this through divisions set up and maintained within their command, or they contract out for the service. Under the NMCI contract, commands can add data storage and Web site service to their contract, but this does not address cross enclave data service standardization issues, particularly replication and data accessibility for users outside NMCI. Additionally, it does not help to identify and eliminate duplicative sources of data as anyone willing to pay can host their content within NMCI.

Maintaining thousands of separate static and dynamic Web servers and databases for content hosting/storage throughout the Navy is inefficient operationally and fiscally. With the advent of the NEP, a presentation mechanism for Web service is in place through the enterprise for interface of data to the end user. As mentioned, the data warehouse could be collocated at the teleport sites managed by the NCTAMS to host the content for these services. The advantages to having Web services content hosting in the enterprise architecture include cost savings due to elimination of individual Web infrastructure at individual commands, savings in manpower and training, improved security by using only DoD standard firewall and router configurations at the teleport sites, easier implementation of a user role-based access service, easier identification of authoritative data sources and elimination of duplicative data sources.

Engineering of these key services into an enterprise architecture under an enterprise-wide governance structure will enable ubiquitous access to data securely, reliably, and rapidly throughout the Naval enterprise. This enterprise architecture will be the basis for achieving the seamless warfighting described in Sea Power 21.



Lt. Cmdr. Danelle Barrett is an Information Professional Officer assigned to OPNAV 09W. She works on the Task Force Web.

IT'S NETWORKING THE FUTURE

By JO1 Jd Walter, Naval Personnel Development Command Public Affairs

In today's high tech, network-centric operational environment the Navy's Information Systems Technicians (IT) represent the core of a command's ability to get and stay connected. In an era of joint strike, multi-platform, network-centric warfare, information technology is central to mission accomplishment and operational readiness. To ensure the Fleet has the best trained Sailors at the ready, the Center for Information Technology (CIT) was stood up onboard Fleet Combat Training Center San Diego, Calif. The Center is charged with providing training that meets the needs of the Fleet using the most relevant and efficient delivery methods supporting the personal and professional development of all ITs in the Navy.

"This is a great day for the Navy," said Commander, Naval Personnel Development Command, Rear Adm. Kevin Moran. *"Establishing the Center for Information Technology marks a significant milestone in the Revolution in Training. In this Center we have created for the first time a single entity responsible for content, curriculum, delivery, and resources for IT training, and for management of information technology in the Navy."*

Working with the Naval Network Warfare Command (NETWARCOM) and the Information Professional Center of Excellence (IPCOE), CIT is building on the efforts of the Task Force for Education through Commitment to Education and Learning (EXCEL). The initial Job Task Analysis (JTA) for the IT rating is currently being used as a foundation for review of existing curriculum and development of new IT training. Additionally, an Information Professional (IP) Officer community JTA is under development in support of the IP Officer basic course and career planning tools for the IP community. Working closely with the Fleet to identify needs and requirements, this effort will ultimately give information technology professionals easier access to career development resources and opportunities, by providing the right training, at the right time, and in the most appropriate location. *"A key part of our mission is ownership of the process for Sailors' personal and professional development through the Sailor Continuum. We are responsible for training and education of all ITs in the Navy from the moment they enter the service to the day they depart,"* said CIT Commanding Officer Capt. Craig Turley. *"Our goal is to enhance both operational readiness and mission accomplishment. Ultimately, information technology touches each and every member of the Navy."*

Unique from its sister Learning Centers, CIT is taking a cross functional approach to the realm of information technology, and provides training to eleven ratings (IT, ET, CTO, CTM, CTT, CTR, STS, ET, FT, FC and OS).

"We are taking training and education to a new and unprecedented level," said Moran. *"We will make the greatest Navy in the world and the best Sailors in the world, even better. Together, we are going to create an educational system that will be the standard all others will follow."*

For more information on the Navy's Revolution in Training and the Center for Information Technology, please log into Navy Knowledge Online at www.nko.navy.mil.