CHIPS magazine

FALL 2004

dedicated to sharing

Vice Adm. James D. McArthur Jr.
Commander, Naval Network Warfare Command

information

Vice Adm. Patricia A. Tracey
Director, Navy Staff

technology

Robert J. Carey
Department of the Navy, Deputy CIO

experience

Rear Adm. Michael A. Sharp
Vice Commander SPAWAR
ASN (RDA) Chief Engineer
Acting DASN C4I/Space

Department of the Navy
Chief Information Officer
Mr. Dave Wennergren

Space & Naval Warfare Systems Command
Rear Admiral Kenneth D. Slaght

Space & Naval Warfare Systems Center Charleston
Commanding Officer
Captain John W. R. Pope III

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Web support
Tony Virata and Bill Bunton
DON IT Umbrella Program

CHIPS is sponsored by the Department of the Navy Chief Information Officer (DON CIO) and the DON IT Umbrella Program Office, Space & Naval Warfare Systems Center, San Diego, CA.

CHIPS is published quarterly by the Space & Naval Warfare Systems Center, Charleston. USPS 757-910 Periodical postage paid at Norfolk, VA and at an additional mailing office. POSTMASTER: Send changes to *CHIPS*, SSC Charleston, 9456 Fourth Ave., Norfolk, VA 23511-2130.

Submit article ideas to *CHIPS* editors at chips@navy.mil. We reserve the right to make editorial changes. All articles printed in *CHIPS* become the sole property of the publisher. Reprint authorization will be granted at the publisher's discretion.

Requests for distribution changes or for other assistance should be directed to Editor, *CHIPS*, SSC Charleston, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 444-8704; DSN 564. E-mail address: chips@navy.mil; fax (757) 445-2103; DSN 565. Web address: www.chips.navy.mil.

Features

CHIPS FALL 2004

Volume XXII Issue IV

Editor's Notebook

Your suggestions about the topics you would like to see us tackle in *CHIPS* are helpful in planning future issues. I want to share with you some comments from *CHIPS* reader, Al Kaniss from Naval Air Systems Command.

"I enjoyed your article in the Summer 2004 CHIPS, 'Why We Need the Navy Marine Corps Intranet.' I realize that the NMCI is not always the most popular of topics, and you did a great job of tactfully addressing its critics. If one looks at any change, like the invention of the telephone or the airplane, there were always naysayers. Too many people take computer security and interoperability for granted — until there's a problem. Thank you for pointing out these important facets of NMCI."

"By the way, I like CHIPS magazine a lot. I notice that over the years, it has expanded its focus from primarily information systems to all DoD IT issues, including the tactical realm. It's also nice to hear what our top level executives are thinking about issues we struggle with."

Thanks, Mr. Kaniss. Feedback from readers indicates great interest in interviews and articles from top Navy and Defense leadership. DON CIO, Dave Wennergren, says leadership should inspire and motivate and that is our aim too — to excite and challenge our readers.

Sept. 9, at a ceremony at the Pentagon, Secretary of the Navy Gordon R. England named two new warships, the USS Arlington and the USS Somerset, in honor of the victims and heroes of the Sept. 11 terrorist attacks on the Pentagon and for the passengers and crew aboard United Airlines Flight 93 and American Airlines Flight 77. Secretary England explained that it is a Navy tradition to name ships after great national or military leaders; heroes who sacrificed for the defense of freedom; great battles; or after great American communities that represent the resiliency, vitality and spirit of America.

The USS Arlington is named for the city and county in northern Virginia, and the 184 victims aboard American Airlines Flight 77 and on the ground, who died during the attack on the Pentagon. It also pays tribute to the first responders: firefighters, police and medical personnel who unhesitatingly rushed to the scene of the attack.

The Somerset is named for the county in Pennsylvania where United Airlines Flight 93 crashed after passengers stormed the cockpit in an attempt to retake control of the plane. Their actions prevented the terrorists from reaching the nation's capital and causing further casualties and destruction. The bravery of the 40 passengers and crew rallied the nation.

The USS Arlington (LPD 24) and USS Somerset (LPD 25) will join the USS New York (LPD 21), named in 2002, as living tributes to those who suffered in the terrorist attacks of Sept. 11, 2001. At the Pentagon ceremony, England spoke to the victims' families and the first responders in the audience. *"We honor and recognize the profound service and sacrifice of all those who lost their lives … who were injured … Soldiers, Sailors and civilians … and the thousands of rescue personnel and citizens who came forward to provide aid to their neighbors."*

Secretary England said the ships are symbols of freedom and military might. *"The USS Arlington and USS Somerset will help America project power to the far reaches of the earth and will support the cause of freedom as we engage in the current war on terrorism…. The courage and heroism of the people aboard those flights, and in the Pentagon, will never be forgotten by the American people."*

Sharon Anderson

Right: Honored guests observe as the Navy unveils a model of a San Antonio-class amphibious dock landing ship (LPD), following the official naming ceremony for USS Arlington (LPD 24) and USS Somerset (LPD 25). Arlington and Somerset join the previously named USS New York (LPD 21), in honoring the heroes and citizens, who provided aid and support during and after the Sept. 11, 2001 attacks.

About 20 first responders and 35 family members of the Pentagon victims attended the ceremony including Herb Wolk, 57, a retired Navy civilian employee, who lost his son-in-law, Lt. j.g. Darin H. Pontell, 26, in the attack on the Pentagon. Mr. Wolk was instrumental in the Navy's naming the Arlington and Somerset according to Capt. Kevin Wensing, Secretary England's spokesman. "We had requests for many names, but none seemed appropriate until Mr. Wolk's letter-writing campaign," said Wensing.

"I am so grateful that the Navy has named these ships. They serve as living memorials to those who died. I hope they motivate and inspire the crews and Marines in their missions," said Mr. Wolk.

U.S. Navy photo by Chief Journalist Craig Stawser.

DON CIO

Putting information to work for our people

The ability to communicate is critical in all phases of our business. We are quickly becoming a society with diverse communication tools that include mobile phones, text messaging, instant messaging, voice mail, e-mail and of course — the desktop phone. We also communicate with data in the form of applications, e-mail, reports and presentations. Video — a growing personal and business communication format — is now poised to be as commonplace as voice, utilizing technologies ranging from camera phones and inexpensive Web cameras to more complex video conferencing equipment.

The Department of the Navy is on the brink of new commercial grade services that will provide true integration among data, voice and video — three former stovepipe technologies. The opportunity to achieve economies from positioning these technologies on NMCI, our Enterprise network, is very attractive.

The world of "converged communication" promises to broaden our horizons, and enable our business processes with communication-based applications that are independent of the communications structure. Such applications will recognize the capabilities and preferences of the destination device/user and convert text to voice, voice to text — and provide video responses. The future will provide the ability to retrieve messages in any format, anywhere, anytime.

While this may sound futuristic, these capabilities are being explored today. The benefits afforded by these capabilities to our business processes and the enhanced features that will support the warfighter are vast. Knowledge management will exploit communication systems to allow combatants and deployed forces a reach back for tutorials, updated manuals and video demonstrations. A single subject matter expert can provide front line consultation for dispersed combatants on a global basis through chat, voice or video. Supply chain communication will provide location, status and availability of critical components to expedite support for the warfighter. Telemedicine can engage surgeons; scientists and other medical staff in complex procedures; biological and chemical analyses; and battlefield triage.

The challenge we face is to constantly refine our Enterprise vision and align our organizational strengths to deliver these services. We have engaged Navy and Marine Corps commands in reviewing today's telecommunication services, and we are developing a telecommunications strategy for the future. What a great challenge! I encourage you to do your part in preparing the way for the opportunities and benefits that the integration of converged communication will bring.

Dave Wennergren

Interview with Vice Adm. Patricia Ann Tracey Director, Navy Staff

Director, Navy Staff Mission

To coordinate and synchronize the internal Navy Staff processes and actions of OPNAV Principal Officials in the execution of current Navy policies and priorities as established by the Chief of Naval Operations.

Vice Adm. Tracey graciously agreed to an interview with CHIPS on her last day of active service, Sept. 1, where she spoke candidly about her three years on the OPNAV staff. Vice Adm. Tracey retired Oct. 1, 2004.

CHIPS: What are some of the accomplishments that you are most proud of during your three years as DNS?

Vice Adm. Tracey: First, is that the Navy staff was back in business by midnight of Sept. 11. In addition to our casualties, we lost 89 percent of our spaces in the Pentagon. This is what I am most proud of because it indicates the character of the people, military and civilian, who choose to serve in the Department of the Navy.

Second, is the evolution of the headquarters business processes becoming less bureaucratic and more in line with the principles of business planning. In my previous tours at headquarters sometimes we would start to re-examine all our priorities again at the beginning of a budget year. With the CNO's leadership and the Sea Power 21 vision we were able to discern a future course. It made sense to pick a path aligned with that course that was most effective, most efficient and one that we use on a continuous growth basis.

Last, we are working to simplify and standardize business processes. We haven't made as much progress as I would have liked to make. We started winnowing legacy applications in connection with cutover to NMCI. But it became apparent that the number of applications was a secondary question.

The first question should have been what kind of business process reengineering would contribute to greater productivity. And the applications that would underpin those business processes should have been the leading factor.

CHIPS: Are you talking about results-based spending in line with the Clinger-Cohen Act?

Vice Adm. Tracey: I'm talking about the whole Navy budget and our focus on a transformational approach to what future Navy capabilities need to be. It is the execution of a headquarters' process that allows us to put together a budget that is on a consistent path reaching far into the future. We understand what kind of capabilities we are supposed to be producing, buying and sustaining for the joint warfighter.

CHIPS: So you are looking at the budget from a Joint Vision 2020 and mission-readiness perspective?

Vice Adm. Tracey: Yes, all those things and the CNO's Sea Power 21.

CHIPS: You mentioned the difficulty in reducing the number of legacy applications. Any other challenges?

Vice Adm. Tracey: Not here on the staff, but for NMCI implementation the Navy was not as quick to understand what was required to adapt to an enterprise approach to information management/information technology from an infrastructure, business process and application perspectives. But this has dramatically improved in the last six to nine months. We were so used to being independent as buyers and users of IT that we did not adapt to the kind of behaviors that are required for an enterprise network — NMCI. This has improved a fair amount, but it is a big change for us. And I don't think that any of us appreciated how big a change it would be.

CHIPS: In an interview with DON Deputy CIO, Rob Carey, he talked about an even greater centralized approach for Department IT.

Vice Adm. Tracey: I think one of the big challenges is knowing what to centralize so that you get the benefits of standardization when processes need to be standardized — at the same time not losing the agility to capture the benefits of information technology. You don't want to become so centralized and bureaucratic that you can't make progress. But it is clear that one of the big payoffs in information technology comes from standardizing processes so that information is reliable and ubiquitous for sharing.

Mr. Carey's right, we will do more centralizing than we have been used to. We would like to go to an approach that is heavily dependent on established standards at the same time giving people the freedom to do what they need to do to get their jobs done within those standards — a kind of federated process of IT management.

This is still a big change for us. In the past every command that could find the resources to purchase an application or set up its own network could do so, but that is inconsistent with where we are trying to go.

CHIPS: Mr. Carey mentioned that the Department is investigating new approaches for centralizing technology solutions for capturing cost savings and efficiencies, for example, Voice over Internet Protocol (VoIP) as part of an enterprise telephony strategy.

Vice Adm. Tracey: I think that is a way off, but it is a good example of the kinds of things that we believe will give us the opportunity

to make us more efficient and to leverage large-quantity buys for these services. We do that now, but in a fragmented way. We are looking not only at standardizing, but leveraging the buying power of the Navy.

CHIPS: Much has been done to reduce the number of legacy applications in the Navy, but we seemed to have slowed down in the last six months. As the head of the Functional Area Manager (FAM) process; do you think the Navy can reduce the number of applications further?

Vice Adm. Tracey: Oh, yes. Our first push was to reduce the number of applications that required NMCI certification to load on the network. The number of applications made a big difference in how long it would take and how much it would cost to cutover a site. So it was important to get the number of applications down quickly. As you probably know, our first round of data was dirty; we had application numbers ranging from 100,000 to 30,000.

The Functional Area Managers identified a portfolio of between 7,000 and 10,000 that we believe can support the Navy IM/IT functions. And we are trying to get that number reduced to about 3,000 applications that are recognized by our largest commands as the ones they need to conduct their business. There will still be duplication inside a portfolio of that size, so we expect to continually reduce the number of applications. We have done some benchmarking and most businesses operate with fewer than 1,000 applications. I don't know if we will get to that number, but we are well above it right now.

In addition to leading all the FAMs, I am the Administration FAM. In my area, many of the applications we use are COTS products that are not individually very expensive. Typically, commands bought a word processing application, did not update it and used it until it was no longer supported by the vendor. So we have to do a business case analysis to see whether forcing a command to migrate to a standardized word processing application before the expiration of the command's current application's useful life will be a good investment.

At this phase we are doing business case studies to make further reduction decisions so that's why it appears that we have slowed down, but we've been busy!

CHIPS: You have extensive experience in training and manpower. Do you foresee any major changes in the way personnel are assigned and rotated from ship to shore because of new technologies?

Vice Adm. Tracey: We are undergoing an intensive Department review of our human capital strategy. Included among the things that we are looking at are the policies, practices and mechanisms for developing and assigning people. We are very focused on developing expertise for warfighting in the future and making sure that people get the experience they need to meet the new demands.

One of the principle drivers for how we assign people right now is the sea-shore rotation policy. We would like to place people in repeated assignments that develop their technical skills. That will take some adjustment to how we organize maintenance and training ashore. So people will be more likely to stay within their specific technical skills.

Now our sea-shore rotation model takes personnel out of their skill areas for an extended period of time. For example, in order to provide shore duty assignments for some of the highly technical skills like Fire Control Technician, we currently assign Sailors in those specialties to Force Protection assignments ashore. We would like them to organize in a way that would enable them to continue to develop their expertise while ashore. Strategies that will distribute training to fleet concentration areas should help us to do that.

The deeper expertise that will come from being able to keep personnel within their skill areas will pay off in terms of the readiness we will need for the future. These are long-term (probably more than a few years) adjustments that require a realignment of training, maintenance and manning strategies.

We want to be ready for the much smaller crews on the ships we are buying now. One thing that will change is our ability to reach-back for some kinds of skills. I expect a number of maintenance functions will be guided by technicians who are not deployed with the ship. So there will be a shift in how the work is distributed from deployed to non-deployed personnel. That is one of the advantages of technology — the advantage the ship can have to stay connected with subject matter experts ashore.

CHIPS: One of the concerns I've heard from female Naval personnel is the limited number of opportunities for them at sea. Will the new ships provide more flexibility for assignments?

Vice Adm. Tracey: Future ships are being designed with an eye toward mixed-gender crews. The thing that has limited our ability to put women to sea has been the time and cost to modify the berthing compartments on existing ships. The ship has to be in a long enough maintenance period to allow the modifications to be made. We have made changes regarding the size of the berthing spaces in the last few years that have shortened the time it takes to make the modifications.

Obviously, it is harder to fill an 80-man compartment than it would two forty-man spaces — one with men, one with women. So there is more flexibility in designing smaller compartments.

I expect in the future there will be no bars to women rotating to sea just the way men do.

CHIPS: The next step after completion of the rollout of the remaining seats is populating the NMCI with the Navy Marine Corps Portal and other capabilities. What are you looking forward to seeing on the NMCI, and what do you think will be most helpful to users?

Vice Adm. Tracey: For an organization the size of the Navy being able to access data that is open to users on role-based authority is significant. Right now I task a subordinate activity to collect information for me, and if I don't ask all the right questions the first time I have to go back and ask for more information. As an example, data warehousing and role-based access to information for someone at headquarters will allow speed in analyzing data and the ability to forward a recommendation without having to exercise the chain of command to get that information. This will make a gigantic difference in the way people do their jobs.

Another example in the supply system: We are getting to the point where a certain number of items in stock will trigger a reorder. This means people will be less involved in rote processes, and we can focus their talent on the more sophisticated decision making and execution end of the warfighting business. I think that is pretty exciting because it enables better decision making, and you won't have to wait for someone to give you information.

Freeing people from the more mundane elements of their jobs also gives them the opportunity to use their talents to do the exciting things that they joined the Navy to do.

CHIPS: What do you think are some of the significant achievements regarding realizing the CNO's Sea Power 21 vision during the last three years?

Vice Adm. Tracey: First, the whole Navy is aligned toward a vision of the future. And for an organization this large to have so many good, forward thinking people pursuing a common vision is important. Since decision making is decentralized to a great extent if we didn't have a common vision you could have people pulling in opposite directions.

Sea Power 21 has redefined the future for us. It has focused us on the capabilities that we need to fight jointly; the ability to base capabilities at sea for the entire joint force is the most compelling achievement. The second one is the notion of FORCEnet as a way to connect the sensor to shooter and make distributed combat capability much more effective, much more precise.

As I said in response to the first question, because we have had this steady view of where we are going, the budget process has been a planning process rather than a re-examination of priorities, and Sea Power 21 has been our guide.

The other big thing is the CNO's view of Sea Warrior — the Sailor of the future — a highly motivated professional who stays motivated because he or she has useful, highly valued work to do with a career path that ensures professional development and provides lots of choices for career development. It will also provide opportunities for a change in direction for what personnel want to do in the Navy. That is probably the most exciting. As the CNO says, it is the genius of our people that makes us the kind of Service that we are and to have our leadership focused on this different approach to making our people even better is just incredible.

CHIPS: The establishment of the Information Professional (IP) Officer Community is a success story. Do you think the community will grow?

Vice Adm. Tracey: Yes, I do — and grow in impact not just in size. It was a long time coming, but recognizing that this is a fundamental skill for our Navy has been a real breakthrough for us.

Vice Adm. Patricia Ann Tracey

Vice Adm. Tracey is Director, Navy Staff (DNS). She serves the Chief and Vice Chief of Naval Operations and directs the Navy Headquarters Support functions for 1,200 personnel.

Admiral Tracey completed Women Officers School and was commissioned as an ensign in 1970, following graduation from the College of New Rochelle with a Bachelor of Arts degree in mathematics. She also holds a master's degree, with distinction, in operations research from the Naval Postgraduate School. Her initial assignment was to the Naval Space Surveillance System in Dahlgren, Va., where she qualified as a command center officer and orbital analyst.

Following a tour on the staff of the Commander in Chief of the Pacific Fleet, she served at the Bureau of Naval Personnel as the placement officer for graduate education and service college students.

From 1980 to 1982, Vice Adm. Tracey served as an extended planning analyst in the Systems Analysis Division on the Chief of Naval Operations' staff. She served as executive officer of the Naval Recruiting District in Buffalo, N.Y., until 1984, where she was assigned as a manpower and personnel analyst in the Program Appraisal Division of the Chief of Naval Operations' staff.

Vice Adm. Tracey commanded the Naval Technical Training Center at Treasure Island from 1986 to 1988. She then headed the Enlisted Plans and Community Management Branch on the Chief of Naval Personnel's staff for two years. She assumed command of Naval Station Long Beach, Calif., in 1990. Upon completion of her command tour, Vice Adm. Tracey reported as a Fellow with the Chief of Naval Operations' Strategic Studies Group at the Naval War College.

Vice Adm. Tracey was assigned as the Director for Manpower and Personnel, J-1, on the Joint Staff from July 1993 to June 1995. From June 1995 to June 1996 she served as Commander, Naval Training Center, Great Lakes. She was the Chief of Naval Education and Training, and Director of Naval Training for the Chief of Naval Operations from July 1996 to December 1998.

From December 1998 to August 2001, she served as the Deputy Assistant Secretary of Defense (Military Manpower and Personnel Policy), Washington, D.C. She was responsible for the establishment of all policies concerning military personnel matters including accessions and retention programs; compensation and benefits; and policies governing classification, assignment and career development for 1.4 million service members of the Department of Defense.

The admiral's personal decorations include two Defense Distinguished Service Medals, two Navy Distinguished Service Medals, three Legion of Merit awards, three Meritorious Service Medals and the French Legion of d'Honneur.

Editor's Note: Navy Vice Adm. Albert T. Church III, is replacing Vice Adm. Tracey as Director, Navy Staff, DNS, Office of the Chief of Naval Operations, Pentagon, Washington, D.C. Church recently served as Inspector General, Department of the Navy, Washington, D.C. CHIPS

Interview with Vice Adm. James D. McArthur Jr. Commander Naval Network Warfare Command

NETWARCOM's Global Mission

Naval Network Warfare Command creates warfighting and business options for the Fleet to fight and win in the information age. We deliver and operate a reliable, secure and battle-ready global network. We lead the development and integration of Information Operations capabilities into the Fleet.

To serve as the Navy's Functional Component Commander to U.S. Strategic Command.

NETWARCOM's Mission Statement

To act as the Navy's central operational authority for space, information technology requirements, network and information operations in support of Naval forces afloat and ashore; to operate a secure and interoperable Naval Network that will enable effects-based operations and innovation; to coordinate and assess the Navy operational requirements for and use of network/command and control/information technology/information operations and space; to serve as the operational forces' advocate in the development and fielding of information technology, information operations and space and to perform such other functions and tasks as may be directed by higher authority.

Vice Adm. McArthur assumed command of the Naval Network Warfare Command March 26, 2004. The admiral talked to CHIPS about several of NETWARCOM's priorities including the new space cadre.

CHIPS: Let's talk about your top priorities starting with FORCEnet. NETWARCOM Deputy Commander Rear Adm. Singer said that the Navy must determine its doctrine and operations before it determines the shape of FORCEnet. Can you elaborate on what this means?

Vice Adm. McArthur: Operationally, FORCEnet refers to the capabilities that dramatically improve the systems and processes for providing effective networked, Naval command and control in 2015-2020. Command and control is the means and methods by which a commander recognizes what needs to be done in any given situation and sees that appropriate actions are taken. The objective of FORCEnet is to provide commanders the means to make timelier decisions with better situational awareness than they currently can and to see to the effective execution of those decisions.

The underlying premise from which FORCEnet gets its power is the network effect, which causes the value of a product or service in a network to increase exponentially as the number of those using it increases. The more commanders, staffs, units, individual platforms, weapons and sensors that are linked together in a network, the more valuable will be each and the more powerful will be the overall network. We're in the process of wrapping up a FORCEnet functional concept, and planners will be able to envision key benchmarks in the developmental process. FORCEnet is not just information technology (IT) — it is the Doctrine, Organization, Training, Material, Leadership and Education, Personnel and Facilities coordination that leverages IT.

CHIPS: Another of your mission areas is Information Operations. Would you explain what this is and how it will impact the way we conduct warfare in the future?

Vice Adm. McArthur: The Chief of Naval Operations has established Information Operations (IO) as a primary Naval Warfare Area, equivalent to Air, Land, Maritime, Space and Special Operations. It is comprised of five core military capabilities: Computer Network Operations, Electronic Warfare, Psychological Operations, Military Deception and Operations Security. IO is a major part of Naval forces' overall strategic planning and operations to shape and influence potential adversaries' understanding and intent. IO significantly enhances deterrence and accelerates the pace of operations.

CHIPS: The CVN-21 program, the next-generation of aircraft carrier and the modernization of the entire fleet of DDG-51 Arleigh Burke-class destroyers have been talked about as part of the FORCEnet effect. Will FORCEnet require a heavy investment in structural changes to Navy ships, aircraft and shore facilities to ensure the flexibility that FORCEnet is expected to achieve?

Vice Adm. McArthur: I think we'll see different equipment but not major structural changes. The concept behind FORCEnet is not just to bring more equipment and systems to the warfighter but to consolidate the existing multiple paths of information flow into a single integrated universal database from which user's can create their own picture of the battlespace. FORCEnet architecture will enforce a discipline on all command, control, computers and combat systems to ensure this shared battlespace environment — within Naval forces as well as in a joint and coalition environment.

CHIPS: Rear Adm. Singer talked about achieving FORCEnet goals of a level one capability in 2007, a level two capability in 2010 and a level three capability in 2014. Can you provide some examples of these levels of capabilities? (See Figure 1 on page 10.)

Vice Adm. McArthur: FORCEnet is built around the synergistic integration of many efforts using a spiral development process that results in a 'system of systems.' It is an architectural framework that integrates warriors, sensors, networks, commanders, platforms, effects and weapons into a networked, distributed combat system.

FORCEnet will take current capabilities and develop them into a hybrid of initiatives to include remote sensors, UAV/UUV/CAVS and advanced human-centric interoperability. This would evolve into integrated systems — seamless, fault tolerant networks, dynamic battlespace deconfliction and be Web-enabled. Ultimately, in the 2015-2020 time frame, we would evolve to a fully integrated and interactive system for all users that would include fully-automated networks, consolidated decision-support tools and full human-centric integration of the 21st century warrior.

CHIPS: What is NETWARCOM's role in enterprise IT in regard to the BLII OCONUS, IT-21, future requirements and IT governance?

Vice Adm. McArthur: To answer this question, let me go back to NETWARCOM's mission — our mandate is to provide a reliable, secure, interoperable and affordable network that creates rapid, high quality decision-making, effects-based operations and combat readiness across the Navy. To do so, we must help to lead Navy's efforts to deliver a seamless network environment for our Sailors and civilians, whether they are at sea, overseas, at home or away from their home station on travel. One of the greatest challenges facing today's Navy is to make our various enterprise and stand-alone networks operate together as a whole and to bring this vision to reality — as soon as possible.

This means that users of today's program of record networks such as the Navy Marine Corps Intranet (NMCI), Overseas Naval Enterprise Network (ONE-NET – a new and more descriptive name for Base Level Information Infrastructure OCONUS – BLII OCONUS), and Integrated Shipboard Network System (ISNS) also known as Information Technology for the 21st Century (IT-21) need to be able to exchange their information seamlessly regardless of which network they're using, and they need to be able to exchange information with their counterparts in the other Services as well — this is the vision of a truly enterprise network.

Our role is to operate, maintain and ensure the security of today's networks — but also to be a forceful advocate for change to integrate the Navy's networks and, most importantly, to ensure that the applications and services that traverse the networks will work together and deliver warfighting capability to our Sailors into the future.

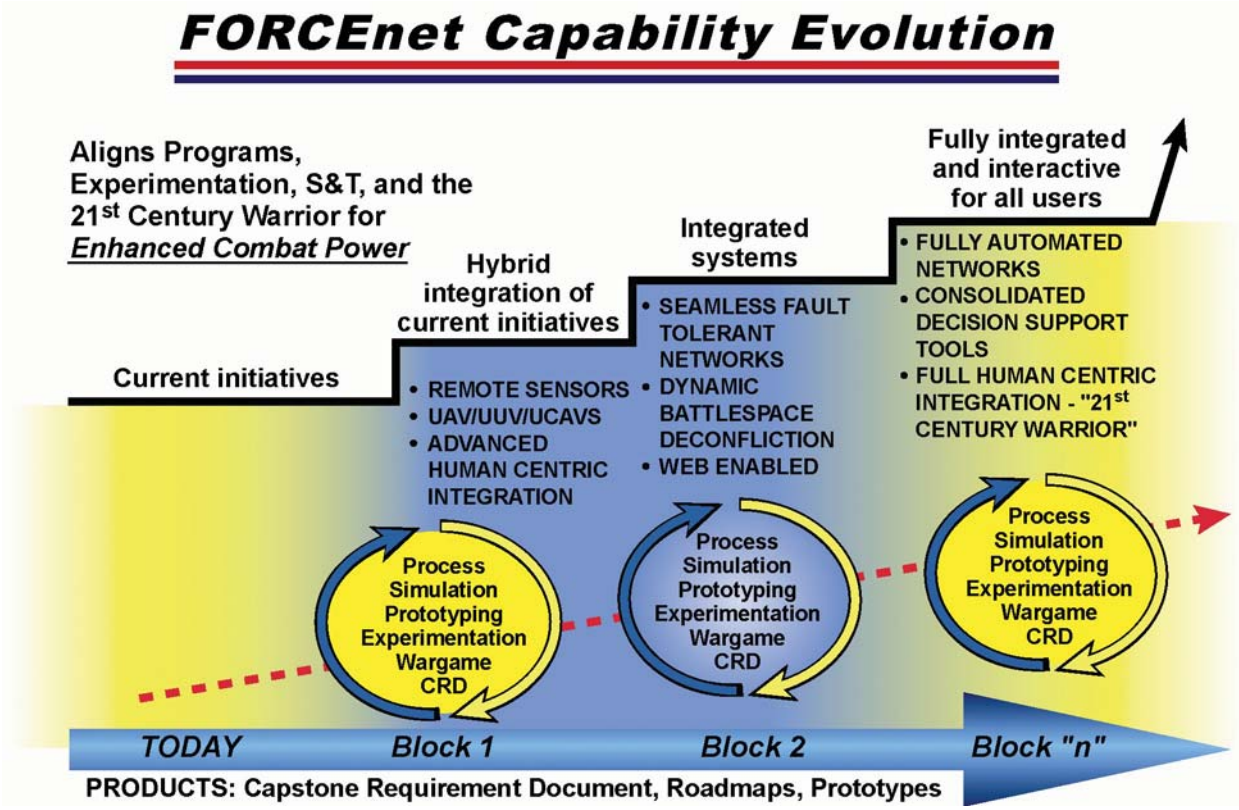
CHIPS: NETWARCOM is working with the Joint Forces Command on Joint Battle Management Command and Control or JBMC2. Can you talk about your role in the JBMC2?

Vice Adm. McArthur: JBMC2 was initiated to promote DoD's goal of fielding fully joint and interoperable battle management command and control capabilities. As a result, JBMC2 cuts across a wide range of commands within the Navy and other Services. Naval Network Warfare Command, on behalf of Commander Fleet Forces Command, serves as the Navy's representative to the JBMC2 Board of Directors (BoD). As CFFC's representative, NETWARCOM provides an operational perspective to the numerous critical issues addressed by the JBMC2 BoD. Our work with Air Force Command and Control, Intelligence, Surveillance and Reconnaissance (AFC2ISR) and Army Training and Doctrine Command (TRADOC) complements the JBMC2 work.

CHIPS: NETWARCOM has evolved since its inception a little over two years ago. Can you describe some of the changes that have taken place?

Vice Adm. McArthur: Yes, we've grown in our mission responsibility, but we have been able to achieve overall net savings for

Figure 1.



Vice Adm. James McArthur in his office at Naval Network Warfare Command during the interview with CHIPS Aug. 30, 2004. The admiral talked about NETWARCOM priorities including FORCEnet; information operations; network assurance and security; and the new space cadre.

the Navy in both manpower and resources. NETWARCOM has assumed duties and responsibilities as a hybrid Type Commander for global C4 and Naval networks. Fleet Forces Command and Commander Pacific Fleet have divested most of the duties and responsibilities for these functions. The alignment of global C4 and network functions to NETWARCOM is intended to increase coherency, efficiency and capability of network management — and provide a single point of contact for network issues ranging from requirements to operations.

This alignment is a perfect opportunity for our Navy and NETWARCOM. Embedded in this alignment are expanded missions, responsibilities, authority and accountability. It centralizes network operations, command and control, information operations and FORCEnet — which were created and developed with a unified fleet and joint perspective.

Ultimately, this expanded mission for NETWARCOM is about giving commanders greater command and control capability through networked C2 and combat systems to better employ a full range of effects in the battlespace. The alignment will ensure that speed, agility, flexibility, discipline and capability are integral to network-centric warfighting capability and business effectiveness.

CHIPS: How is the Navy and NETWARCOM dealing with space policy and management related to Navy space personnel?

Vice Adm. McArthur: Navy has established a space cadre to integrate the essential capabilities provided by space systems at every appropriate level throughout the Naval force and to shape the outcome of joint deliberations on future space systems capabilities to ensure combat effectiveness of Naval forces. The professional space cadre, competing for appropriate senior leadership positions in joint, national, and Naval space programs and organizations, will accomplish these important functions.

We've taken a multifaceted approach in partnership with the Bureau of Naval Personnel, Naval Post Graduate School and SPAWAR Space Field Activity. In addition, we share responsibilities with the Chief of Naval Operations staff to engage with the Department of Defense space architect and National Security Space Office. Additionally, we have developed a Fleet Space Campaign Plan to improve fleet effectiveness with smarter, more aggressive use of space.

For more information about the Naval Network Warfare Command's priorities go to the command's Web site at http://www.netwarcom.navy.mil/.

CHIPS

Vice Adm. James D. McArthur Jr.

Vice Adm. McArthur graduated from the U.S. Naval Academy in 1972. Following his commissioning, he served on the USS Caloosahatchee (AO 98) and qualified as Officer of the Deck (U/I) prior to entering flight training. He was designated a Naval Aviator on Dec. 6, 1975.

Admiral McArthur arrived at his first fleet squadron, VF-211, in December 1975 and deployed twice to the Western Pacific/Indian Oceans on the USS Constellation (CV 64). After three and one-half years, Vice Adm. McArthur reported to VF-124 as an instructor pilot and landing signals officer. In July 1982, he returned to the fleet with VF-1, and deployed on the USS Ranger (CV 61) and USS Kitty Hawk (CV 63).

Vice Adm. McArthur was then assigned to the Office of the Chief of Naval Operations for Strategy, Plans and Policy (OP-60) in December 1984. In August 1986, he reported to VF-24 as executive officer, and assumed command of the squadron in December 1987. Upon detachment in May 1989, he reported to Carrier Air Wing FIFTEEN as the deputy commander. In July 1991, he transferred to the Bureau of Naval Personnel to become the Head, Aviation Commander Assignment Branch.

Following the BUPERS tour, he took command of Carrier Air Wing ELEVEN embarked on the USS Abraham Lincoln (CVN 72). After a deployment to the Arabian Gulf, he was reassigned briefly as the Head, Aviation Officer Distribution/Aviation Captain Assignments (PERS 43) and then was selected to serve as Executive Assistant to the Vice Chief of Naval Operations in July 1995. In August 1996, he became the Executive Assistant to the Chief of Naval Operations.

In May, 1998, he reported to the Joint Staff as the Deputy Director for Strategy and Policy (J5). He was relieved as Commander, Carrier Group TWO on May 25, 2000, and deployed to the Arabian Gulf with the Harry S. Truman Battle Group. After deployment, he was assigned as the Director of Operations (J3) at U.S. Space Command and subsequently, the Director of Global Operations, U.S. Strategic Command. March 26, 2004, Vice Adm. McArthur assumed command of Naval Network Warfare Command in Little Creek, Va.

Vice Adm. McArthur has more than 1,100 arrested landings and 4,300 flight hours and has been awarded the Defense Superior Service Medal (two), the Legion of Merit (three), the Meritorious Service Medal (four) and the Navy Achievement Medal.

Interview with Rear Adm. Michael Sharp
SPAWAR Vice Commander
ASN (RDA) Chief Engineer
Acting DASN C4I/Space

The goal sounds simple enough: Provide warfighters with battlespace information that is optimally relevant, timely, accurate and usable. In reality, however, creating the architecture to align myriad frequencies, protocols and systems — all the bits and bytes that cut across platforms and warfighting missions — proves much more challenging.

It's a complex subject Rear Adm. Michael A. Sharp knows well because no matter which of the four hats he wears, questions regarding interoperability, integrated systems and capability-based acquisition are never far away.

As the Space and Naval Warfare Systems Command Vice Commander, Sharp has a vital role in developing FORCEnet and network centric-capable systems for the warfighter. "FORCEnet has become part of our language …. It is the standards and architectures that allow all of our individual programs to work together," explained Sharp, who has been Vice Commander since December 2002.

As the Chief Engineer for the Assistant Secretary of the Navy for Research, Development and Acquisition, Sharp implements capability-based acquisition for the Navy to develop systems that are born with net-centric potential. "The RDA Chief Engineer has always been looked at as an honest broker," said Sharp, who served as a nuclear attack submarine commanding officer earlier in his career. "When we're involved with an architecture, it allows us to determine what's best for the Navy — and not necessarily what's best for an individual systems command."

As the 30-year veteran prepares for retirement this fall, Sharp discussed with *CHIPS* what FORCEnet development obstacles have been overcome and where capability-based acquisition is heading.

CHIPS: Could you tell us about your responsibilities in each of your assignments?

Rear Adm. Sharp: I actually wear four hats. But they're all very closely related, which is how I can manage to juggle them all. I am the third Chief Engineer for ASN (RDA), Assistant Secretary of the Navy for Research, Development and Acquisition. The first two engineers primarily operated out of NAVSEA (Naval Sea Systems Command) because they were physically located there. When I became the first SPAWAR Vice Commander to be located in Washington D.C., Secretary John J. Young, ASN (RDA), thought it would be a good fit for his chief engineer, and it's worked out very well.

The chief engineer job is focused on C4ISR. The challenge that SPAWAR has had is putting together a capabilities-based architecture. Capabilities-based products are a similar challenge for Secretary Young. We get Navy acquisitions organizations involved — NAVSEA, NAVAIR (Naval Air Systems Command), SPAWAR, MARCORSYSCOM (Marine Corps Systems Command) and NAVSUP (Naval Supply Systems Command) — but we also have to work in the joint arena because our Navy architecture must fit into the larger joint and coalition architecture. That is a mandate for FORCEnet.

The chief engineer hat gives me a role in acquisition that I wouldn't have solely as Vice Commander. Personally, it gives me the ability to operate in whatever swim lane I choose to.

The acting Deputy Assistant Secretary of the Navy position came up earlier this year when Dr. Dale Euler moved to U.S. Special Forces Command, and Secretary Young asked if I could take on that role.

It has fit quite well too because I'm looking at the specific attributes of the major command and control programs that I deal with. The focus is on how the programs fit into the acquisition and less on how they fit into the big picture of architecture development. We help develop acquisition strategy and documents, and support the PEO C4I and Space and the program offices. I'm also the Navy representative to the Base Realignment and Closure subgroup for C4I. That has given me some insight into where we are trying to go jointly.

CHIPS: When did that role come up?

Rear Adm. Sharp: I've been doing it for about a year. While I can't discuss the specifics of the deliberations, the BRAC process is based upon public law, and the Services are responding to military-value questions. The BRAC process includes measuring the capacity we have across the Services in specific capability areas — C4ISR in my case.

"… Over the past year, FORCEnet has begun to develop its true meaning. FORCEnet is really the standards and architectures that allow all of these individual programs to work together."

Right now, each of the Services and we at SPAWAR are responding to a set of military value-based questions. We want to quantify attributes that constitute military value and decide what critical elements the Navy and the other Services will need over the next 20 years. The process will continue throughout the year, and then some time early next year each of these subgroups will work through their Office of the Secretary of Defense-led working groups and submit proposals that will eventually go to the Secretary of Defense.

The difference in this BRAC compared to the ones in the 1990s is that this round is being driven from the OSD level. Secretary of Defense Donald Rumsfeld really wants joint solutions, and while the Services are submitting their inputs, this year the process is being driven from the joint/OSD perspective.

It's an interesting process and I don't know what's going to come from it. What's also interesting is reading in newspapers and magazines what decisions are being made, because I'm on the inside and most of the articles and their conclusions aren't accurate.

CHIPS: So you're looking more at capabilities across DoD rather than specific billets or organizations?

Rear Adm. Sharp: We're looking at capabilities, but also examining capabilities-based acquisition. You can talk capabilities, but when you install it on a ship — it's still boxes and wires. You have to examine both. With BRAC, you can start with capabilities, but in the end it's still about facilities and people, and that's what makes it hard.

CHIPS: You mentioned how your roles complemented each other. How does your role as ASN (RDA) Chief Engineer complement your role as SPAWAR Vice Commander?

Rear Adm. Sharp: I'm located in Washington D.C., to represent SPAWAR at the Pentagon, the other systems commands and Services. This helps me, and I believe it helps SPAWAR stay aligned. One of the things I'm most proud of is as a motivator in the alignment we're seeing with FORCEnet and NAVSEA's open architecture. This has been very successful in opening up avenues and moving toward a true alignment and a single document that not only covers the communications, command and control architectures that SPAWAR is working on but also the weapons information and management systems that NAVSEA is working on.

CHIPS: Can you talk more about your Chief Engineer role and organization?

Rear Adm. Sharp: We've developed a good skill-set in managing architectures. Anytime you put together an architecture across the Navy — NAVSEA, SPAWAR and NAVAIR — or jointly, you might get some local influence. Each systems command or Service wants to skew it toward their view. The RDA Chief Engineer has always been looked at as an honest broker. When we're involved with an architecture, it allows us to determine what's best for the Navy — and not necessarily what's best for an individual systems command.

On the capability-based acquisition side, we have a group called Large Scale Systems Engineering. One of the challenges we have, particularly in the C4ISR area, is how to build systems of systems, and this gets back to capability-based acquisition. A system is set up to fulfill a specific requirement. For example, there is a requirement for a specific radio in a specific spectrum that can talk to specific people. The program manager could do a perfect job designing the radio under the requirements. But then the radio doesn't work when you try to use it outside a specific architecture. There are interoperability issues because it wasn't built to talk to other people.

When you put a lot of these systems on a ship, for example, you can have some big problems. So through the LSSE, which is really a small group of people leveraging a large group of people in NAVSEA, NAVAIR and SPAWAR, we're getting people to see that we should be designing systems for the greater good, which may mean that we suboptimize a certain piece.

For configuration management, the Navy started what's called the common systems function list (CSFL). How do you build systems across the Navy and joint communities when each Service has a different language for different functions? CSFL will create a dialect and a set of functions that we'll all use. We've gone to Joint Forces Command to create a joint common systems function list. Our job is to manage it, once again as an honest broker, to ensure there's some configuration control and to ensure we're all working from the same sheet of music.

CHIPS: What are the major Navy, OSD and joint programs you're involved with?

Rear Adm. Sharp: This kind of crosses all three so I won't try to categorize this: JBMC2 (Joint Battle Management Command and Control), JTRS (Joint Tactical Radio System), most recently JCC (Joint Command and Control), which is supposed to replace the GCCS (Global Command and Control System) family of systems. I've been involved in the next generation, joint tactical radio version of MIDS (Multifunctional Information Distribution System). I'm mostly involved with joint programs. This is really the way ahead because it's critical for the joint programs to stay on track and deliver as we all start planning from a budget standpoint to transition.

On the DASN side, I've gotten into the business process, DMIRS (Defense Military Integrated Resource System), NSIPS (Navy Standard Integrated Personnel System), TMIP (Theater Medical Information Program), which brings medical technology to our ships at sea.

"The RDA Chief Engineer has always been looked at as an honest broker … it allows us to determine what's best for the Navy — and not necessarily what's best for an individual systems command."

Above: Rear Adm. Mike Sharp at SPAWAR headquarters July 28, 2004, during the interview with CHIPS.

*CHIPS: SPAWAR has been working hard to develop the architecture and standards for FORCEnet. How do you evaluate the support FORCEnet has from Navy leader*ship?

Rear Adm. Sharp: Support has been tremendous — starting with the Chief of Naval Operations and Sea Power 21. You get a tremendous amount of alignment when the CEO of any company stands up and says, 'This is what we're going to do.' Since then the message has stuck, and FORCEnet has become part of our language. And over the past year, FORCEnet has begun to develop its true meaning. FORCEnet is really the standards and architectures that allow all of these individual programs to work together.

Let's say you want to shoot missiles from a surface ship in a littoral environment. You want them shot beyond the horizon of what the surface ship can control because there are mountains in the way. You will need the missile to be targeted by an aircraft or satellite, someone else to control that missile in-flight. There are a number of operational concepts out there that we can't quite do yet because the systems on these platforms weren't built that way. When a missile is built, it should have a standard set of communications links and radar capabilities so it can interoperate across different platforms and the different Services.

It's complex because you're talking about bits and bytes of software, radio frequencies, protocols and a litany of technical items. But that's what FORCEnet will allow us to do. It's a discipline where requirements will be written to build systems that fit into this larger architecture that will allow us to get to capability-based acquisition. That's what FORCEnet is.

CHIPS: How can SPAWAR improve the understanding of those who may not know what FORCEnet is?

Rear Adm. Sharp: We have a set of maturing documents that examine the architecture and standards. We create documents that go out to industry partners and the other Services. Senior SPAWAR folks also get out every time we can to talk about FORCEnet. This goes back to the support we receive from leadership. My boss on the acquisition side, Secretary Young, chaired two FORCEnet executive committees that have brought together key representatives from resources, fleet and acquisition.

FORCEnet will only succeed if the acquisition folks — from Secretary Young to the PEOs to the program managers — are onboard because it will require changing what the programs are doing. We're trying to do this incrementally so we don't break the bank, but getting the acquisition core onboard is critical to the success of FORCEnet.

CHIPS: How do you gather the requirements for FORCEnet?

Rear Adm. Sharp: SPAWAR's development of the FORCEnet Implementation Baseline is a great example. On the acquisition side, we start with the requirements that the Navy or Joint Forces Command gives us. Then we look at the systems that are being built and figure out which ones can evolve to meet those requirements. Those are the systems we want to nurture and revise as necessary to become part of FORCEnet.

We also look at legacy systems that will never be part of FORCEnet, even though they may be providing critical capabilities to our forces today. We want to retire them as soon as we can and replace them with FORCEnet-capable systems.

CHIPS: How do you stay close to the fleet and joint operations in gathering these requirements?

Rear Adm. Sharp: We have a lot of people in Norfolk who work intimately with NETWARCOM (Naval Network and Warfare Command), which is the voice of the fleet for C4I and the N6 for Fleet Forces Command. We have full-time people at NETWARCOM who make sure what we're doing fits in with the way ahead. We also have people proactively working with Joint Forces Command to ensure that the architectures we create are in line right from the beginning.

CHIPS: How do you work with the platform PEOs in gathering requirements and coordinating initiatives?

Rear Adm. Sharp: There are a number of challenges, but we're working more closely with the platform PEOs than ever before precisely because of these challenges. A platform requirement document can be very difficult to interpret – six UHF radios, three EHF radios, etc. Everything is in boxes because for space purposes that's how a ship is designed. Capabilities-based acquisition is key, but you need to know boxes, wires, connectors and how they all fit together when it comes to installing things on ships.

We're trying to influence the requirements process so the focus is less on boxes and more on required bandwidth, for example. Capability is very important, but it creates uncertainty in the shipbuilding process. How can shipbuilders bid something

"FORCEnet is more than a bumper sticker. It's the concept of interoperable and more capable systems that will allow our operators to be able to talk with whomever they need to at any time."

when they don't know exactly what is going into the space? So that continues to be a challenge we're working out with the platform PEOs.

Another challenge is the rapidly changing nature of information technology and communications, which is why I like this business. This creates uncertainty for a shipbuilder though, because it can increase cost. Every time a ship — it doesn't matter what kind — overruns cost it makes newspaper headlines and makes things difficult. So we're working on providing the right capability for the ship and at the same time minimizing the uncertainty for the shipbuilder. I've had meetings with both Dennis Bauman, PEO C4I and Space and Rear Admiral Charles Hamilton, PEO Ships, and we're doing very well in trying to resolve some of these issues.

CHIPS: Do you see continued support for FORCEnet in the future?

Rear Adm. Sharp: Absolutely. FORCEnet is more than a bumper sticker. It's the concept of interoperable and more capable systems that will allow our operators to be able to talk with whomever they need to at any time.

CHIPS: The Virtual SYSCOM was created to find common tasks among the systems commands, to reduce duplication and to create efficiency. How do you evaluate its progress and where it's going in the future?

Rear Adm. Sharp: I think we're going to find the Virtual SYSCOM to be a tremendous success story because developing common processes across the Sea Enterprise effort will reduce the cost of doing business. It's proven to be a significant arena for vetting some of the issues between the SYSCOMs, which have traditionally been the technical authority, and the PEOs, which are the builders of products. Rear Admiral Kenneth Slaght's work as the FORCEnet Chief Engineer across the Virtual SYSCOMs has been very successful.

We want to make sure the C4I products developed by NAVAIR and NAVSEA are built to an architecture that we all can use but not duplicated. The Virtual SYSCOM has matured considerably since it first started, and I believe it will be the way we implement FORCEnet and solve other challenges.

CHIPS: You have a lot of experience in the submarine community. Do you miss it?

Rear Adm. Sharp: Absolutely. The submarine force is unique because it's a collection of relatively small ships with relatively small crews. You establish a tremendous camaraderie with that community, but I'm also very happy that I chose to go into the acquisition community at the end of my command tour.

Rear Adm. Michael A. Sharp

Rear Adm. Michael A. Sharp is Vice Commander of the Space and Naval Warfare Systems Command. As Vice Commander, he is responsible for development, acquisition and life cycle management of command, control, communications, computers, intelligence, surveillance and reconnaissance systems for the Navy and select Marine Corps and joint service programs.

In May 2003, Rear Adm. Sharp was designated Chief Engineer for the Assistant Secretary of the Navy, Research, Development and Acquisition as an additional duty. In February 2004, Secretary Young appointed Rear Adm. Sharp to be acting Deputy Assistant Secretary of the Navy, C4I/Space as another additional duty.

Previously as the SPAWAR Chief Engineer, he reported as the Program Executive Officer for Mine and Undersea Warfare in Washington, D.C. In December 2002, the Chief of Naval Operations announced his assignment as the SPAWAR Vice Commander.

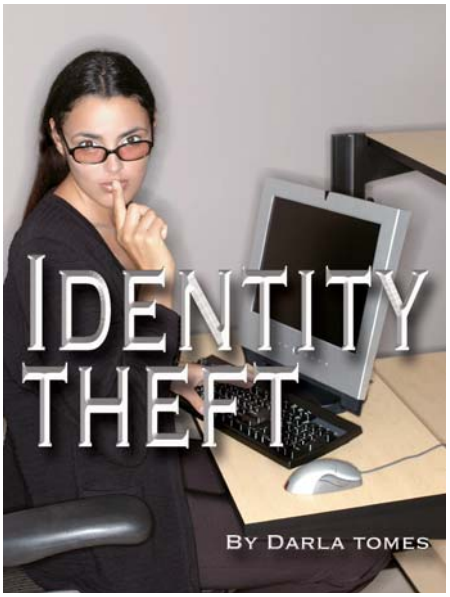
Rear Adm. Sharp was designated as an Acquisition Professional and attended the Defense Systems Management College Intermediate Acquisition Course prior to reporting to the USS Seawolf Combat System Program Manager as Assistant Program Manager for Operability. Other shore duty assignments have included: AN/BQG-5 Wide Aperture Array Program Manager and Seawolf Ship Control System Program Manager. He also served as the Deputy, Direct Reporting Program Manager (Advanced Technology) and the Advanced Tactical Data Links Program Manager (PMW 159). Following these duties, Sharp then served as the Submarine Communications Program Manager (PMW 173).

Rear Adm. Sharp reported as commanding officer of USS San Francisco (SSN 711) completing an extended Western Pacific deployment. He also served as executive officer of USS Swordfish (SSN 579).

Rear Adm. Sharp is entitled to wear the Legion of Merit with one Gold star, the Meritorious Service Medal with three Gold Stars, the Navy Commendation Medal with two Gold Stars and the Navy Achievement Medal with two Gold Stars.

Rear Adm. Sharp graduated from Oregon State University with a Bachelor of Science degree in chemical engineering in 1974. He earned a Master of Science degree in systems management from the University of Southern California in 1981 and is a 1999 graduate of the Advanced Management Program from the Harvard Business School.

For more information about the role of the ASN (RDA) Chief Engineer go to https://asnrdacheng.navy.mil/. For more information about SPAWAR go to http://www.spawar.navy.mil/. CHIPS



Identity theft occurs when a person illegally obtains another person's name; Social Security Number; bank or credit card account number; or other identifying information and uses it to commit fraud or another crime. Among other things, the criminal can use this information to set up credit card and bank accounts, take out loans and counterfeit checks. This serious crime can cost victims considerable time and expense to resolve.

The Federal Trade Commission (FTC) report on National and State Trends in Fraud & Identity Theft January – December 2003 says the FTC received over 500,000 consumer fraud and identity theft complaints. It should be noted that this number just represents the *reported* number of incidents. The September 2003 FTC Identity Theft Survey report concluded that approximately 9.91 million Americans were victims of some form of identity theft in 2003. The study also estimated the financial cost to victims at $5 billion, and the total hours victims spent resolving the theft at 297 million.

Department of the Navy (DON) personnel are not at higher risk than the average American for having their identities stolen. But the DON is taking steps to further protect the identities of Navy personnel. Section 208 of the E-Government Act of 2002 requires that all federal agencies perform Privacy Impact Assessments (PIAs) on their information systems. This requirement is for identifying only the privacy impact on the public, not the federal employee. Going a step further than the Act requires, the DON is conducting PIAs on information systems to identify the privacy impact on civilian and military personnel.

Public Key Infrastructure (PKI) is used to securely authenticate a user's identification to networks and Web sites that may contain personal identifying information. It can also allow digitally signed electronic transactions and encrypt information. The combination of the Common Access Card (CAC), PKI certificates stored on the CAC, the individual's CAC Personal Identification Number (PIN), and Public Key enabled networks and Web sites, is a more secure method for authentication to networks and Web sites than user ID and password, which can easily be compromised by someone with criminal intentions.

Using PKI to digitally sign electronic transactions guarantees that the initiator of the transaction cannot later deny having initiated the transaction, and ensures that the information was not changed. Using PKI to encrypt e-mails that may contain personal identifying information protects information at the desktop and in transit.

The Department of Defense (DoD) formed the Identity Protection and Management Senior Coordinating Group (IPMSCG), chaired by the DON Chief Information Officer (CIO), Dave Wennergren. This group rolls the work of the smart card, biometric and PKI steering groups into one group. The IPMSG is looking for new ways to further protect the identities of DON personnel.

The DON has taken steps to protect employees' personal information in its information systems, but the Department also encourages personnel to be proactive in protecting their information. Below are some precautions to take to help protect your identity from being stolen.

Personal Security Tips
√ Call the organization handling your account and follow up with a letter if you suspect someone is illegally using your identity or making charges in your name.
√ Shred all credit card, bank and other financial statements for disposal.
√ Order your credit report once a year and look for any anomalies. Title II of Public Law Number 108-159, The Fair and Accurate Credit Transactions Act of 2003, requires certain nationwide consumer reporting agencies to furnish free credit reports upon consumer request once during any 12-month period.
√ Be wary of anyone calling or sending you an e-mail, also known as "phishing," to "confirm" personal information. Phishing is a tactic that uses spam e-mail to trick consumers into disclosing sensitive personal information such as passwords, credit card and bank account numbers.
√ Review all bank, credit card and phone statements for unusual activity and report problems to appropriate authority immediately.
√ Properly dispose of ATM receipts.
√ Monitor when new credit cards, checks or ATM cards are being mailed to you and report any that are missing or late.
√ Close all unused credit/bank accounts, destroy old credit cards and shred unused credit card, insurance or subscription offers.
√ Ask for the carbon copies of credit card receipts.
√ Use secure Web sites for Internet purchases.
√ Never use any easily recognizable information, such as your date of birth or mother's maiden name as a password for ATMs or access to Web sites.
√ Do not discuss financial matters on wireless phones.
√ Do not leave credit card payments in your mailbox.
√ Do not place your Social Security Number on checks.

For more information regarding identity theft, please refer to guidance published by the FTC at http://www.consumer.gov/idtheft/. Darla Tomes is on the DON CIO Information Assurance Team. CHIPS

Interview with Robert J. Carey
DON Deputy CIO

Mr. Robert J. Carey serves as the Department of the Navy Deputy Chief Information Officer for Policy and Integration. Reporting directly to the DON CIO, he is the principal adviser to the CIO. Mr. Carey is responsible for managing and leading the DON CIO staff and developing strategies for achieving information management/ information technology (IM/IT) enterprise integration across the DON.

CHIPS: What is the DON Information Management/Information Technology (IM/IT) Strategic Plan 2004-2005? Why is it important, and who should read it?

Mr. Carey: The importance of the plan can't be understated because it lays out the high level roadmap as to where the Navy and the Marine Corps will be going in the broad context of information technology.

Navy and Marine Corps Deputy CIOs contributed heavily to the plan, and careful attention was paid to ensure the goals and objectives of the plan support the Department's larger vision for the warfighting capability of the future. So the goals and objectives in the plan are aligned with our warfighting capabilities documents like Naval Power 21, Marine Corps Strategy 21 and Joint Vision 2020.

We linked these documents to the IM/IT Strategic Plan so it is clear that IM/IT is an integral enabler of every Naval program and initiative. So, for example, if you are in logistics, aviation or a Marine on the ground, the DON IM/IT Strategic Plan will help you understand the IM/IT capabilities the Department is building that will help you do your job.

The plan is also aligned with DoD's IT plans and with the suite of legislative statutes and the Office of Management and Budget (OMB) guidance that govern IM/IT. It is not an execution plan; it doesn't go down to the program level. But it is something that everyone in the Department's IT workforce should read to gain a fundamental understanding of the types of things the Department as an Enterprise is trying to accomplish. Because this is where we should be shaping investments tied to corporate management and functional objectives.

The next step is to strengthen the tie between the IT capabilities in the strategic plan, IT programs and investment decision making, and we are working with the Navy and Marine Corps to improve this linkage.

CHIPS: The list of DON IM/IT initiatives is extensive, how does the DON CIO prioritize these programs in order of importance?

Mr. Carey: Yes, the list is long. Because of the way programs are funded, we are not at a place yet where we can say: 'Let's fund ATMs-at-Sea but not Enterprise Resource Planning.' Our greatest opportunity to influence IT investment decision making, lies in strengthening the alignment of claimant IT programs with the Department's vision for the Enterprise, and we are making tremendous progress. In the past, our major opportunity to influence the IT budget was just prior to its submission, but we now

Robert J. Carey

Prior to his position as DON Deputy CIO, Mr. Carey served as the DON CIO eBusiness team leader from February 2000 through June 2003 and Director of the DON Smart Card Office from February through September 2001.

Carey began his career with the Department of the Army in October 1982 at the Aberdeen Proving Ground, Md., where he was a test director managing developmental and operational testing of small arms and automatic weapons. In February 1985, Carey went to the Naval Sea Systems Command assigned to the Surface Ship Sonar Dome Program Office, managing the Rubber Keel Dome project. Over the next five years he held various positions in the Undersea Warfare Directorate such as the AN/SQS-53C Sonar Project engineer and director of the Surface Ship Sonar Dome Program Office. Following his return from active duty in Operation Desert Shield/Storm, he was a senior systems engineer on the staff of the Program Executive Office for Surface ASW Systems.

From January 1995 through August 1998, Carey worked in undersea weapons systems engineering, culminating in a tour as the chief engineer in the new Undersea Weapons Program Office, PMS 404 where he managed systems engineering efforts for all Navy torpedo programs. In August 1998, he served as Deputy Program Manager for PMS 404 where he managed nine ASW weapons programs including Foreign Military Sales.

Carey has a Bachelor of Science degree in engineering from the University of South Carolina and a Master of Engineering Management degree from George Washington University. Mr. Carey has been awarded the Navy Civilian Meritorious Service Award and the Navy Superior Civilian Service Award.

He is a Commander, Civil Engineer Corps in the U.S. Naval Reserve serving as a Contingency Engineer for the U.S. European Command.

can influence the budget throughout the Planning, Programming, Budgeting, and Execution (PPBE) process by releasing policy and guidance documents at strategic points throughout the PPBE cycle.

For instance, during the last budget review cycle we issued DON CIO IT Policy Guidance for FY 2004 Expenditures in coordination with the Assistant Secretary of the Navy (Financial Management and Comptroller (ASN (FM&C)). This guidance tied programs' authorization to expend funds to specific national, DoD and DON IT policies and made every organization's comptroller office responsible for enforcement. Similar guidance for FY 2005 will help make sure that commands are working on things that are aligned with the Department's IM/IT strategy. Another example of progress in this area, is the continuing work by the DON's Functional Area Managers (FAMS) to rationalize and consolidate the DON's software portfolio.

Dave Wennergren, the DON CIO, co-chairs the FAM Council with Vice Admiral Albert Church, Director, Navy Staff. Together they help shape the guidelines about how applications are going to be examined, measured and renewed. Programs that are not meeting the goals and objectives that the Department has laid out can be modified. The Clinger-Cohen Act also helps shape the level of initiatives.

As acquisition programs come up for milestone decisions, Clinger-Cohen requires agency CIOs to review them for security and architectural compliance. As we move into net-centricity all of these programs and their applications and databases must work together. Requirements for security, interoperability, authoritative databases, collaborative environments, and efficient use of limited resources demand that agencies shift away from the traditional paradigm of decentralized IT decision making to Enterprise solutions.

CHIPS: What are some of the DON IM/IT capabilities that the DON CIO has fostered?

Mr. Carey: There are quite a few; I'll give you a short list, for example, cryptographic logon. We are the champions of smart card technology with Common Access Cards (CAC) in the Department. Since last summer, the DON CIO staff has been logging on to NMCI workstations with the CAC card. This eliminates the need to remember passwords. One of the benefits of the smart card is the ability to log on to the network securely using your PKI (Public Key Infrastructure) credentials contained on your CAC card. Once fielded, the Navy Marine Corps Portal will be your window to the world, and your CAC will be the key that authenticates your identity to the portal, giving you access to all of the applications that you need to do your job.

Another initiative is Internet Protocol version 6. IPv6 is the next state of the Internet Protocol, and it is going to require a fair amount of change. Internet use has exploded, but the number of IP addresses on the current IP is finite. IPv6 will help us deal with the exponential growth of the Internet. As we move to network-centric warfare and Web services, using the current IP, our servers, routers, PCs and Web sites would have addressing issues. In a policy memorandum, the DoD CIO mandated the transition to IPv6 by FY 2008. Transition is a few years off, but it is a strategic initiative that the DON CIO is working with the DoD CIO and the Defense Information Systems Agency (DISA).

Voice over IP (VoIP) is an exciting technology with huge opportunities to explore. The Naval Sea Systems Command (NAVSEA) has already implemented a VoIP network-based telephone system. This technology has wide application across the Department. We will do a business case analysis to determine the best application for VoIP; and we are championing the examination of VoIP as part of a greater telephony strategy, so that we understand its integration with the "plain old telephone system," commonly known as POTS, and with wireless devices like cell phones and Blackberries. We are examining where it makes sense to distribute converged devices like Blackberries, other PDAs and cell phones for people to do their jobs.

We are working with the Navy and Marine Corps to develop an Enterprise portal capability. This is something we must have to provide a common framework for information sharing across the Department. When you log on to the NMCI and you click on the Internet icon, you will be on the Navy Marine Corps Portal. It will provide access not only to your applications but also options like chat rooms, a global directory and other information that you will need. Underlying this simple concept is a lot of work — singling out databases, applications and access paths — to provide seamless, near real-time access to the authoritative data and intellectual capital of the Department.

Other portals will become aligned with the Navy Marine Corps Portal so we can share content across the Enterprise. Ultimately, we look to commands to stop spending precious resources on the latest greatest portal; and focus instead on delivering the quality, authoritative content, they need to share. We want commands to be spreading knowledge and creating knowledge warriors on the pointy end of the sword — from Iraq to the Naval Medical Center in Bethesda.

We are also working on XML naming conventions. XML is quickly becoming the cornerstone between legacy applications, data and Web services. We have created taxonomies within XML that allow people to identify, tag and create naming conventions so that the word 'ship' means the same thing every time you see it. XML is critical for moving to net-centricity, enterprise-wide services, authoritative data and knowledge on demand.

I have touched on just a few of the Navy's IM/IT transformation initiatives. I encourage all of our readers to go to the DON CIO Web site at http://www.doncio.navy.mil and read the Department's IM/IT agenda — the DON IM/IT Strategic Plan.

CHIPS: Getting back to IPv6, is DoD waiting for industry's lead to make the leap to IPv6?

Mr. Carey: Today, industry and DoD are both moving toward the IPv6 standard. The ideal would be that industry would work the issues, and we would adopt them as soon they were done. Currently, this does not appear to be the case. DoD has made a

serious commitment to transition to IPv6. Our goal, defined by John Stenbit, former ASD (NII)/DoD CIO, is that we will have this capability by 2008. We are working toward this. DISA and the other Services are working on this. We have guidance that says we will buy devices that are IPv6 capable so that when the time comes to make the shift our devices can be used. In some ways DoD is leading industry because we foresee the real need to move to IPv6, and have taken positive steps to get there.

CHIPS: Do you think commands will need to make a significant investment to transition to IPv6, similar to the Y2K bug issue?

Mr. Carey: No. I foresee, if this is done correctly, that as you normally refresh your technology, hardware and software, whether you upgrade or buy new — you will have a device or application that is IPv6 capable. So you will eliminate the need for a stand-alone investment to bring your technology up to the IPv6 standard. I think some people have fears that there is a huge bill associated with this transition. The cost will be affordable when you consider that you are going to do a tech refresh anyway.

CHIPS: How does the DON CIO work with the other Service CIOs to ensure that solutions aren't duplicated but interoperable?

Mr. Carey: David Wennergren and I have a very close working relationship with the other military Department CIOs and their staffs. When one of us finds a victory we are very quick to share. We meet with the Deputy Assistant Secretary of Defense (Deputy Chief Information Officer), Priscilla Guthrie, on a biweekly basis.

The purpose of these meetings is to understand from the DoD perspective where we need to be going and what we need to be sharing. One example of an interoperable solution produced by the DON CIO is the OMB Exhibit 300, Capital Asset Plan and Business Case tool. The Exhibit 300 is a lengthy 25 to 50-page report on all major IT systems that everyone in DoD has to complete. The tool we created helps a program manager better understand what OMB is looking for in the content of the various sections of the 300 exhibit and how OMB would score an answer. DON IT programs realized significant improvements in OMB scores since we began using the tool.

The Army was so impressed that it has adopted our work as a best practice and used the tool to prepare its reports for the last two years — a huge payoff in terms of not duplicating something that was already done.

We participate on the DoD Executive Board and other boards in the federal government like the Federal CIO Council. We work to share our best practices not only with the other Services but also throughout government. We all know that we don't have the resources to recreate solutions so that if the Army, Air Force or another government agency has built a best practice on something — we will use it.

CHPS: Does the DON CIO have a role to play in Homeland Security?

Mr. Carey: Absolutely. We have a huge role to play. Since before the Department of Homeland Security stand up, we have been managing the DON Critical Infrastructure Protection program and Dave Wennergren has been the Department's Critical Infrastructure Assurance Officer (CIAO) reporting to OSD. Dave is the link to the DHS CIO in terms of how vulnerable the DON IT infrastructure is in regard to homeland security.

We conduct NIVAs, Naval Integrated Vulnerability Assessments, and look at an integrated view of the parameters of a Naval base, the force protection plan, its dependencies on public utilities that come from outside the fence, network defense and its overall posture to understand where the weaknesses are. We have conducted NIVAs at Navy Region Southwest; Southeast; Oahu, Hawaii … and we get an understanding of the relationship between the local government services and the Naval installation.

We integrate the cyber view with the force protection view and assess the base's reliance on commercial infrastructures and services outside the fence to get an integrated sense of what local commanders should be concerned about to assure mission readiness. For example, if there were a building that housed the Internet connections for the entire base 50 yards from the fence line, wouldn't you want to know that it wasn't the best location for a building with the vital Internet connection for the whole base?

We have a NIVA team going to Italy this October to look at the support activities in Naples and Gaeta. When we did a NIVA in Hampton Roads, the commonwealth of Virginia engaged the DON CIP team to better understand what it could be doing to improve its security posture.

With this information an organization can decide if it needs to improve so that in the event of a terrorist attack or disaster such as hurricane (because a hurricane can cause as much damage as a terrorist attack), it is prepared. We look at how Navy assets can work with public services to get back in business.

CHIPS: Would the DON CIO be able to conduct a NIVA for any state?

Mr. Carey: Yes, any state with a significant Navy presence. We have been asked by several members of Congress to work with Naval installations. The Hawaii Congressional delegation wanted us to help them help themselves because they realize how heavily dependent Hawaii is on the Navy. The South Carolina Congressional delegation understood what we had done in Hawaii and other states, and asked us to study the bases and report any of the issues we found so they could prepare in case of an attack or natural disaster.

CHIPS: Sandra Smith's CHIPS articles on the IM/IT workforce always draw a lot of reader interest. What message do you have for the military and civilian IM/IT workforce?

Mr. Carey: My message is that the world is changing — and that is not news to anyone in the IM/IT workforce — uniform or civilian. The CNO, Admiral Vern Clark is developing a human capital strategy for the entire Department. He is working with Secretary England to determine how we are going to best use the people that we have, and the IM/IT workforce is a component of the strategy.

We examine the skill sets the workforce has, what they are used for, what skills we need, whether there is a path for growth, what career path should be followed — these are things Sandy is working on to ensure that the IT workforce is viable and properly skilled to meet current and future needs. We also look at where technology is going and what training is required to attain the certifications the workforce will need to have a certain level of competency and credibility as technology and job requirements change.

The acquisition community has done a fabulous job of laying out certification levels, training curricula and requirements. To a large extent the IT workforce has done this, but we need to go a bit further in defining accreditations and certifications that allow workers to build a pedigree and compete for different jobs — jobs that will make great use of these skills sets.

CHIPS: I am still surprised by the number of people who think that the NMCI is just for secure e-mail. What are some of the capabilities that will be populating the NMCI once cutover is completed?

Mr. Carey: Currently, there are about 200,000 users with the authority to deploy up to 360,000. To think that this is only an e-mail system is a misnomer. NMCI is the highway system for information sharing in the Department. It is an enterprise asset spanning the Navy and Marine Corps. NMCI is the fundamental underpinning of how we intend to use IT to execute the Department's mission.

The NMCI is one of the most secure networks in the world. It has dealt with a few viruses recently in as little as a couple hours where industry experienced loss of service. With NMCI we can deal with security in a uniform and consistent manner across the Department. Spending is now controlled. It has also provided a performance measurement mechanism for IT where we didn't have one before. The ASN (FM&C) is very excited about the NMCI because the IT budget is over $6 billion and prior to NMCI no one could accurately say how much the Department was spending on desktop IT or information services.

The NMCI gives the Department an enterprise portal. We can't have an enterprise portal without an enterprise network. With NMCI we have integrity and consistency of information deployed across the Department. We can have authoritative databases and file sharing access. NMCI provides the ability to have enclaves, for example, the Naval Nuclear Propulsion community of interest. They have information that is not germane to the rest of the Navy. However, it will be on the NMCI on their portion of the network. So they are on the NMCI, but they are able to keep information secure within their community. This is unclassified information, but it is information only they need to know.

Another consideration is that we can control the desktop — we can have the same Gold Disk set of applications running on everyone's desktop, which makes technology updates easier. Completing the NMCI hasn't gone as quickly as we would have liked, but when it is complete it will be the largest intranet in the world.

Looking to emerging technology, NMCI allows us to consider whether we want to leverage this huge network to convert commands to VoIP. So we don't have to pay a public telephone service or long distance carrier, we can use our own network. I don't know to what extent we will do this, but NMCI gives us the flexibility to consider it. Cisco uses VoIP in all its facilities worldwide, but outside its facilities, Cisco uses another vendor's connections to carry cell phone signals back to the office. Because of the Navy's desire for security, we could use DISA pipes or pipes provided by a vendor with the required security, but if we choose we could use the NMCI.

We will have to start recognizing and rewarding people for not building their own mousetraps, but for finding the best one already being used and adopting it instead.

CHIPS: What does Enterprise IT in the Department really mean?

Mr. Carey: When Dave Wennergren and I talk about the Enterprise we open our presentation with three pictures of an enterprise: the Navy aircraft carrier, the USS Enterprise (CVN 65); the *Star Trek* Starship Enterprise and the Space Shuttle Enterprise. The point is that it really depends on who is the audience, doesn't it? If you are at the Department level like I am, I view the Enterprise as the Navy/Marine Corps team — all 1 million of us. If I am in the Navy, I view it probably as the blue side, and if I am in the Marine Corps, I would probably view it as the green side. None of these are wrong.

In the past, IT in the Department has been very much decentralized in how it is managed. However, we have learned that it makes sense to centralize IT. As we move toward more Enterprise activity, more centralization, we will have more and improved efficiency. Let's talk about the ESI, for example, the Enterprise Software Initiatives licensing agreements. This is where I can best maximize the buying power of the Department by maximizing the customer base at the DON level. My definition of enterprise is looking at the greater good where it is appropriate. You would look at the greatest application or expansion until it doesn't make sense anymore. This is a concept that is foreign to most of us.

That is why Enterprise IT may be hard words to swallow if you were a NAVSEA program manager, which I was, and you were paid to solve a program problem. When you defined the problem within the enterprise of NAVSEA, things got really hard and if you defined the enterprise as the Navy, things got an order of magnitude harder. If you defined it in terms of the Department, your eyes probably crossed — it was just too hard. We need to understand which problems really call for solutions at the DoD or the DON Enterprise level and how to recognize when a federation of multiple solutions might make more sense.

And we need to put reward mechanisms in place that recognize folks who are solving issues on behalf of the Enterprise. There is a fundamental change in culture and mindset that must take place as we move into the work of NCW and Enterprise services. We will have to start recognizing and rewarding people for not building their own mousetraps, but for finding the best one already being used and adopting it instead. CHIPS

DoD ESI's Successful New Approach for Enterprise Resource Planning

By Chris Panaro

The Enterprise Software Initiative

The Department of Defense (DoD) Enterprise Software Initiative (ESI) is a joint Defense Department project to leverage the buying power of the DoD for commercial information technology products and services. By consolidating requirements and negotiating Enterprise Agreements with vendors, the DoD realizes significant Total Cost of Ownership (TCO) savings in services, software acquisition and maintenance. The ESI goal is to develop and implement a DoD-wide process to identify, acquire, distribute and manage enterprise information technology (IT) assets.

In the next five years, it is estimated that DoD will invest over $12 billion on commercial-off-the shelf (COTS) software and related services to automate business systems and operations. Considering that the 2004 Standish Group Chaos Report estimates that over 70 percent of IT projects are late, over budget or fail, the focus on best practices in the acquisition and implementation of these software applications is critical.

With the mandate of the Clinger-Cohen Act to "develop and use best practices in the acquisition of information technology," the DoD has become a leader in leveraging buying power and implementing best practices in program management.

In late 2001, the DoD Logistics Domain made a significant commitment to adopt and deploy commercial best practices in the acquisition and implementation of COTS business application software. The "Log Domain" gathered program managers and experts from DoD Enterprise Resource Planning (ERP) and supply chain programs to form the Program Implementation Group (affectionately termed the "PIG").

The PIG was chartered to capture and deploy best practices so that all programs will benefit from the lessons learned and overall experience of the group. The group immediately recognized the benefit of using the experience of industry representatives to gather commercial perspectives on major software implementation projects. Among the many tools it shares, the PIG developed an Enterprise Integration Toolkit (EI Toolkit), illustrated in Figure 1, to provide a roadmap, tools, templates and checklists for programs to use when embarking on a COTS IT project.

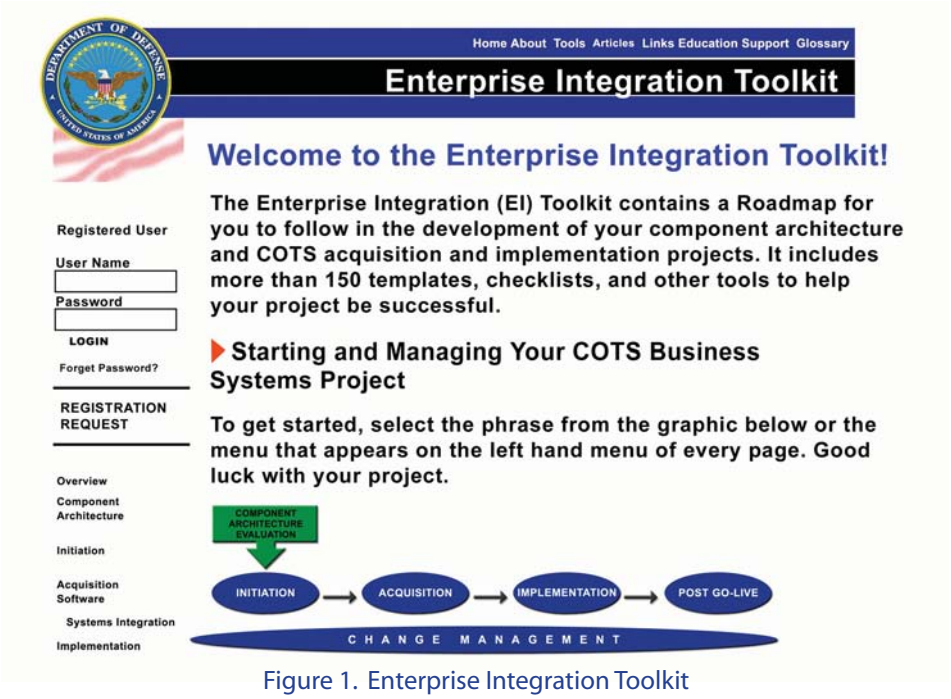


Figure 1. Enterprise Integration Toolkit

The Web-based toolkit includes sample business cases, Request for Proposals (RFPs), contracts, status reports and hundreds of other tools to use through an entire program life cycle. The EI Toolkit can be accessed by government personnel at http://www.eitoolkit.com/. Already, the toolkit has been discovered and used by other government agencies, including the California Department of Motor Vehicles, Alberta, Canada and the Australian Navy.

One immediate benefit of the toolkit is the ability to share common software objects needed to interface ERP software with other DoD systems. If an object has been developed by one program, another program can leverage that investment and use the object for its operations. This has resulted in considerable savings already since the budgeted costs of an ERP project typically allow up to 40 percent of the total cost for software objects.

Collaboration throughout DoD

With a common mission to use the buying power and expertise of the Defense Department, the ESI has been negotiating DoD-wide software license and maintenance agreements since 1998. Obtaining deep discounts off GSA Federal Supply Service prices, ESI has saved the Defense Department more than $1.5 billion by securing terms that help even the smallest program reap the benefits of DoD's cumulative buying power.

After years focused on software license and maintenance agreements, ESI joined forces with the PIG to tackle the contracts that demand the largest percentage of a COTS IT program budget — software implementation/systems integration.

In a typical commercial IT project involving COTS packaged software, $5 is spent for a systems integrator for each $1 spent on software license fees. Based on an Office

Methodology Phase → Blueprint → Pre-configured price tables in accordance with methodology

Services to be performed by contractor	Deliverable(s)	Duration	Acceptance Criteria	Payment upon Acceptance
Establish project documentation standards	Project documentation standards	2 weeks	The documented deliverable shall conform to the format and structure of the sample attached as Attachment D-4	$17,200
Determine project team training requirements	Documented team training plan	3 weeks	The documented deliverable shall conform to the format and structure of the sample attached as Attachment D-5	$15,500
Perform process and functional gap analysis and document proposed resolutions	Detailed gap analysis report including proposed resolutions	4 weeks	The documented deliverable shall conform to the format and structure of the sample attached as Attachment D-6	$42,500

Figure 2. Fixed Price Table Example

of Management and Budget (OMB) 2003 finding, the government ratio is as high as $15 to $1. ESI brought to the table its expertise in negotiating enterprise-wide purchases — and the PIG brought its collective expertise in ERP and supply chain software implementations.

Fixed-Price Services

The result of this cross-organization effort is a contractual structure that follows the phases and steps of implementation methodologies proven in more than 18,000 business systems projects. The Enterprise Agreements were awarded in May 2004 to five systems integration firms: Accenture LLP, BearingPoint, Computer Sciences Corp., Deloitte Consulting LLP and IBM. The agreements permit any DoD program to order fixed-priced services that follow a vendor's phased methodology and include descriptions of tasks, deliverables, acceptance criteria, duration and price.

The agreements provide a full range of services including: configuration; integration; installation; data conversion; training; testing; object development; interface development; business process reengineering; project management; risk management; quality assurance; and other professional services for COTS software implementations.

The concept of "commoditizing" a service so that future DoD programs can order services using a best practices contract structure and not just a menu of discounted labor rates is timely — and at the leading edge of acquisition excellence.

Developing a process in accordance with a proven implementation methodology brings discipline to scope management of COTS implementations and ties payment firmly to the achievement of desired results. Each vendor provided a fixed-price table describing services aligned to methodology for a standard project scenario, including a baseline of user quantities, modules, locations and other key factors involved in a typical ERP project. Figure 2 is an example of a fixed price table.

Where a future DoD program deviates from the standard scenario, fixed prices are provided for variances in scope (e.g., additional number of users, locations, interfaces, etc.). To accommodate these variances, a fixed-pricing menu, shown in Figure 3, was developed and reflects the extensive experience of the integration firms selected and the maturity of their respective methodologies.

In addition, contractors are required by the Enterprise Agreements to follow procedures to ensure that the government is not paying for services or products that have been purchased in an existing DoD program using similar COTS products. Objects referred to as reports, interfaces, conversions, extensions (RICE) permit the reuse of technology assets and eliminate redundant purchases. This practice is enforced by the Enterprise Agreements and is expected to result in considerable savings. RICE objects are priced as commodities in the Enterprise Agreements. Figure 4 shows an example of a commoditized RICE pricing table for software objects.

Performance-Based Payment

The ESI and PIG joint effort focused on contracting practices that reward contractors for achieving stated government objectives — not just for time and effort spent.

The Enterprise Agreement process incorporates a performance-based approach to tie contract payments to the achievement of an organization's goals and objectives. The Enterprise Agreements incorporate an incentive structure using baseline variables, acceptance criteria, performance metrics and a payment approach.

Outcomes are defined by project, phase or deliverable to best fit the goals of the

Bold type shows the baseline scope and price for each task/deliverable

Task ID	Task/ Deliverable Name	Variability	Factor Description	Factor	Quantity	Unit Price	Project Total Price
1.1.1	**Work Plan**	**Yes**	**Number of sites or commands**	**1**	**1**	**$26,391.08**	**$26,391.08**
				3	1	$29,030.19	$29,030.19
				7	1	$31,669.30	$31,669.30

Description of the factor that causes a variable price

The variable number that determines the adjusted price

The adjusted price for the variable number of sites or commands

Figure 3. Fixed Pricing Menu Example

R.I.C.E. Pricing Table			
	Complexity		
	Low	Medium	High
Reports & Forms	$3,592.52	$6,286.91	$8,083.17
Interfaces	$3,592.52	$10,777.56	$21,555.13
Conversions	$7,668.88	$23,006.63	$46,013.27
Extensions and Workflows	$9,580.06	$29,937.68	$80,232.98

Price includes creation of technical specifications, coding, documentation and unit testing.

Figure 4. Commoditized RICE Software Object Pricing Table

customer. Figure 5 depicts one of the performance-based approaches.

The Enterprise Agreements provide flexibility in ordering based on specific scenarios. For example, the selected approach may use incentives to reward on-time performance, high customer satisfaction or quality of post-implementation support. A share-in-savings incentive is also provided to better align government and vendor interests in reaching targeted improvements in operational metrics.

The key to entering a performance-based payment structure is having a clear and objective baseline which you can measure against the desired improvement. Think of it as needing a clear understanding of your current body weight before you would pay someone to help you lose weight. Without knowing where you are (your baseline) and where you want to be (your target), performance-based payment structures are difficult to nail down.

As with all acquisition efforts, the work done early in the life cycle is crucial to an effective contract. The program team must clearly articulate the business case or financial justification for the investment being made. This gets defined in greater detail in the requirements gathering process so that a formal requirements document can be attached to the final contract. This process ensures that the contractor will provide services that satisfy the requirements or objectives set by the business sponsors.

Competition

As with all major acquisitions, it is to the buyer's advantage to solicit bids from multiple vendors. You will find that pricing can be reduced and team qualifications enhanced with the proper level of competition.

In a performance-based payment scenario, the percentage of payment that is tied to performance should be a variable that bidders compete until the highest percentage of risk is appropriately borne by the contractor.

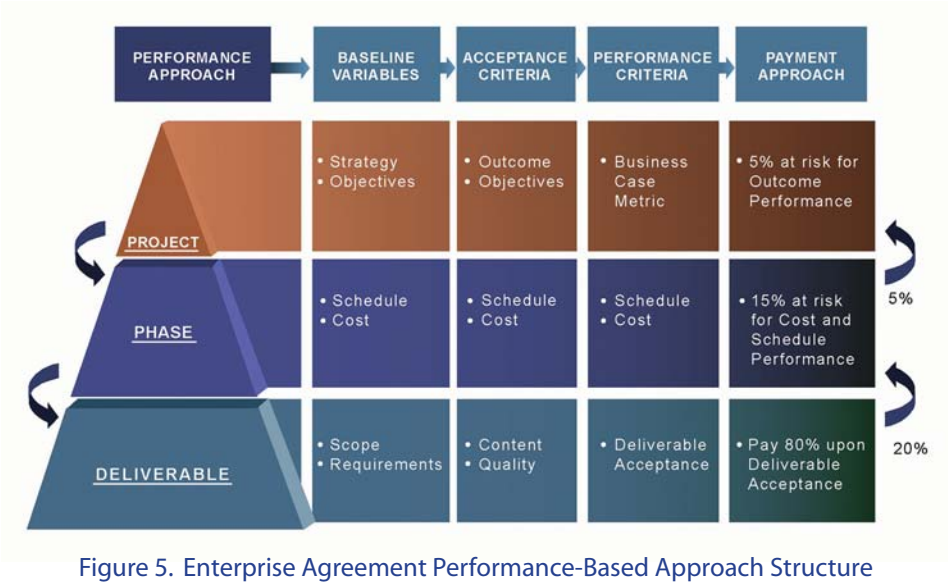


Figure 5. Enterprise Agreement Performance-Based Approach Structure

The Enterprise Agreements were solicited using the GSA Federal Supply Service and eBuy, a component of GSA Advantage. eBuy is an electronic Request for Quote (RFQ) system designed for federal buyers to prepare RFQs, directly online for a wide-range of services and products offered through the GSA Multiple Award Schedule (MAS) program. e-Buy allows RFQs and quotes to be exchanged electronically between federal buyers and Schedule contractors.

We used e-Buy to satisfy the requirements of Section 803 of the National Defense Authorization Act of 2002. These agreements were established on a competitive best-value basis as GSA Schedule Blanket Purchase Agreements (BPAs) and are available for ordering by all DoD components. Task orders must be competed among the five BPA holders in accordance with the fair opportunity provisions unless a regulatory exception applies.

Conclusion

The Enterprise Agreements are much more than negotiated discounts. They provide an in-depth knowledge base for any program about to embark on a COTS implementation. Following a disciplined methodology reduces risk, and tying payment to desired results transfers risk to a vendor that has proven technical expertise.

The Enterprise Agreements are excellent examples of government and industry working together to bring best practices to DoD programs that will be investing billions of dollars on business systems during the next five to 10 years.

The Enterprise Agreements can be accessed through the ESI Web site at the following link: http://www.don-imit.navy.mil/esi/.

Chris Panaro provides contract support to the Assistant Deputy Under Secretary of Defense (OADUSD) Logistics Systems Management. He is an adviser to the DoD ESI program.

NETCOM - THE ARMY'S TECHNOLOGY COMMAND

By Gordon Van Vleet

NETCOM Soldiers, civilians and contractors are found virtually everywhere around the globe to ensure that the Army's portion of the Global Information Grid is operational and secure.

With a mission similar to the Naval Network Warfare Command mission, the U.S. Army established the Network Enterprise Technology Command/9th Army Signal Command (NETCOM/9th ASC) in October 2002 as the sole authority to operate, manage and defend the Army's portion of the Global Information Grid (GIG).

Taking on this tremendous task, Maj. Gen. James C. Hylton assumed the position of commanding general, after serving as the commander of the Army Signal Command for 15 months. NETCOM/9th ASC is a direct reporting unit to Headquarters, Department of the Army, under the oversight of the Army's Chief Information Officer/G-6, Lt. Gen. Steven Boutelle.

Headquartered at Fort Huachuca, Ariz., NETCOM/9th ASC has a worldwide presence and mission. *"We are a global C4 (command, control, communications and computers) mission organization that supports enterprise execution of the Army's information systems mission,"* Hylton said.

With more than 14,000 Soldiers and civilians in more than 100 locations around the world, NETCOM provides direct mission support to the Army, its service component commanders and theater combatant commanders.

"NETCOM's pacing mission priority is as the Army's single authority to operate, manage and defend the Army's infostructure and network environment at the enterprise level," the general said. *"We do this by focusing on the network. The network is our central nervous system and protecting it is a key mission priority."*

The Army Signal Command formed the core of NETCOM. NETCOM retained its major force structure and its major subordinate commands deployed throughout the world. In addition, there was an extensive reorganization which created two new subordinate organizations: the Army Network Operations and Security Center (ANOSC) and the Enterprise Systems Technology Activity (ESTA).

NETCOM assumed command over three operational staff elements from the former Directorate of Information Systems for Command, Control, Communications and Computers (DISC4); the Spectrum Management Division, Office of the Chief Technology Officer; and the Information Assurance Division, all located in the Washington, D.C., area.

NETCOM is an outgrowth of the Army's information management transformation efforts. It is focused on goals three and four of the Army Knowledge Management five strategic goals: (1) Adopt a funding strategy, governance and cultural change to become a knowledge-based organization; (2) Integrate knowledge management concepts and best business practices into Army processes to improve performance; (3) Manage the infostructure as an enterprise to enhance capabilities and efficiencies; (4) Scale Army Knowledge Online (AKO) as the enterprise portal to provide universal, secure access for the entire Army; and (5) Harness human capital for the knowledge organization.

It was imperative for the Army to move toward an enterprise focus for NETCOM to achieve goals three and four. An integral part of protecting the Army network is done through NETOPS. Network Operations has emerged as a mission core competency of NETCOM's enterprise mandate.

Soldiers from the 11th and 93rd Signal Brigades set up a tropospheric scatter antenna during a sandstorm during the first days of hostilities in Iraq.

Soldiers and equipment from the 504th Signal Battlion, 11th Signal Brigade, provide communication support for the Coalition Forces Land Component Early Entry Command Post (CFLC EECP) at a former Iraqi presidential palace during Operation Iraqi Freedom (OIF).

Sgt. Gary Smith (foreground) and Spc. Jermaines Thomas of the 44th Signal Battalion, 5th Signal Command, work in a satellite communications terminal van located at Kaposvar South, Hungary, during Operation Joint Endeavor.

"We are moving from the decentralized execution approaches of the past to enterprise efforts that are focused on network-centric, knowledge-based force objectives," said Hylton. *"This is executed within a joint operational context and requires close integration across the Army, joint and governmental levels,"* said Hylton.

NETOPS is an integrated approach to systems and network management, information assurance, computer network-defense and information dissemination management.

"By enabling operational and technical capability for net-centric warfare, we get the right information to the right place at the right time, while providing the appropriate level of protection for that information. NETOPS allows us to provide information and decision superiority to the warfighter," said the general.

The nerve center for NETCOM is the Enterprise Systems Technology Activity. ESTA leads the integration of the Army's information systems environment. In doing so, ESTA creates the framework for how we execute enterprise systems management throughout the Army. ESTA's primary mission is to ensure delivery of enterprise-level information technology standards, practices and capabilities in support of the Army's information management environment.

In a move to better serve IT users, NETCOM collocated its regional offices with the regionally based Installation Management Agency regions. Under ESTA's technical oversight, the regional offices execute and enforce command, control, communications and computers for information management (C4IM) policies, standards, architectures, programs and plans for information technology issues within their assigned region.

ESTA has moved from the past systems-focused approach to a service-focused approach.

"The goal is for NETCOM, through the efforts of ESTA, to change the way the Army approaches C4 capabilities. It allows us to measure performance and determine costs. For the warfighter, we will provide a common language for IT service provisioning."

"In short, our Army customer will not have to worry about how a capability is provided. All the customer will do is request the type of service needed and NETCOM will figure out the best way to provide the needed service. We will negotiate service-level agreements that will ultimately lead to monetary savings and significant improvements in the way the Army's network users communicate," said Hylton.

ESTA's move toward a complete service-focused approach has resulted in enterprise level agreements on certain Microsoft software products. These agreements provide the Army with access to required state-of-the-art Microsoft desktop, application and server software and six years of software upgrades.

"We are buying in bulk and standardizing the software at the same time," said Hylton.

In the wireless environment, ESTA is working closely with the Information Technology E-Commerce and Commercial Contracting Center (ITEC4), to develop blanket purchase agreements, which will provide an enterprise solution to wireless technology.

In its focus on the Army Knowledge Management mission strategic goals, NETCOM works to scale AKO as the enterprise portal to provide universal, secure access for the entire Army. In conjunction, ESTA is working to link with the Army Transformation Campaign Plan to incorporate technology and leverage streamlined knowledge processes into the Army at a cultural level.

"NETCOM is taking the lead as the global information provider. We are consolidating servers, strengthening and centralizing Army entry points into the Global Information Grid, and establishing centralized processing centers," said Hylton. *"We ensure reliable, sustainable and survivable capabilities in support of Army and joint information technology requirements."*

The goal is to transform the Army's information systems infrastructure through enterprise management.

"One Army portal, one Army-wide security policy and posture, and one comprehensive and universal Army communications directory is what we envision," said Hylton.

Soldiers from the 5th Signal Command hook up cables to the communications shelter from a tropospheric scatter radio antenna.

All qualified users would have single sign-on capability and have the capability to log on to the portal from any computer, anywhere, anytime, using their names and passwords. Once in the Army Knowledge Online system, users can push or pull all the information they need.

Explaining that the Army portal could be compared to Internet services like AOL, Goggle and Yahoo, the general said it was much more useful than those services.

"It is a controlled environment that is password protected for authorized users. Our young Soldiers pick up on its uses rather quickly because most of them were raised with the Internet in their homes."

"The uses for AKO are endless," said Hylton. *"AKO is constantly evolving. It provides authentication for more than 100 applications, and through the use of a common user ID and password, it is faster and easier for users to traverse the portal from application to application."*

Under the supervision of the chief technology officer, AKO provides services for all users, such as immunization status, TDY information, pay and promotion information, HIV/DNA status, and alerts to Soldiers who have a college loan repayment deadline looming.

Since August 2001, AKO use has increased from 160,000 accounts to more than 2.5 million. AKO isn't only for the Soldier and Department of the Army civilian employee. AKO gives family members a way to stay in touch with their own family member account, through account sponsorship capabilities.

"For its part in the war on terrorism, NETCOM/9th ASC, using the collective capabilities of all its major subordinate commands, provides the services associated with use of the GIG," said Christopher Gandy, deputy chief of current operations G-3, NETCOM/9th ASC.

Support includes SIPRNET, NIPRNET, video teleconferencing capabilities, voice telephone, and the Defense Red Switch Network connectivity. *"This, in turn, through the seamless nature of the GIG, provides our sister Services joint connectivity through those same services,"* said Gandy.

"Support for the war is provided primarily through our tactical brigades, but supported by our strategic brigades, through deployment of tactical satellite, (both multi- and single channel), tropospheric scatter radio, microwave radio and line-of-sight radio capabilities," Gandy said.

NETCOM units maintain network connectivity at echelons above corps headquarters deployed worldwide. Since the war on terrorism NETCOM had deployed almost 10,000 personnel for signal support worldwide, an increase of almost 100 percent from pre-war figures.

"NETCOM also provides network visibility worldwide through the Army Network Operations Security Center (ANOSC) and a number of Theater Network Operations Security Centers (TNOSCs) that monitor and track communications status of communications links throughout the Army's portion of the GIG," said Gandy.

Additionally, the ANOSC is NETCOM's front line force in the realm of computer network defense, working hand-in-hand with the Army Computer Emergency Response Team (ACERT) to protect the Army's portion of the GIG from electronic threats such as worms, viruses and denial of service attacks.

"We've provided commands and organizations throughout the theater the same kind of informational capabilities they have available to them at their home stations," said Hylton.

"In fact, to support the growing need for communications support in Southwest Asia, NETCOM activated a permanent strategic signal brigade, the 160th Signal Brigade in Kuwait. The success in the campaigns in Afghanistan and Iraq can be partially attributed to network-centric operations," said the general.

"We know we must have a signal force that is modular, joint and capabilities based. We must shape our signal units so they can provide effective C4 capabilities for joint contingency operations, and in order to do that, our structure and capabilities must reach across our entire signal team — active, Reserve and National Guard."

Maj. Gen. James C. Hylton
Commanding General
NETCOM/9th ASC

"Our operations in Afghanistan and Iraq prove the information-enabled Army is at the foundation of the future force. Our rapid and seamless flow and exchange of information and situational awareness during these operations proves that our ability to rapidly and securely deliver the message is a significant combat multiplier."

"The fact is that today our operating environment is one of sustained engagement and our signal units must be structured and capable of supporting our warfighting commanders, often with little or no notice," said Hylton.

"Given the reality of sustained engagement, we are applying the important lessons learned from the experiences we've gained from supporting operations in Bosnia, Kosovo, East Timor, Afghanistan and Iraq. We know we must have a signal force that is modular, joint and capabilities based."

"We must shape our signal units so they can provide effective C4 capabilities for joint contingency operations, and in order to do that, our structure and capabilities must reach across our entire signal team — active, Reserve and National Guard."

NETCOM is currently engaged in the effort of providing a commercial communication network in Iraq that will provide robust communications to the multiple Joint Task Forces supporting the Joint Forces Land Combat Commander (JFLCC), Joint Forces Commander, U.S. State Department, our allies and other civilian authorities.

The future of signal is here, the general said.

"We have already begun the process of restructuring our units so that we can very quickly deploy integrated theater signal battalions capable of providing a full range of transmission, data and networking capabilities."

The modular design allows us to tailor specific communications packages to support specific mission requirements — a critical capability necessary in providing the complex command and control tools that our warfighters have come to expect in the wide range of joint environments we find ourselves operating in today.

"By modifying our signal unit organizational structure, we increase our ability to provide warfighting commanders with rapidly deployable, flexible and highly capable modular communications packages that are easily tailored to meet specific mission requirements while providing them with critical C4 capabilities needed to successfully meet their objectives in our sustained engagement joint operating environment," said Hylton.

"Our Army's battlefield success is contingent on the right information reaching the right Soldier at the right time, and to do this we must consolidate our networks into a single enterprise. That is what NETCOM is all about."

Editor's Note: Thanks to Gordon Van Vleet, NETCOM/9th ASC, Public Affairs Officer, for interviewing Maj. Gen. James Hylton and Christopher Gandy for this article. CHIPS

The Navy's Transition to IPv6

By Mark Evans

One of the more significant evolutions in the history of the Internet is upon us. Internet Protocol version 4 (IPv4), the standard upon which the Internet has operated for the last 20 years, is running out of addresses. Several work-arounds have been implemented in the past few years which enabled the Internet to continue to function. While experts do not agree on the time remaining prior to exhausting the pool of IPv4 addresses, most indications are that it is less than a decade.

The next generation Internet Protocol, IPv6, will solve the address shortage by providing an almost incomprehensible number of IP addresses. Unlike the original implementation; however, there are now millions using the Internet every day. This has prompted some to say that changing protocols now is like changing the engine in a moving airplane. The Department of Defense, a core Internet user, is leading the effort to enable a smooth and timely transition.

The Department of Defense, a core Internet user, is leading the effort to enable a smooth and timely transition to IPv6 …

The Assistant Secretary of Defense for Networks and Information Integration (ASD NII) established a Department goal for transitioning all enterprise-wide networks from IPv4 to IPv6 by FY 2008. ASD NII directed that beginning Oct. 1, 2003, all assets developed, procured or acquired shall be IPv6 capable in addition to maintaining interoperability with IPv4 systems/capabilities. In response to the DoD directive, Chief of Naval Operations, Navy Information Office (NIO) designated OPNAV N6F and N61 to lead Navy IPv6 transition plan development. OPNAV in turn delegated the Space and Naval Warfare Systems Command 057A as the designated IPv6 transition technical lead.

Introduction to IPv6

IPv4 uses a 32-bit/4-octet addressing scheme. It's stability and simplicity have been the catalysts of the Internet explosion. IPv4 was originally implemented on ARPANET, a network collaboration of U.S. universities and research centers, funded mainly by the federal government. The designers could not have foreseen the global Internet expansion, and as a result, IPv4 suffers from some serious deficiencies that are driving it to obsolescence.

Available IPv4 address space continues to be depleted and now must be very carefully allocated. These shortages have been partially mitigated through Network Address Translation (NAT) and Classless Interdomain Routing (CIDR). NAT is in widespread use but it is inflexible, often presents a single point of failure and

ASD NII directed that beginning Oct. 1, 2003, all assets developed, procured or acquired shall be IPv6 capable, in addition to maintaining interoperability with IPv4 systems/capabilities …

prevents, in most cases, the deployment of new peer-to-peer Web-based applications such as gaming and collaboration.

The global demand for more unique IP addresses prompted the Internet Engineering Task Force (IETF) to develop a more robust addressing scheme, IPv6. IPv6 increases addressing availability several orders of magnitude along with other optimizations and improvements. These are summarized below.

Larger Address Space: 128-bit addresses ensure a virtually inexhaustible supply.

Streamlined Routing: The IPv6 header, while larger, is also less complex, which allows route aggregation (simplified hierarchical routing), dramatically reducing the size of routing tables and improving router performance.

Multicast Support: IPv6 inherently supports multicast.

Mobility: Provides an improved version of Mobile IP, which allows mobile nodes to connect to the network at different locations without disrupting communications.

Quality of Service: Although implementation details are yet to be resolved, the IP header includes fields to support real-time and priority traffic.

Auto-configuration: IP addresses and other network-related parameters can be configured automatically.

Native IP Security: All IPv6 implementations must support the IP security features.

The Transition to IPv6

Once the domain of researchers and the government, the Internet is now a well-established commercial entity. Its exact size and configuration are unknown and constantly changing. There is no single controlling authority, and DoD represents only a percentage of the global Internet constituency. Transition to a new underlying protocol will require substantial time, effort, and in some cases, new hardware.

It is predicted that the IPv4 address shortage will become critical by 2010. This presents a reasonable time frame for a gradual

IPv6 increases addressing availability several orders of magnitude along with other optimizations and improvements …

transition to IPv6. During the transition phase, a hybrid environment comprised of both IPv4 and IPv6 addressing will be fully supported, an approach supported by industry and DoD. Transitional mechanisms, such as tunneling, will exist to ensure connectivity for all programs, although in doing so some of the enhanced features of IPv6 may not be fully utilized.

While some programs may not transition to IPv6, such as those nearing the end of their life cycle, most infrastructures, systems and applications will be affected. To plan adequately for transition, major assessments will need to be made with regard to engineering; procurement; information assurance; test and certification; and deployment.

IPv6 promises a substantial payoff. IPv6 will be an enabling technology of network-centric operations and warfare that will include: mobile platforms; networked sensors; unmanned systems; unmanned aerial vehicles; space systems; and reach-back to logistics bases, facilities, people and information. IPv6 native security will add another layer to the Defense-in-Depth approach to network information assurance. Quality of Service (QoS) features inherent in IPv6 will enhance traffic engineering to an extent not possible with IPv4.

The Navy's IPv6 Transition Plan envisions the evolution of the Navy's institutional and operational networks into one network-centric entity, improving access to the warfighter knowledge base and institutional support systems that will enhance interoperability; mobility; security; reliability; scalability; and assured information integrity.

SPAWAR 057A is chartered as the Navy's IPv6 Transition Office. Its purpose is to help all acquisition activities plan up front and early to maximize the effectiveness and minimize the financial impact of transitioning to IPv6 …

SPAWAR 057A is chartered as the Navy's IPv6 Transition Office. Its purpose is to help all acquisition activities plan up front and early to maximize the effectiveness and minimize the financial impact of transitioning to IPv6.

For further information on Navy IPv6 transition, please contact navyipv6@navy.mil or visit https://c4isr.spawar.navy.mil/ipv6/.

Mark Evans is the deputy director for Navy Enterprise IT Services, IPv6 Transition Office - 057A SPAWAR. CHIPS

Climbing the Knowledge Management Mountain

Lessons Learned from Operation Blinding Storm

By Cmdr. Kathy Donovan and Lt. Cmdr. Danelle Barrett

Introduction

New collaborative tools and cross-domain technologies being introduced to the fleet are presenting knowledge managers with exciting opportunities and significant challenges. These tools are the means to achieve new levels of operational efficacy, efficiency and interoperability, but users must incorporate process changes to gain maximum advantage. Knowledge managers must find ways to ensure users understand and embrace these capabilities by making the introduction of new technology relevant, quick and easy.

The following definitions are provided to ensure an understanding of the terms used in this article. Knowledge management (KM), as defined by Karl-Erik Sveiby, "is the art of creating value from intangible assets." Sveiby states that knowledge management aims to direct the ways in which we create, discover, exploit, disseminate and retain the expertise, understanding and practical know-how that individuals and organizations possess. (This information is available on Sveiby's Web site at http://www.sveiby.com/.)

In Navy terms, we interpret a knowledge manager as someone who obtains and analyzes information, sorts out what is needed, how it will be evaluated in operational context and used by operators. Operators use "know-what" and "know-how" to gain tacit knowledge and wisdom as depicted in Figure 1. This knowledge becomes a decision point for the commander.

Know what - *Raw material for decision making*

Know how - *Resources required to act effectively*

Facts	Beliefs
• List of who knows what	• Assumptions – mental models
• Concepts, theories	• Values, attitudes
• Data on sales, costs, markets, etc.	• Common sense
Procedures and Rules	**Attitudes**
• Assumptions – mental models	• Expertise/artistry
• How-to manuals	• Learned behaviors
• Automated processes	• Culture
• Contingency plans	• Body Skills
• Methodologies	• Intuition

Information - *Structured and coded*

Tacit Knowledge - *Unstructured, not coded*

Figure 1. Karl-Erik Sveiby's Internal Knowledge Resources

Background

In the context of a Carrier Strike Group (CSG) we define information management (IM) as the understanding of the operational environment coupled with technology and command and control, communications, computers and intelligence (C4I). IM is a convergence of the tools, processes and procedures to expedite data, information flow and analysis.

Commander, Cruiser-Destroyer 8 (COMCRUDESGRU 8) participated in Combined Joint Task Force Exercise (CJTFEX) 04-2, Operation Blinding Storm, as the Combined Forces Maritime Component Commander (CFMCC) aboard USS Mount Whitney (LCC 20), May 21 - June 21, 2004.

This exercise introduced new tools to improve IM and KM: cross-domain chat, Web replication between network enclaves and cross-domain mail guards. (See the IM Sample Toolkit on page 31 for more information.) More importantly, it provided opportunities for operators to change processes to leverage technologies to full potential — opportunities which were met with varying degrees of success.

During CJTFEX 04-2, the CFMCC reported directly to the Combined Joint Task Force Commander – Commander, Second Fleet. As an afloat CFMCC, our staff was responsible for operational control of five Subordinate Maritime Commanders (SMCs) including the USS John F. Kennedy (CV 76) CSG; USS Harry S. Truman (CVN 75) CSG; HMS Invincible Task Group; Commander, Mine Warfare Command; and the Maritime Patrol and Reconnaissance Aircraft Group under the direction of the Canadian Air Division Commander Maritime Air Commander Atlantic.

The maritime coalition consisted of 60 ships and 200 aircraft from the United States, Canada, United Kingdom, Germany and Peru. The challenges from an interoperability and KM perspective were immediately apparent.

√ *How could the coalition forces exchange knowledge and information rapidly and securely in a bandwidth disadvantaged environment?*

√ *What set of common collaborative tools existed to communicate?*

√ *How could users be quickly registered and indoctrinated to the new tools, including the cross-domain chat, secure mail guards and document sharing via Collaboration at Sea II?*

√ *How could existing tactics, techniques and procedures be improved using the new tools?*

The KM Mountain

The tools and people are in place, the summit is within view, how then does the knowledge manager facilitate the users leap to the top?

First and foremost, an organizational understanding and acceptance must take place. Specifically, that KM is not an N6 or techie function — it is a process that belongs to everyone with the knowledge manager serving as the lead change agent. True KM and its ultimate by-product, wisdom, do not occur in a vacuum. There must be an

alignment across the organization and its key functional areas. On a Strike Group staff this would include N2 (Intelligence), N3 (Operations) and N6 (Communications). Without proper alignment, the sum of the parts will never exceed the whole — and the potential exists for inefficiencies, stovepipes within departments or poor operational choices.

The knowledge manager instructs users about KM practices and its subset IM. By encouraging and fostering an understanding of these concepts, people can begin to re-evaluate existing tactics, techniques and procedures (TTP) with the goal of shared tacit and implicit information. Tools that are cumbersome or confusing are quickly abandoned. The knowledge manager can facilitate by: Making tools easy to register for, understand, use and leverage. For users, a process should be reengineered and technology applied (best scenario) or an existing process can be used with a new technology (the least desirable scenario).

There was both KM success and failure during Operation Blinding Storm. A success was the Second Fleet Knowledge Management Board, chaired by the Canadian Navy Deputy Chief of Staff for Commander, Striking Fleet Atlantic, Capt. James T. Heath. The board was attended by key stakeholders from every department and executive agents from the public affairs offices, flag staffs and component commanders' liaison officers (LNOs). Using standard operating procedures, the board worked on the process piece, the most important and challenging aspect of KM.

Within the CFMCC, the human element was the area that required the most improvement. While there were many new tools available, most people reverted to old processes using new tools rather than changing the process to leverage new tools to advantage. A lot of time was spent pushing information, but not a lot of time was spent analyzing and taking action. In short, there was too much time spent on the output and not enough time on the outcome.

To counter this process problem, all cells within the CFMCC should have a full-time, trained knowledge manager — a "power user" — someone experienced in information technology, who also has operational understanding to ensure information is shared for timely decision making. Although the watchbill included a knowledge manager for every watch section, this function was not clearly understood. People assigned quickly became tasked with other work, and the KM function was perceived as a collateral duty.

The elements of KM, and even basic elements of IM, fell by the wayside as people reverted to known processes and methods for sharing information and knowledge. CFMCC knowledge management cells sprouted like mushrooms when there was an information crisis and dissipated as the crisis went away.

The CFMCC knowledge management successes realized were not necessarily orchestrated, rather they emerged. As the tools and processes associated with IM and KM become well understood throughout the fleet, important lessons can be learned and shared.

The following are several lessons learned that resulted from our experience in Operation Blinding Storm that are applicable on the Carrier Strike Group level.

√ The knowledge manager should be a special assistant to the chief of staff (COS). While the function of knowledge manager relies heavily on the tools and paths provided by N6, KM is not inherently or solely an N6 function. Rather, it cuts across all disciplines within a Strike Group from operations and logistics to force protection and administration.

√ The COS should chair the KM Board. The COS is in the best position to ensure a process is instituted for evaluating data and providing analytical information to the commander.

√ Everyone must understand that KM is a critical element of any staff and must be built into the battle rhythm.

√ Each ship in the CSG should designate, at a minimum, a khaki level N3 and N6 representative to actively participate on the board.

√ Prior to CSG work-ups, group sails and deployment, the KM Board must have high priority with an updated KM Plan and IM Matrix that are understood and tested in C4I Fast Cruises. The cruises should test capabilities, tools and processes to ensure that the most effective tools are used during actual operations. If the plan is formulated prior to group sails with all key stakeholders, then bandwidth limitation issues can be resolved resulting in real process improvement.

√ As the CSG deploys, the KM Board should meet frequently, virtually and in a collaborative environment when possible and face-to-face communications are impractical or unnecessary. At a minimum, the board should collaborate prior to entering a new theater of operations, so unique requirements are understood and solutions are leveraged throughout the CSG. This allows the group to be more proactive using strategic planning rather than reacting to the latest information crisis.

The KM lessons learned from Operation Blinding Storm are common and practical suggestions. While much can be shared in terms of lessons learned, it is a mistake to think that any one KM Plan or Navy-Wide OPTASK Information Management Plan will be a one-size-fits-all solution.

This type of plan is beneficial for overarching guidance and recommendations where standardization is realistic operationally or technically. However, each theater and each situation has unique knowledge requirements that must be considered, such as joint and coalition requirements, availability of IM tools, information assurance and foreign disclosure issues, etc.

KM is in its infancy in the Navy. It can be challenging to organize, but with proper tools, training and process improvements it can be an empowering force enabler. The summit can be reached and success achieved through proliferation of appropriate IM tools and iterative Navy-wide training.

One suggestion is that the resource sponsors of the major communities within the Navy could ensure KM training is integrated into all warfighting and supporting disciplines — not just as a standalone topic. Training included in every level of tactical instruction for officers and enlisted will instill a sense of process ownership from Sailor to Admiral.

Information Management Sample Toolkit Operation Blinding Storm

The following are the technologies we worked with in Operation Blinding Storm and our evaluation of their effectiveness. The first step in discerning the effectiveness of operational tools is to look at their capabilities and concepts.

Cross-domain Secure Mail Guards. This technology has been around for several years, but the fleet is just beginning to use it. An example of the mail guards used in Operation Blinding Storm were: (1) Secure mail guard at COMUSNAVEUR connecting the SIPRNET and the classified United Kingdom national network Combat Support Systems (CSS); (2) Pacific Region Network Operations Center connecting SIPRNET with the Combined Enterprise Regional Information Exchange System (CENTRIXS) Four-Eyes (United Kingdom, United States, Canada and Australia); and (3) Global Reach Interactive Fully Functional Information Network (GRIFFIN) connecting SIPRNET to several other nations' national classified systems.

As e-mail passes through the guards, messages are screened for a classification line at the top, embedded malicious code, and inappropriate or unauthorized words that may result in an inadvertent disclosure of classified information. If the format line is incorrect or an unauthorized word is discovered, the message is rejected and returned to the user. Many of these guards allow e-mail attachments, and this capability proved extremely successful in aiding information flow. Most of the difficulties encountered with the guards were process not technology based. The registration process can be cumbersome, errors in the classification line (which causes the message to be rejected) are common, and the inappropriate words lists were not readily available, so users did not always know why an e-mail was rejected. Users were also confused by the different guards and the unique e-mail address associated with each guard.

The CFMCC N6 staff assisted users with registration, and we loaded Classify software, which preconfigures mail guard classification line options for users to choose from. Having a drop down menu of options with clear guard titles reduced the occurrence of human error. This was particularly important because there were five different mail guard options, each with different classification line requirements. Users who didn't learn how to use the guards were quickly frustrated with their inability to move information easily.

Multi-Level Secure Chat. This program, developed by the Naval Research Laboratory and the Naval Warfare Development Center, was beta tested during the exercise. It allowed operators to chat between the CENTRIXS Four-Eyes and SIPRNET enclaves. The program provided user authentication, an important security feature in any chat tool, and a necessity as chat becomes more acceptable for passing tactical information and orders.

From a user perspective, this tool had several attractive features, such as the ability to view the discussion that preceded the user joining the chat room. This is important for maintaining situational awareness for afloat units which frequently lose satellite connectivity and need to rejoin a discussion. Another great feature was that this tool allowed U.S. watchstanders to remain at their SIPRNET workstations rather than move to CENTRIXS workstations, which were limited in number and not located in spaces where key staff members operated.

A follow-on goal could be to expand this tool between national systems. Development of the tool should continue as a Web service and be integrated into the shared infrastructure of the Fleet Application Server. While the program is based on homegrown proprietary code, giving the code to the open source community for further development could yield big results at little cost. Additionally, the program should be tested by the Joint Interoperability Test Command for inclusion into the Defense Collaborative Tool Set.

Cross-Domain Replication. Document sharing was facilitated using the IBM Lotus Domino based Collaboration at Sea (CAS) II on CENTRIXS and SIPRNET. Cross-domain replication, enabled by the Pacific Region Network Operations Center, assisted in this capability. CAS has been used successfully for several years, but a new feature was added during Operation Blinding Storm — users could post information on the CAS II Web site hosted on both SIPRNET and CENTRIXS Four-Eyes. The CAS architecture presents an excellent way to smartly replicate change only data in a discontinuous, bandwidth disadvantaged environment.

The Operation Blinding Storm CAS II site, designed and maintained by Navy Cmdr. Paul Matheson from Second Fleet, was the central repository for information sharing between all component commanders and the CFMCC Subordinate Maritime Component Commanders. While this tool presented a leap in cross-domain information sharing, lessons learned included: (1) Lengthy replication times between domains (three hours to several days); (2) Shipboard Web browsers had to point to the server afloat to conserve bandwidth; (3) Training was needed for posting and retrieving information, registration and avoiding replication collisions.

Solving these problems involves both technology and process changes. Latency issues could be mitigated by hosting servers at the Unified Atlantic Region Network Operations Center and the Naval Computer and Telecommunications Area Master Station, Naples, which could replicate and synchronize databases at the primary point of presence locations for afloat units. Information managers could help users by working with CAS II developers to create a tool to mass register users of deployed afloat commands traveling from one server to another (i.e., COMCRUDESGRU Eight to Second Fleet to USS Harry S. Truman).

Information managers could also develop a way to prioritize replication for smaller files first, and integrate a notification capability that would inform users of updates to specific sections of Web sites they subscribe to.

Cmdr. Donovan and Lt. Cmdr. Barrett are Information Professional Officers assigned to Commander, Cruiser-Destroyer Group 8. Cmdr. Donovan is the Deputy N6 (C4/IW) Officer and Barrett is the Communications Officer.

Can You Hear Me Now?

The JCEOI - Another Facet of Spectrum Management

By the DON CIO Spectrum Team

To use a current phrase, "being on the same page," is not adequate for military communications. If your unit or aircraft is not on the correct frequency, with the correct call sign and encryption scheme, coordinated operations are in jeopardy and potential friendly fire situations develop rapidly. The establishment and use of effective tactical communications are instrumental to successful training and peacetime operations — and they are critical in combat situations. Vital command and control (C2) mechanisms rely on the ability to quickly transmit information across the battlefield and throughout the world.

Individually, the military services are well trained and knowledgeable in their use of service-specific communication procedures. However, joint operations significantly complicate standard operating procedures and introduce a myriad of factors that must be overcome to ensure joint communications meet and exceed C2 requirements. Some of these complications include the use of new technologies and equipment, unfamiliar communication equipment capabilities and stovepipe, proprietary type equipment issues.

Most joint communication interoperability factors are overcome by establishing communication plans that create and assign common procedures and standards. To this end, the U.S. military uses a number of communication documents. For example, the Navy's primary communication control document is called an Operational Tasking of Communications (OPTASKCOMS). The overall operational plan (OPLAN) includes an Annex K that serves as the communication plan for all services.

Unique to aviation missions is the Air Tasking Order (ATO) used to task and disseminate projected sorties, capabilities and forces for targets and specific missions to components, subordinate units and command and control agencies. The Communications Electronics Operating Instructions (CEOI) are issued to control and promulgate communication procedures and standards.

The CEOI (known by the U.S. Army as the Signal Operating Instructions or SOI) is widely used by the Army and the Marine Corps, and to a lesser extent by the Navy and the Air Force. When jointly used, the CEOI is called the Joint CEOI or JCEOI. The JCEOI is the most widely used communication control document in any given area of operation. It is used by aviators, communicators and technical personnel in control facilities and joint staff positions.

What is the JCEOI?

JCEOIs are the primary controlling document for single channel radio communications in joint operations and exercises. The Single Channel Ground and Airborne Radio System (SINCGARS) is a family of Very High Frequency (VHF), Frequency Modulated (FM) radio sets. SINCGARS is capable of short- or long-range operation for voice or digital communications. It can be used for single channel operation or in a jam-resistant, frequency-hopping mode, which can be changed as needed. Since SINCGARS provides the primary means of command and control for infantry, armor and artillery units, formal coordination and automated tools are vital.

The JCEOI is the "telephone directory" for single-channel radio communications. A JCEOI details radio information for joint forces, service-specific elements and units including:

- Daily changing and non-changing frequency assignments
- SINCGARS cue, manual and net identification assignments
- Call sign assignments (example: Xray 3 Tango)
- Call words assignments (example: shooter)
- Daily changing code words (example: sign and countersign words for challenge and reply)

Other information found in JCEOIs, includes document handling instructions, controlling authority data, effective dates and reproduction instructions. Because of the sensitive information in JCEOIs, they are almost always classified documents.

How is JCEOI information used?

A lesson learned from the Vietnam War was that the use of non-changing radio frequency assignments and call signs often resulted in the compromise of information because the enemy was able to find and exploit radio frequencies and the information they carried. Because of that, modern JCEOI information is routinely provided in 10 individual time periods as displayed in Tables 1, 2 and 3 on the next page.

Who is responsible for creating the JCEOI?

Every individual unit and organization that uses single-channel tactical radio in a joint operation is generally assigned its single channel information (frequency assignments, call signs, etc.) in the JCEOI. Given the multitude of units and organizations involved, JCEOIs are often significantly large. Because of their overall size, individual services often reproduce and disseminate only the information they require.

JCEOI Individual Time Period Information	
Time Period	Day of the Month
1	1/11/21/31
2	2/12/22
3	3/13/23
4	4/14/24
Etc.	Etc.

Table 1.

Call Sign	Time Period					
Unit	*01*	*02*	*03*	*04*	*05*	*Etc.*
Radio Battalion	*Z2M*	*X7M*	*F5H*	*Q0N*	*F0Y*	

Table 2.

Frequency	Time Period					
Unit	*01*	*02*	*03*	*04*	*05*	*Etc.*
Radio BN Command	*4.6710*	*10.5150*	*9.0890*	*10.2580*	*8.7015*	

Table 3.

Although JCEOIs can be formatted in many different ways, a standard JCEOI assignment looks like the tables above. This JCEOI for Radio Battalion assigns the call sign "Zulu Two Mike" for time period 01 (used on the 1st, 11th, etc., day of the month). Additionally, the frequency for Radio Battalion is 4.6710 MHz (a HF assignment) for time period 01. The use of changing call signs and frequencies with encryption, provides a high degree of secure operations.

Creating a JCEOI is a complex, difficult task that requires a comprehensive understanding of all unit and equipment requirements, as well as an understanding of coordinating shared information that exists in other communication control documents. The JCEOI is considered a living document that is routinely updated.

The genesis of JCEOI development begins in initial planning conferences and continues throughout the entire planning period. Communications personnel, including spectrum managers (aka frequency managers), interpret the overall concept of operations, identify the supporting units and organizations, and begin to craft the JCEOI. In almost all cases, the actual development of JCEOIs is done by spectrum managers.

The spectrum manager's role in JCEOI development presents an interesting dichotomy in joint operations because the most widely used communications control document is created by some of the junior-most servicemen and women. Generally, spectrum managers are E-6s and E-7s, well trained and knowledgeable, with specialized training in spectrum management, including JCEOI development.

… Spectrum managers are E-6s and E-7s, well trained and knowledgeable, with specialized training in spectrum management, including JCEOI development …

Automated capability for creating the JCEOI

There are two automated tools that are widely used by spectrum managers to create JCEOIs. The oldest is the Revised Battlefield Electronics Communications Equipment Operating Instructions System (RBECS). The newest is the Joint Automated Communication System (JACS). While both programs are capable of compiling and generating JCEOIs, both programs fall short of providing all single-channel radio information used in today's joint operations.

Neither the RBECS nor the JACS program is capable of supporting advanced communications equipment such as Enhanced Position Location Reporting System (EPLRS). EPLRS is a synchronous Time Division Multiple Access (TDMA) system that provides the basic tactical functions of identification, position location and navigation information automatically to a centralized Net Control System or Land Mobile Radio (LMR) trunking. LMR trunking allows automatic sharing of a small number of radio frequencies (channels) between large numbers of radio users' information.

… A lesson learned from the Vietnam War was that the use of non-changing radio frequency assignments and call signs often resulted in the compromise of information because the enemy was able to find and exploit radio frequencies …

Because of the deficiencies in RBECS and JACS and other factors, the Military Communications Electronics Board (MCEB) authorized the development of a new JCEOI program in early 2004.

Military operations with international partners and continued joint service deployments have made the modernization of communication tools a priority. Expanded use of sensors, unmanned aerial vehicles and sophisticated weapons systems, which are all spectrum-dependent, require more precise communication planning and operational implementation. Our spectrum managers — those who prepare the JCEOIs and those who execute those plans in the field — are working hard to ensure our ability to communicate and recognize friend from foe.

For more information, contact the DON Spectrum Team at DONSPECTRUMTEAM@navy.mil. CHIPS

Developing a Net-Centric Test and Integration Process

By Rebecca Rowsey

Horizontal fusion helps ensure data is available on the Global Information Grid (GIG) for those who need it …

For the second year, the Space and Naval Warfare Systems Center Charleston (SPAWAR Charleston) is supporting the Office of the Deputy Chief Information Officer, Department of Defense, on the transformational horizontal fusion effort. Net-centric testing and integration began in earnest May 2004 in the new Horizontal Fusion Test and Integration (T&I) Lab at SPAWAR Charleston.

Establishing the T&I Lab is an essential step on the road to achieving Defense Secretary Rumsfeld's vision of net-centric transformation. It provides an environment to measure successful integration of new net-centric services moving into the warfighter, business, enterprise information environment and intelligence mission areas.

The Horizontal Fusion Portfolio strategically selects and funds service and data providers, called horizontal fusion initiatives. This approach allows the submitter to maintain its management structure and development team, while helping them to become net-centric more rapidly. Net-centricity means providing an information advantage (enhanced information sharing, improved shared situational awareness and better knowledge of commander's intent) that can be turned into a warfighting advantage, which translates into faster self-synchronization, speed of command and increased combat power.

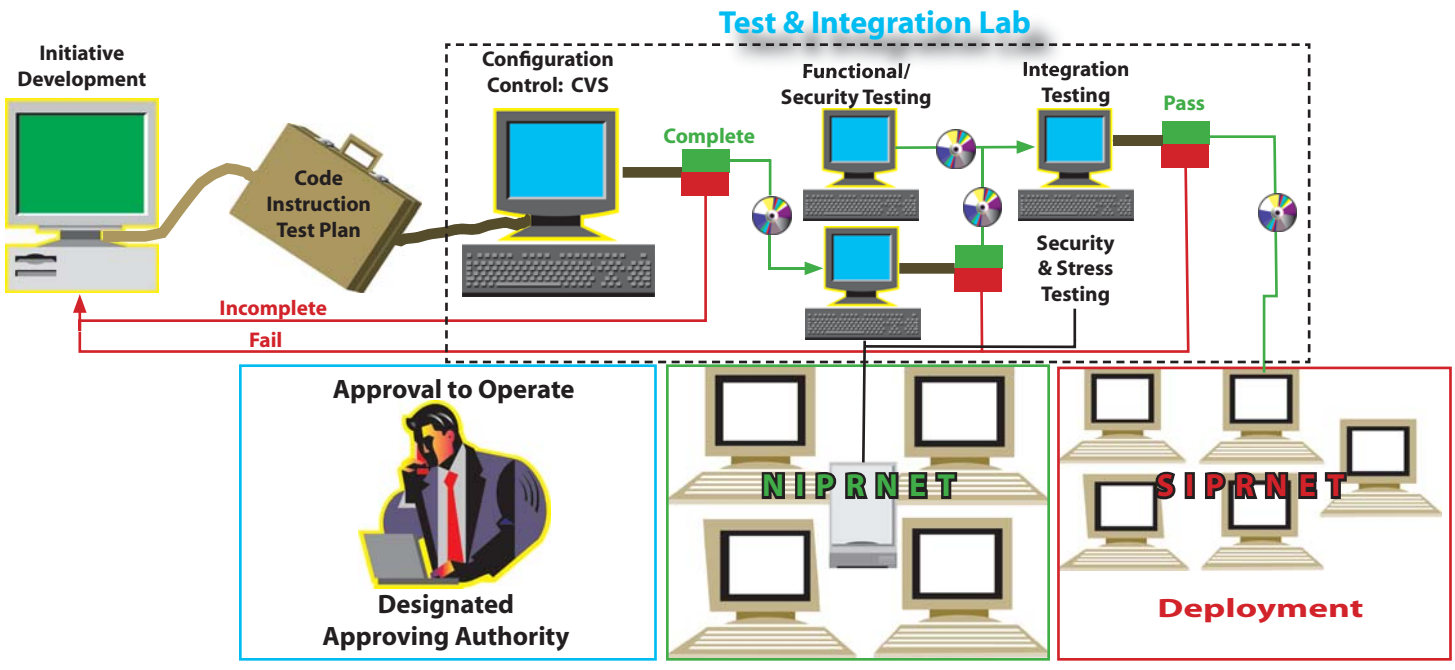
Horizontal fusion helps ensure data is available on the Global Information Grid (GIG) for those who need it, when they need it, anywhere they need it. Using horizontal fusion also ensures net-centric services facilitate manipulation of the data into information and knowledge that can be used for decision making.

Horizontal fusion is focusing on tough security policy issues that will need to be revised to accommodate a net-centric environment. For the Quantum Leap-2 demonstration on August 11, coalition and cross-domain security were introduced, surfacing key requirements for metadata tagging, issuance of SIPRNET Public Key Infrastructure (PKI) certifications and single sign-on.

The SPAWAR Charleston T&I lab team groups the initiatives as data providers, portlet providers, or as data and portlet providers. A portlet is a Java-based Web component, managed by a portlet container that processes requests and generates dynamic content. Portlets are used by portals as pluggable user interface components that provide a presentation layer to information systems.

Data providers may be producers or consumers — or both. Other key integration considerations are the external dependencies. Some initiatives depend on the output data of one or more

Figure 1. The Test and Integration Lab Process



Net-centricity means providing an information advantage (enhanced information sharing, improved shared situational awareness, better knowledge of commander's intent) that can be turned into a warfighting advantage …

Rebecca Rowsey reviews test and integration procedures for team members.

initiatives as the input data for their initiative. For example, in order to display the operational picture to support situational awareness, timely track data feeds must be supplied to the application that displays the current picture of the battlefield situation.

The T&I Lab process starts (see Figure 1) when the initiative submits to SPAWAR Charleston its software code, installation instructions, test plans and other related materials needed to accomplish functional integration and security testing. This information is stored in the Concurrent Versions System (CVS). CVS provides a means for the T&I Lab personnel to ensure they are testing the most recent version of an initiative's code (each initiative is responsible for maintaining version control of its own code). CVS also maintains all versions of the portal baseline. If the submitter's input is incomplete, the submitter will be notified to update the initial submission.

Prior to commencement of testing, the Designated Approving Authority (DAA), required by the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), reviews the Systems Security Authorization Agreement (SSAA) and the initiative's in-house testing to determine if the program is mature enough to enter testing.

The first action of the SPAWAR Charleston lab testers is to install a clean copy of the Horizontal Fusion Mars Portal (user entry point to horizontal fusion capabilities) and the initiative's code on one of the "clean" test stations. After installation, the initiative's functions are tested based on the cases submitted in the test plan. The T&I Lab also develops test cases.

The security certification and accreditation team, with assistance from the SPAWAR Charleston T&I Lab, may also perform initial security scans and checks during this test period. If these tests are successful, then the initiative's code will be installed on the server being used for integration testing. If not, the submitter will be notified of the problems found and asked to revise and resubmit the code.

Integration testing involves installing an initiative's code onto the test portal and verifying that it performs in accordance with the applications operating instructions and satisfies the mandated security requirements. SPAWAR Charleston testers then run more use cases to simulate the expected performance of the portal. During this testing, the team will look for interoperability problems as well as any other conflicts. If any are found, then the team will document the problem and work with the submitter's development teams to isolate the problem and determine what corrective action may be needed.

Clarissa Miller discusses the lab schedule with Dale Messer, Tom Glabb and Joanna Shirley.

If the integration testing is successful, remaining security testing is done to support an Interim Approval to Operate (IATO) or to grant an Approval to Operate (ATO) on SIPRNET from the DAA. Assuming successful security tests, the next step is stress testing. Stress testing is accomplished on the portal to benchmark the performance of the current configuration of the portal to assist planners in properly scaling it to support expected user loading under varied operational conditions.

The goal of horizontal fusion's test and integration process is to move new net-centric capabilities to the operational Mars Portal Server on SIPRNET as quickly as possible so its capabilities can be easily accessible to warfighters. The latest capabilities were successfully demonstrated during Quantum Leap-2. This demonstration was the second in a series designed to show the potential of new net-centric initiatives.

The goal of horizontal fusion's test and integration process is to move new net-centric capabilities to the operational Mars Portal Server on SIPRNET as quickly as possible so its capabilities can be easily accessible to warfighters …

SPAWAR's testing and integration approach in support of the Horizontal Fusion Portfolio is well underway. Having a net-centric test and integration process and proven resident expertise allows SPAWAR Charleston to provide a knowledge base and initial sourcing capability that readily facilitates the development of other net-centric programs such as FORCEnet, Joint Raptor, Net-Centric Enterprise Services, as well as other transformational services for military services and agencies.

Rebecca Rowsey, Horizontal Fusion Program Manager and account manager for SPAWAR Charleston, leads the team in providing testing and integration for the portfolio, program logistics, collaborative workspace and Joint Task Force for the Quantum Leap demonstrations.

CHIPS

Speeding Capability to Warfighters
Trident Warrior 04

By the Naval Network Warfare Command FORCEnet Execution Center

Trident Warrior 04 is the Navy's premier FORCEnet Sea Trial experiment …

U.S. military services have made significant progress in networking weapons systems and sharing battlefield data during the last 10-15 years, but more work needs to be done to ensure seamless information flow and improve joint command and control.

During the period of Oct. 4-14, Naval units of the USS Tarawa Expeditionary Strike Group will participate off the coast of Southern California in Trident Warrior 04, the Navy's premier FORCEnet Sea Trial experiment. Participants include Expeditionary Strike Group ONE (ESG-1), 13th Marine Expeditionary Unit (MEU), USS Tarawa (LHA 1), USS Pearl Harbor (LSD 52), USS Chosin (CG 65), USS Cleveland (LPD 7) and USS John Paul Jones (DDG 53).

Trident Warrior is sponsored by the Naval Network Warfare Command (NETWARCOM). Others supporting commands are the Space and Naval Warfare Systems Command (SPAWAR), Naval Postgraduate School, Naval Sea Systems Command (NAVSEA) and the Naval Personnel Development Command (NPDC).

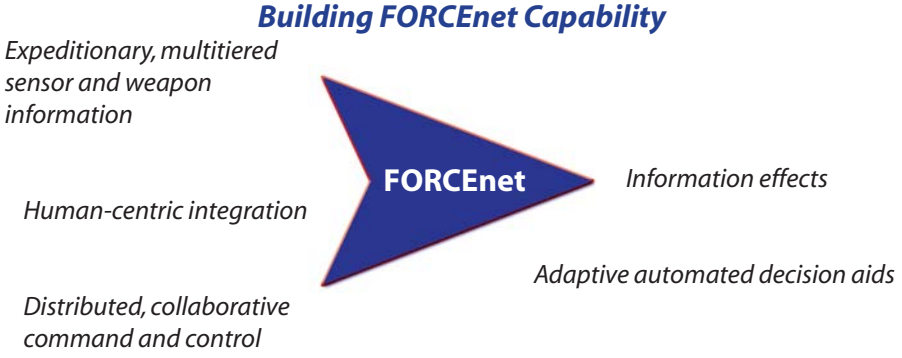
Trident Warrior's purpose is twofold. First, it will provide speed to capability, a rapid fielding of improved FORCEnet command and control warfighting capability to the fleet. And it will develop supporting tactics, techniques and procedures (TTP) designed to optimize the employment of new technologies in Naval operations. The overall intent is to identify and assess the capabilities available when operational and tactical nodes are connected in a near real-time environment.

FORCEnet, the networked command and control component of Sea Power 21, is the driving force behind Trident Warrior. FORCEnet empowers commanders to make better decisions faster and see the effective execution of those decisions. Building FORCEnet capability, Trident Warrior 04 will focus on:

- ⇒ Expeditionary, multitiered sensor and weapon information
- ⇒ Human-centric integration
- ⇒ Distributed, collaborative command and control
- ⇒ Dynamic, multipath and survivable networks
- ⇒ Information effects
- ⇒ Adaptive automated decision aids

Trident Warrior will exploit several Navy information technology initiatives, and a detailed analytical process will measure the effectiveness of these technology initiatives to help watchstanders at various levels.

Web-Enabled Warrior (WEW) is an initiative that provides integrated Web-service enterprise tools and network capabilities to assist in the completion of watchstander tasks. Increased task accomplishment will be achieved through improved knowledge of information placement and by the visualization of complex data in an effective format.



Trident Warrior 04 will organize around these six capabilities.

The following are a few of the WEW systems scheduled for evaluation:

• Navy-Marine Corps Portal (NMCP) – a suite of information services useful to tactical watchstanders in a preconfigured workstation environment. These services will increase watchstander efficiency in the performance of operational tasks by reducing his or her level of effort.

• Global Command & Control System-Maritime (GCCS-M) eWeb – a Web-enabled version of the GCCS-M picture available to all SIPRNET Web browser enabled computers.

• Naval Integrated Tactical Environmental System (NITES) - Next – an upgraded gateway to a variety of useful METOC products designed for deployed forces through distributed Web services architecture. A suite of METOC services will also be available to tactical watchstanders through NMCP.

Another program fundamental to Trident Warrior is the Naval Networks initiative, which focuses on optimizing the communications bandwidth available to the fleet. Lessons learned during Operation Iraqi Freedom identified the need for increased and better bandwidth

management in support of tactical operations. Implementing the newest version of the Advanced Digital Network System (ADNS), the networks initiative provides multipath, multitiered network architecture and uses prioritization and compression techniques to increase the throughput of tactical data between ship and shore nodes.

The Tarawa ESG will be linked using a satellite network called Extremely High Frequency, Time Division Multiple Access Interface Processor (EHF TIP), thus greatly improved tactical communications will be possible between ESG units via a point-to-point, ship-to-ship satellite architecture.

Additionally, the networks initiative provides data rate improvement for technical support applications through the Distant Support 2.0 server. As a result, afloat and ashore maintenance personnel can share system data and other information in collaborative, real-time equipment troubleshooting and repair.

Trident Warrior will also exercise FORCEnet's Expeditionary Maneuver Warfare capabilities through the achievement of limited intelligence, surveillance and reconnaissance (ISR) and Fires objectives. The Naval Fires Network or Fires is intended to provide support for combined arms strike missions in a joint task force. The goal is to improve the key linkage between ISR and Fires and to enable timely and accurate employment of Fires support in planned, immediate and time sensitive target scenarios.

The ISR-Fires evaluation will focus on watchstanders' ability to move target intelligence rapidly between sensors, C2 systems and the engagement grid with a minimum amount of manual data entry. The result will be decreased detect-to-engagement times and reduced target data errors. As an additional benefit, FORCEnet will improve the ability of geographically dispersed forces to access ESG fire support and information resources.

Like the other Trident Warrior systems, integrated TTP will be developed for ISR-Fires to improve the use of new technologies in target identification, tracking and attack. The TTP will contain guidance

The amphibious assault ship the USS Tarawa (LHA 1). U.S. Navy photograph by Photographer's Mate 1st Class David A. Levy.

on: The major functions to be accomplished at each workstation; information exchange capabilities and requirements between associated systems; information archiving and retrieval; and the processing, execution and assessment of attacks.

The greatest challenge facing commanders today is not making all of this technology work — it is making it work together. Battlespace dominance is dependent on information management — the integration of numerous and diverse technologies and the coordination of their individual applications in Naval operations.

Thus, a major Trident Warrior 04 deliverable is a comprehensive information management plan for the Tarawa ESG. This document will establish the philosophy and procedures for tactical use of information technology systems and allow their integration into ESG planning processes. As a result, commanders will have guidance on how best to employ multiple systems in planning and executing operations, and watchstanders will have a quick reference that enables them to access only that information necessary to the tasks at hand.

The success of Trident Warrior 04 will provide lasting benefits. Improvements in command and control through Web-based communications, increased and better bandwidth management and enhanced tactical and technical support through broader and more efficient information systems that will signal a dramatic step in the Navy's ability to plan, coordinate and execute complex and dynamic operations using the latest information technologies.

Quantitative measures of efficiency of human-technology interaction will improve current systems and provide a basis for the design and development of new technologies. Additionally, lessons learned from Trident Warrior will be immediately incorporated into training programs at schools like the Tactical Training Group Pacific and Expeditionary Warfare Center Pacific.

Trident Warrior 04 will be linked with Silent Hammer, another Sea Trial experiment that documents and explores the concept of operations for nuclear guided missile submarines (SSGN) and Special Operations Forces (SOF). Silent Hammer builds on the groundwork laid in Giant Shadow, which experimented with the SSGN/SOF strike force as an independent element.

Trident Warrior and Silent Hammer have important individual experimental objectives as well as shared objectives that will act as a force multiplier in achieving greater success of the overall mission of improving combat capability. CHIPS

NO MORE BAND-AID FIXES

When confronting a short-term need that calls for a fast fix to "stop the bleeding," many organizations have turned to the technological equivalent of a Band-Aid — a customized off-the-shelf solution. Like many well-known remedies, they offer some initial relief, but their long-term side effects can ultimately cause the original wound to deepen and expand. In this information technology (IT) analogy, the bleeding might be a breach in e-mail security. The supposedly simple fix is to apply a patch or application that is customized for the system. The result controls the breach, but will not prevent future intrusions. The long-term side effect is a system with a series of patches that affects total cost of ownership and results in lack of interoperability and inflexible system architectures.

Voluntary consensus standards (VCS) bodies offer an alternative to Band-Aid fixes. They provide a way to anticipate and solve the root of systems problems before they occur, and they eliminate the need for customized fixes. Congress has recognized this and included provisions in the 1995 National Technology Transfer and Advancement Act (PL104-113) for active VCS participation by government agencies.

The Department of the Navy Chief Information Officer (DON CIO) recognizes the value of the VCS bodies and participates in several key standards bodies. In this capacity, the DON is one of many government agencies and private-sector organizations that are seizing the important opportunities these groups provide for shaping product specifications and influencing vendors.

What VCS Bodies Do

VCS bodies promote development through open standards, which is a critical element for planning, developing, implementing, operating and sustaining a global information infrastructure. The specifications and decisions of VCS bodies will directly impact architecture initiatives focused on moving the DON to a Web-centric environment. From the broader DoD level, they are in step with initiatives such as the Net-Centric Enterprise Services, which include:

- Navy Marine Corps Intranet (NMCI)
- Information Technology for the 21st Century (IT-21)
- Base Level Information Infrastructure (BLII)
- Marine Corps Tactical Data Network (MCTDN)
- FORCEnet

By participating in VCS bodies and their technical committees and work groups, the DON is ensuring that its specific requirements are included (or at least addressed) in technical specifications. The result is that commercial products are based on known standards and can be more easily implemented and integrated with other systems. This translates into more efficient, cost-effective, technology-sound solutions for DON IT initiatives.

DON VCS Membership: W3C and OASIS

The DON is a member of the two VCS bodies — the World Wide Web Consortium (W3C) and the Organization for the Advancement of Structured Information Standards (OASIS) — that have the most influence over specifications for the Internet and interoperability. Membership in these VCS bodies is a sensible approach for supporting the Department's architecture initiatives, which are layered on top of the Web and its technologies.

W3C promotes and develops its vision of the Web's future by developing specifications, guidelines, software and tools that together constitute the architecture of the Web. W3C activities include Extensible Markup Language (XML), Hypertext Markup Language (HTML), Web services, security and the semantic Web. W3C specifications are used by virtually every software and hardware company as the basis of their product offerings.

OASIS drives the development, convergence and adoption of technical and e-business standards. The OASIS technical standards are practical implementations of W3C specifications. OASIS technical specifications include the suite of Electronic Business Initiative XML (ebXML) specifications for secure messaging, registry services, service-oriented architecture, security assertion and Web services. OASIS members produce more Web services standards than any other organization in the public sector. They also produce standards for security and standardization efforts and application-specific markets. Both W3C and OASIS are dedicated to developing specifications that are complementary — not conflicting or competing.

Business Standards

In addition to technical standards, OASIS develops business standards such as the XML and ISO 11179 (Metadata Registries) and the Universal Business Language, which is the basis for the recently released DON XML Naming and Design Rules publication. Another key business standards body is the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). This body develops international standards for business information exchanges used by governments and industries around the world, which includes many of our coalition partners.

Both UN/CEFACT and OASIS are collaboratively developing different facets of ISO 15000-5 Core Components specifications. The UN/CEFACT Modeling Methodology and ISO 15000-5 Core Components methodologies are being adopted by a number of U.S. government agencies. Mark Crawford of LMI Government Consulting, who supports the DON CIO, leads several international VCS standards efforts. He believes that DON involvement in VCS technical and business standards will significantly enhance the Department's ability to use commercial products. More importantly, it will provide unique insight into future trends in Internet and Web architectures, protocols and information standards, and

will enable DON IM/IT efforts to optimally implement those trends in support of its warfighter mission.

DON VCS Representatives

DON commands and individual employees with IT or e-business development responsibilities are encouraged to actively participate as Department representatives to W3C, OASIS, UN/CEFACT and other VCS initiatives. The benefit of participation is the opportunity to learn, and to insert DON requirements as part of the standards development process. Representatives can expect to:

- Provide input into shaping Internet, Web and XML specifications.
- Have access to subject matter experts to discuss best practices and leading-edge implementations.
- Review draft standards (including variations) before they are approved.
- Obtain early insights into the future direction of continually evolving technologies. These insights provide an opportunity to plan for inserting new capabilities in a timely manner, rather than responding after initial deployments in industry.
- Receive indirect benefits such as the opportunity to beta test new products that meet W3C standards and DON requirements.

The DON CIO is the coordinator for all DON interactions with VCS bodies. Commands or individuals that would like to participate on a W3C work group, OASIS technical committee, UN/CEFACT working group or other VCS endeavor should contact the DON CIO representative, by going the DON CIO Web site at http://www.doncio.navy.mil/.

CHIPS

The Department of the Navy Issues XML Naming and Design Rules

The Department of the Navy (DON) has updated its initial guidance on the use of Extensible Markup Language (XML) by issuing new DON XML Naming and Design Rules (NDR). These rules require standardization of XML development and implementation within the DON. More than a coding language, XML is a system for defining languages that provides a means of creating an environment that facilitates and supports adaptable business processes and a net-centric environment. Standardization of XML throughout the DON is critical for interoperability and will ensure that DON applications and systems are being built on commercial products rather than proprietary government requirements.

The NDR is a tool for developing robust enterprise level XML, an approach that allows for a catalog of reusable XML components – elements, attributes, types, schema – that will ensure that XML enhances, rather than detracts from, DON enterprise interoperability. The result will be an environment that is sustainable, responsive and agile. The NDR in conjunction with DON XML Policy requires program managers to avoid using proprietary extensions or XML schema and other elements that are specific to a vendor's software.

"Many program managers and vendors are adding customizations to specifications in an attempt to build market share, which leads to proprietary implementations and expensive middleware solutions," said Robert Green, lead for the DON CIO XML Interoperability and Standards Team. "We're mindful of that. By prohibiting proprietary extensions as part of the DON XML Policy, specifically articulated in the NDR, we are proactively seeking to ensure that vendors adhere to voluntary consensus standards in their products."

DON contractors will now know exactly what is required for DON XML, instead of being presented with competing XML requirements for different entities within the Department. Compiled in a 170-page handbook, the NDR provides specific rules that require conformance for consistent XML development and enterprise interoperability. It also provides closure for a number of standardization issues that were unresolved when the NDR's predecessor, the DON XML Developer's Guide, was published in 2002.

The handbook contains standards-based rules for 18 XML categories, including: attribute declaration, element naming, namespace management and schema structure modularity. The DON XML Work Group developed the NDR, working in close partnership with representatives from voluntary consensus standards bodies such as the Organization for the Advancement of Structured Information Standards (OASIS), the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and the International Organization for Standardization (ISO).

This new version incorporates key voluntary consensus standards such as ISO 11179 Metadata Registry and ISO 15000-5 ebXML Core Components, aligns with the forthcoming Federal Enterprise Architecture Data Reference Model and is based on the OASIS Universal Business Language Technical Committee and UN/CEFACT Applied Technology Group XML Naming and Design rules.

By basing the NDR requirements on voluntary consensus standards (VCS) from leading standards bodies such as OASIS, UN/CEFACT, ISO and the World Wide Web Consortium (W3C), the DON is also supporting the goals of Public Law 104-113 and the Office of Management and Budget Circular A-119, which encourage agency use of such standards.

The NDR is available as an Adobe PDF at https://www.nko.navy.mil/ on the DON XML Program page or at http://www.doncio.navy.mil/. It will also be published in HTML and XML formats.

CHIPS

DICE Supports Joint Interoperability Testing, Training and Exercise Transformation Initiatives

By Capt. Paul Dunbar, Marty Mendoza, Ric Harrison and Chris Watson

The Department of Defense (DoD) Interoperability Communications Exercise (DICE) is an annual training exercise, sponsored by U.S. Joint Forces Command (JFCOM) and conducted by the Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC).

DICE is the only DoD exercise whose primary purpose is to certify systems for joint interoperability. DICE builds upon the successes of other DoD technology demonstration and risk mitigation events. As the sole interoperability certifier of DoD Information Technology Systems (ITS) and National Security Systems (NSS), JITC conducts DICE in support of DoD joint interoperability testing, training and exercise transformation initiatives.

Figure 1. Representative Joint Task Force used during DICE.

Participation includes communications equipment and personnel from each of the Services as well as U.S. Northern Command (NORTHCOM), the Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA).

DICE has evolved from its birth in the late 1980s into one of DoD's premiere net-centric advanced technology joint certification exercises that involves more than 30 switch systems geographically dispersed over seven time zones. DICE reduces the warfighters' risk of operational failure by aggressively testing new versions of software, equipment and employment techniques in a representative Joint Task Force (JTF) communications network. Figure 1 is an illustration of the DICE Joint Task Force.

DICE employs a robust and realistic joint architecture that provides opportunities to vigorously evaluate voice, data and video interfaces, which are critical to split-base operations.

Actual operational units install, operate and maintain the equipment and systems for the exercise. These configurations are characteristic of those used in real world combat and contingency operations by the warfighting community and provide sufficient data to assess interoperability and determine if anomalies experienced in the past were corrected.

DICE provides Joint and Service communicators with an opportunity to achieve a degree of comfort using new versions of hardware and software. This is achieved through JITC's emphasis on the three components of interoperability: ***Forces***, ***Procedures*** and ***Equipment***. DICE allows tremendous training opportunities. Typical DICE objectives include:

Interoperability: Successfully demonstrate a high degree of interoperability of new versions of hardware and software employed in Joint transmission, switching and information systems.

System Certification: Successfully integrate and conduct Joint interoperability tests on selected new systems.

Assessments: Successfully conduct developmental assessments that may not conclusively qualify for certification, but may provide valuable insight into possible future capabilities.

Training: Replicate Joint communications architectures and operational or organizational structures that allow participating units to develop mission performance-oriented training. This includes developing interoperability skills with current and legacy communications equipment and systems.

Network System Control: Establish a Joint Communications Control Center that will provide operational direction and management for all Joint net-centric resources.

Feedback to the warfighters and acquisition communities is provided in several ways. JITC publishes a DICE Test Report, Interoperability Assessments Reports, Interoperability Certification Letters and additions to our quarterly Lessons Learned Report.

DICE 2004 proved to be a huge success and involved equipment and personnel from the Army, Air Force, Marine Corps, Joint Communications Support Element (JCSE), Special Operations Signal Units, Canada, FEMA and industry. FEMA's involvement and National Guard and Reserve personnel in nontraditional roles helped supplement operational unit participation during this year's event.

Contractors with DoD sponsorship were also invited to participate in DICE. JITC's DICE '04 network successfully supported 18 tests, assessments and demonstrations. DICE '04 allowed JITC and all participants to aggressively test new versions of software, equipment and critical net-centric technologies.

It also created a dynamic training environment for enhancing the warfighter's skills in tactical network planning, management disciplines and operational awareness.

Clearly, DICE is not just a certification exercise. Organizations may participate in DICE in a number of ways. Some are required to participate as part of a fielding or maintenance process. Other organizations voluntarily participate as their Operations Tempo (OPTEMPO) allows for testing new equipment or by taking advantage of the joint network environment for training.

Vendors use DICE as a method to demonstrate solutions for warfighter issues or problems or to have their products certified for joint interoperability. JITC absorbs the majority of JITC testbed costs and costs for commercial satellite access (Ku- and C-band if required). Program managers, vendors and individual organizations take advantage of the DICE exercise because it lowers their testing expense while contributing to overall network robustness. Specific test results obtained during the event are shared only with the participants and JITC as their trusted agent.

JITC will conduct next year's event February through April 2005 at nationwide locations. Although involvement in DICE is voluntary, JITC is confident that participation in DICE 2005 will substantially increase because of the many synergistic opportunities it presents to all the Services and agencies. For example, the Navy plans to have a considerable presence in DICE '05.

By capitalizing on DICE resources, the Navy can increase the level of Joint systems testing of key FORCEnet technologies and pilot programs such as: CVN-21 – the Nimitz class nuclear aircraft carrier; DD(X) – the Next Generation Destroyer Program; and the Broad Area Maritime Surveillance (BAMS) Unmanned Aerial Vehicle (UAV). Other interoperability certification test and assessment events planned for DICE '05 include the following:

√ Marine Forces Systems Command (MARFORSYSCOM) Joint Enhanced Core Communications System (JECCS) with Digital Tech Control (DTC) Joint Certifications

√ Air Force Theater Deployable Communications Integrated Communications Access Package (TDC-ICAP) Joint Certification

√ U.S. Central Command (USCENTCOM) Time Division Multiple Access (TDMA) System Joint Certification

Above: The interior of the humvee shown at right containing the Marine Corps Joint Enhanced Core Communications System (JECCS) with Digital Tech Control (DTC) systems. JITC will conduct Joint Interoperability Certification tests of the JECCS with DTC systems during DICE '05.

√ Army Communication Electronics Command (CECOMs) Software Engineering Center (SEC) with the Common Baseline Circuit Switch software (CBCS) Joint Certification

√ U.S. Transportation Command (USTRANSCOM) Vocality 100 assessment

√ USNORTHCOM Lynx System assessment

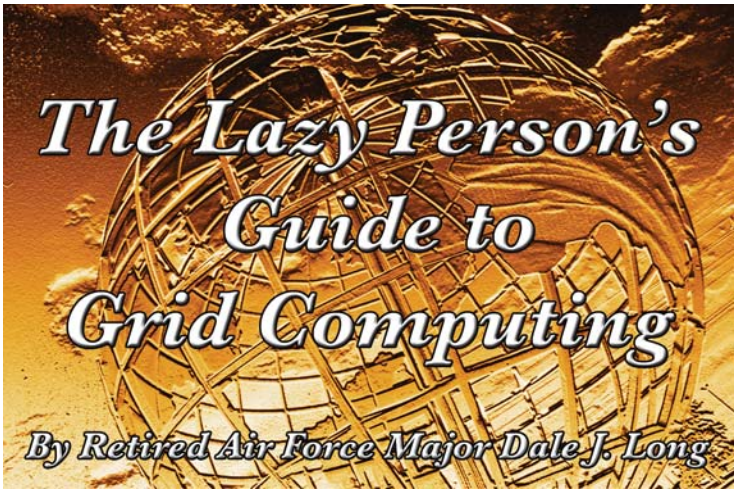
√ Numerous vendor-sponsored demonstrations and interoperability assessments

√ DoD Global Information Grid (GIG) Internet Protocol Version 6 (IPv6) interoperability assessments

√ Deployed DMS Messaging interoperability assessment

For more information regarding DICE '05 planning events, go to JITC's main Web site at http://jitc.fhu.disa.mil/dice/.

Marine Capt. Paul Dunbar, Marty Mendoza, Ric Harrison and Chris Watson are Information Technology Systems Project Officers at the Joint Interoperability Test Command (JITC). CHIPS



I would like to state up front, that I wrote this article because I lost a bet. No money changed hands. The bet was just a gentleman's agreement with myself that I would have to do an article on the subject of the winner's choice if a military organization ever produced a functional workflow system that also met federal records management requirements. Thanks to Navy Lt. Jamie Gateau and his demonstration of the Prototype ERM (Electronic Records Management) Implementation at Naval Network and Space Operations Command (NNSOC), this issue's edition of the Lazy Person's Guide will address grid computing.

The term "grid computing" came into fashion in the mid-1990s to describe a wide variety of distributed computing projects. The term itself brings to mind an interconnected grid of machines that form a single, massive entity. Reform that vision slightly to account for the fact that the "grid" can be any shape, can cover the entire world, and consist of computing devices that can range in size from desktop PCs (personal computers) to large mainframes, and you should get a good mental picture of a global grid system.

However, grid computing involves more than just the physical architecture that comprises its network. It also includes all the associated information resources and the protocols used to make dozens, hundreds or thousands of disparate devices essentially function as a single unit. Properly implemented, a grid could become the organizational equivalent of an intelligent, nominally self-aware technological central nervous system that provides access to and coordination of computing power, data, information and knowledge for an organization by efficiently using every available resource all the time.

Divide and Conquer

Before we get to a more detailed look at grid computing, let's first look at its most famous predecessor: *distributed computing*, which also involves a number of devices each sharing a single purpose. However, distributed computing is a much simpler basic concept: Break up an activity that consists of many similar, repetitive tasks and distribute those tasks to every available machine for processing. Here's a simple example of how to construct a distributed computing exercise. Let's say we want to build a multiplication table listing all the multiples of positive integers from 1 through 12 (e.g., 1x1, 1x2 through 12x12). Including duplicates (like 3x5 and 5x3), there are 144 calculations. The application controlling the distribution then sends each calculation, one at a time, to each of the machines contributing processor time. So, 1x1 is sent to machine A, 1x2 is sent to machine B, etc., until all the available processors are working. As each machine completes its task, it sends the result back and is given a new one.

Probably the most famous example of distributed computing is the Search for Extraterrestrial Intelligence (SETI) project. SETI is a scientific effort to determine if there is intelligent life outside Earth, primarily by using the Arecibo Observatory radio telescope in Puerto Rico to detect artificial radio signals coming from other stars. However, the telescope was collecting more data (about 35 gigabytes per day) than SETI could process by using its own systems. They could not afford a multimillion dollar supercomputer and processing on the systems they could afford would take decades. It is a problem that anyone suffering from information overload can sympathize with: Too much information, not enough resources to process it.

Then someone on the SETI team looked around the office, saw toasters flying across every idle desktop computer in the room, and got a brilliant idea: Develop a screen saver that would process SETI data. Distribute that screensaver to millions of users around the world and let it use spare clock cycles to process packets of SETI data. Thus was born SETI@home which lets anyone with a computer and an Internet connection participate in the SETI project simply by loading a distributed computing client on his or her home computer to analyze packages of data collected by the Arecibo Observatory. Because all of the packages can be processed independently, much like our multiplication table example, the SETI project is a perfect match for a distributed computing application.

Consider that there are over 5 million registered SETI@home users, some with more than one computer running the SETI screensaver. An average desktop computer with a 1-gigahertz central processing unit (CPU) can process 1 billion floating-point operations per second (flops), or 1 gigaflops. The world's most powerful supercomputer, Japan's Earth Simulator, runs at 35 teraflops (or 35 trillion floating point operations per second). As of July 2004, the SETI distributed computing project is running at about 14 teraflops, which would easily make it one of the top 5 supercomputers in the world if it were a single system and teraflops were the only measure that counted. It's an impressive amount of computing power all dedicated to helping search the skies for signs of intelligent life in the universe.

Breaking encryption is another use for distributed computing. It was a distributed computing project that originally cracked the National Security Agency's 56-bit digital encryption standard (DES) in 30 days. On the next try, it was done in 30 hours. On the last attempt it only took 3 hours, which is impressive if you consider that 56-bit DES was once considered secure enough for most Internet transactions. Part of the speed increase has been attributed to faster processors, but an equal measure of the improvement was due to better management of distributed computing resources.

The Dark Side of Distribution

In addition to SETI's rather benign use of distributed computing, there have been some less friendly applications. Chief among these have been distributed denial of service (DDS) malware (malicious software) spread through various means that infects a large number of computers and then uses them as attack platforms to flood Internet servers with more traffic than they can handle.

More insidious use of distributed computing is spyware, software that loads itself onto your computer and then reports on what you do to some central database. Most spyware is commercially motivated. Marketers are simply sampling to better target their advertising, goods and services. However, there are some spyware applications that will steal data from your computer. Credit card numbers and activation codes used during online shopping are a prime target for this type of distributed malware.

A less nasty but still annoying form of distributed application is adware. Once installed, adware will pop up or insert advertisements on your screen. Some adware actually comes bundled with commercial software programs. I highly recommend that you read every line of every end-user license agreement (EULA) that comes with every piece of software you buy. Pay particular attention to anything that reads, "…and we reserve the right to install software on your computer that will periodically send information back to us." Starting with the stage.dat file incidents 12 years ago where the Prodigy consumer information service was discovered sampling subscribers' hard drives, various companies have tried many methods over the years to grab as much data from PCs as possible without either getting caught or arousing the ire of their customers. Given the potential information bonanza, can foreign intelligence agencies be far behind?

Less capable than spyware and adware, but still in the same class are the cookies you pick up while visiting various Web sites. Cookies are small files associated with particular Web sites that store information about your interaction with the site. Sometimes they store more than that. Cookies come from two main sources.

First-party cookies come from any Web site you visit directly. They can either be long-term cookies that are intended to reside on your computer for several years or session cookies that only track what you do during your current interaction with a site. Long-term cookies are usually used to store information like ID and password for automatic login, personal data that identifies you to the site owner and other information collected through your interaction with the site that may be of use to either you or the site owner. Session cookies are usually used for information with less long-term value, like what's in your current shopping cart at an online shopping site.

Third-party cookies come from sites other than the ones you visit directly. Visiting a commercial news site like CNN or *The Washington Post* Online will load their cookies, but you may also get cookies from advertising sites like HitBox or DoubleClick that have agreements with the host sites. Third-party cookies are of no benefit unless you like advertisers knowing your shopping demographics. If you want to shut them out: From Internet Explorer, go to Tools/Internet Options/Privacy/Advanced and set the third-party cookies option to "Block."

If you're concerned about spyware, adware or cookies, I recommend a couple of free programs that may help: Spybot S&D (for "search and destroy") and Ad-Aware v6. Both are freely available from http://www.spybot.info and http://www.lavasoftusa.com respectively.

Bear in mind that all this information harvesting is not limited to the Internet and World Wide Web. It all started with the introduction of the bar code scanner in the retail commercial world. Every product purchased and scanned goes into some retailer's database, which then mines the data to see what, how much, when and where people are buying. If you use a credit or debit card of some type, companies can develop detailed individual buying profiles on individual customers.

Let's take a look at what separates modern grid computing from other forms of distributed computing. While distributed computing resembles an anthill, with all the little drones working to support the queen, grid computing is a more communal system with complex resource and rights management issues. It is the next order of magnitude in networking.

Enter the Grid

There are a wide variety of opinions as to what qualifies as grid computing and some people with a project to push or a product to sell will slap a grid label on whatever they have to offer. However, I did find one reference that I believe covers all the bases: "*The Anatomy of the Grid: Enabling Scalable Virtual Organizations*," by Ian Foster of the Argonne National Laboratory and the University of Southern California (USC), Carl Kesselman of the University of Chicago, and Steven Tuecke from USC, in the International Journal of Supercomputer Applications in 2001.

While not the most recent document I have seen on the subject, it is a comprehensive and detailed description of what a grid should be. I will attempt to quote and summarize the main points here, but if you are interested in grid computing on any level I highly recommend you read the entire paper, which is available on the Web at http://www.globus.org/research/papers/anatomy.pdf. In addition, the Globus Alliance Web site (http://www.globus.org) is the single most comprehensive collection of objective information on grid computing I have found. Here are a few of the key points from the paper:

⇨ *"The real and specific problem that underlies the grid concept is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations."*

Traditional networks tie together computing resources so they can communicate but not necessarily cooperate. All the various networked personal computers on a LAN use universal services like file storage, networked printers or access to an e-mail server. But if your desktop computer runs out of processing power for whatever it's trying to do on a traditional LAN it can not call on your neighbor's desktop (or one 1,000 miles away) to pick up the extra work. That capability, however, is a goal of the grid.

⇨ *"Because of their focus on dynamic, cross-organizational sharing, grid technologies complement rather than compete with existing distributed computing technologies."*

Intranets tie machines together, network storage provides repositories for data and information, and system inventories and file indexes list available resources. Grid technologies provide the next level of evolution by replacing the "static configurations" associated with connected but stand-alone processors and storage forming a dynamic, shared pool of resources. A grid can allow remote access to information, applications, sensors, etc., that previously were only available through dedicated systems.

➨ *"Resource sharing is conditional: Each resource owner makes resources available, subject to constraints on when, where and what can be done."*

This will keep someone else's computations from taking over every clock cycle on the grid. Beware of limits on access to data and information because the whole point of a grid is to facilitate sharing.

➨ *"In defining a grid architecture, we start from the perspective that effective [virtual organization] operation requires that we be able to establish sharing relationships among any potential participants."*

This means interoperability, interoperability and interoperability. It is absolutely essential that a grid, as with any networked system, be based on common operational protocols, services and application programming interfaces.

Foster, Kesselman, and Tuecke also describe a model of grid architecture consisting of the following five layers:

• *"The grid fabric layer provides the resources to which shared access is mediated by grid protocols: for example, computational resources, storage systems, catalogs, network resources and sensors."*

• *"The connectivity layer defines core communication and authentication protocols required for grid-specific network transactions. Communication protocols enable the exchange of data between fabric layer resources. Authentication protocols build on communication services to provide cryptographically secure mechanisms for verifying the identity of users and resources."*

• *"The resource layer builds on the connectivity layer communication and authentication protocols to define protocols (and Application Programming Interfaces (APIs) and Software Development Kits (SDKs)) for the secure negotiation, initiation, monitoring, control, accounting and payment of sharing operations on individual resources."*

• *"While the resource layer is focused on interactions with a single resource, the next layer in the architecture contains protocols and services (and APIs and SDKs) that are not associated with any one specific resource but rather are global in nature and capture interactions across collections of resources. For this reason, we refer to the next layer of the architecture as the collective layer."*

• *"The final layer in our grid architecture comprises the user applications that operate within a [virtual organization] environment."*

The authors also include discussion of other issues, including dealing with user authentication; single sign-on; integrating application and storage; and enterprise and peer-to-peer technologies within a grid. And finally, in a very useful section, they describe that a grid:

➨ *Is not a next-generation Internet, but a set of services and applications that enhance the connectivity the Internet provides.*

➨ *Is not a source of "free" cycles. Grids enable "controlled sharing," not unlimited access to everyone else's stuff.*

➨ *Does not require a monolithic distributed operating system, but should instead follow the Internet Protocol model of open standards.*

➨ *Does not require new programming models, as the challenges of building a grid are not fundamentally different from those already encountered in traditional networking.*

➨ *Does not make high-performance supercomputers superfluous. They will still be needed for computational problems requiring low latency and high bandwidth. The authors suggest that grid computing may actually help increase demand for them by allowing more participants to tap their resources remotely.*

Updates and Final Words

In the *CHIPS Summer 2003* issue I reported that Apple Computer had developed a zero-configuration networking technology called Rendezvous. In a development that I believe will play a role in grid development, they have now released a Rendezvous developer's toolkit for Windows, Linux, BSD and Java. You can find more news on the Web at http://maccentral.macworld.com/news/2004/06/30/rendezvous/index.php. (Due to resolution of a trademark dispute, Apple has now changed the name from Rendezvous to "OpenTalk.")

For those of you whose grids may eventually include wireless networking, you may be interested in the recently released 802.11i wireless Ethernet security standard. The best link I have found is at Wikipedia at http://en.wikipedia.org/wiki/IEEE_802.11b, a free Web-based encyclopedia that is becoming one of my favorite sites on the Web.

It has been said that we humans only consciously use, at most, 15 percent of our thinking power. Perhaps that ís why our networks, at least compared to the potential we have seen for grid computing, seem to follow suit. However, if you already have or are building the physical structure necessary to support a grid (i.e., an organizational intranet), planning for the evolution to a grid before the intranet is set is stone is a good idea.

Well, I hope I settled my debt. Thanks again to Lt. Gateau and NNSOC for the inspiration. I look forward to hearing about their grid project some day — or maybe writing about it!

Until next time, Happy Networking!

Long is a retired Air Force communications officer who has written regularly for CHIPS since 1993. He holds a Master of Science degree in information resource management from the Air Force Institute of Technology. He is currently serving as a telecommunications manager in the U.S. Department of Homeland Security. CHIPS

Enterprise Software Agreements Listed Below

The **Enterprise Software Initiative (ESI)** is a Department of Defense (DoD) initiative to streamline the acquisition process and provide best-priced, standards-compliant information technology (IT). The ESI is a business discipline used to coordinate multiple IT investments and leverage the buying power of the government for commercial IT products and services. By consolidating IT requirements and negotiating Enterprise Agreements with software vendors, the DoD realizes significant Total Cost of Ownership (TCO) savings in IT acquisition and maintenance. The goal is to develop and implement a process to identify, acquire, distribute and manage IT from the enterprise level.

In September 2001, the ESI was approved as a "quick hit" initiative under the DoD Business Initiative Council (BIC). Under the BIC, the ESI will become the benchmark acquisition strategy for the licensing of commercial software and will extend a Software Asset Management Framework across the DoD. Additionally, the ESI was incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) Section 208.74 on Oct. 25, 2002, and DoD Instruction 500.2 in May 2003.

Unless otherwise stated authorized ESI users include all DoD components, and their employees including Reserve component (Guard and Reserve) and the U.S. Coast Guard mobilized or attached to DoD; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities such as NAFI employees; Intelligence Community (IC) covered organizations to include all DoD Intel System member organizations and employees, but not the CIA nor other IC employees unless they are assigned to and working with DoD organizations; DoD contractors authorized in accordance with the FAR; and authorized Foreign Military Sales.

For more information on the ESI or to obtain product information, visit the ESI Web site at http://www.don-imit.navy.mil/esi.

Software Categories for ESI:

Business and Modeling Tools

BPWin/ERWin

BPWin/ERWin - Provides products, upgrades and warranty for ERWin, a data modeling solution that creates and maintains databases, data warehouses and enterprise data resource models. It also provides BPWin, a modeling tool used to analyze, document and improve complex business processes.

Contractor: ***Computer Associates International, Inc.*** (DAAB15-01-A-0001)

Ordering Expires: 30 Mar 06

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Collaborative Tools

Envoke Software (CESM-E)

Envoke Software - A collaboration integration platform that provides global awareness and secure instant messaging, integration and interoperability between disparate collaboration applications in support of the DoD's Enterprise Collaboration Initiatives.

Contractor: ***Structure Wise*** (DABL01-03-A-1007)

Ordering Expires: 4 Sep 05

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Click to Meet Software (CT-CTM)

Click to Meet Software - Provides software license and support for Click to Meet collaboration software (previously known as CUSeeMe and MeetingPoint), in support of the DoD's Enterprise Collaboration Initiatives. Discounts range from 6 to 11 percent off GSA Schedule prices.

Contractor: ***First Virtual Communications, Inc.*** (W91QUZ-04-A-1001)

Ordering Expires: 05 Nov 08

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Database Management Tools

IBM Informix (DEAL-I/D)

IBM Informix - Provides IBM/Informix database software licenses and maintenance support at prices discounted 2 to 27 percent off GSA Schedule prices. The products included in the enterprise portion are: IBM Informix Dynamic Server Enterprise Edition (version 9), IBM Informix SQL Development, IBM Informix SQL Runtime, IBM Informix ESQL/C Development, IBM Informix ESQL/C Runtime, IBM Informix 4GL Interactive Debugger Development, IBM Informix 4GL Compiler Development, IBM Informix 4GL Compiler Runtime, IBM Informix 4GL RDS Development, IBM Informix 4GL RDS Runtime, IBM Informix Client SDK, IBM Informix Dynamic Server Enterprise Edition (version 7 and 9), and IBM Informix D.M. Gold Transaction Processing Bundle.

Contractor: ***IBM Global Services*** (DABL01-03-A-0002)

Ordering Expires: 30 Sep 05

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Microsoft Products

Microsoft Database Products - See information provided under Office Systems below.

Oracle (DEAL-O)

Oracle Products - Provides Oracle database and application software licenses, support, training and consulting services. Inventory exists for Navy customers, contact Navy Project Managers below for further details.

Contractors: ***Oracle Corp.*** (DAAB15-99-A-1002)
Northrop Grumman – authorized reseller
DLT Solutions – authorized reseller
Mythics, Inc. – authorized reseller

Ordering Expires: 30 Nov 04

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

www.it-umbrella.navy.mil

Special Note for Navy users:
On Nov. 28, 2003, the Department of the Navy Chief Information Officer (DON CIO) executed an order for an Oracle Database Enterprise License for Ashore Navy programs and offices. This agreement provides significantly reduced pricing to programs and organizations for new products, reduced logistics costs by consolidation and management of maintenance and no escalation in maintenance costs for the next 10 years.

The Oracle Navy Shore Based Enterprise License will provide all U.S. Navy shore-based employees (including all full-time or part-time active duty, reserve or civilian U.S. Navy shore-based employees, not assigned to a ship) and U.S. Navy shore-based contractors (on-site contractors or off-site contractors accessing U.S. Navy owned or leased hardware for the purposes of supporting U.S. Navy shore-based operations) the ability to use Oracle Database Licenses without the requirement of individual programs or offices having to count users. The number of licenses required by the U.S. Navy will be managed at the DON CIO level. In accordance with the DFAR Supplement Subpart 208.74, if an inventory exists, new requirements must be purchased through the DoD Enterprise Software Initiative following the related procurement process.

We are currently in the consolidation phase of this enterprise license agreement scheduled to be effective Oct. 1, 2004. Until that date, organizations should continue to operate in accordance with their current Oracle license agreement. If an organization's scheduled renewal is prior to Sept. 30, 2004, they will receive a prorated quote for maintenance support for the remainder of FY 2004. The intent of this prorating is to have all Navy shore-based Oracle maintenance contracts begin concurrently Oct. 1, 2004. Excess funds which result from this prorating should be reserved pending further guidance.

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/deal/oracle/oracle.shtml

Sybase (DEAL-S)

Sybase Products - Offers a full suite of software solutions designed to assist customers in achieving Information Liquidity. These solutions are focused on data management and integration, application integration, Anywhere integration, and vertical process integration, development and management. Specific products include but are not limited to Sybase's Enterprise Application Server, Mobile and Embedded databases, m-Business Studio, HIPAA (Health Insurance Portability and Accountability Act) and Patriot Act Compliance, PowerBuilder and a wide range of application adaptors. In addition, a Golden Disk for the Adaptive Server Enterprise (ASE) product is part of the agreement. The Enterprise portion of the BPA offers NT servers, NT seats, Unix servers, Unix seats, Linux servers and Linux seats. Software purchased under this BPA has a perpetual software license. The BPA also has exceptional pricing for other Sybase options. The savings to the government is 64 percent off GSA prices.

Contractor: ***Sybase, Inc.*** (DAAB15-99-A-1003); (800) 879-2273; (301) 896-1661

Ordering Expires: 15 Jan 08

Authorized Users: Authorized users include personnel and employees of the DoD, Reserve components (Guard and Reserve), U.S. Coast Guard when mobilized with, or attached to the DoD and nonappropriated funds instrumentalities. Also included are Intelligence Communities, including all DoD Intel Information Systems (DoDIIS) member organizations and employees. Contractors of the DoD may use this agreement to license software for performance of work on DoD projects.

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Architecture Tools

Rational Software (AVMS-R)

Rational Software - Provides IBM Rational software licenses and maintenance support for suites and point products to include IBM Rational RequisitePro, IBM Rational Rose, IBM Rational ClearCase, IBM Rational ClearQuest and IBM Rational Unified Process.

Contractor: ***immixTechnology,*** (DABL01-03-A-1006); (800) 433-5444

Ordering Expires: 25 Aug 05

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Popkin (AMS-P)

Popkin Products and Services - Includes the System Architect software license for Enterprise Modeling and add-on products including the Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Extension, which provides specific support for the U.S. Department of Defense Architecture Framework (DoDAF), Envision XML, Doors Interface and SA Simulator as well as license support, training and consulting services. Products vary from 3 to 15 percent off GSA pricing depending on dollar threshold ordered.

Contractor: ***Popkin Software & Systems, Inc.*** (DABL01-03-A-0001); (800) 732-5227, ext. 244

Ordering Expires: 13 Apr 05

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Management

CA Enterprise Management Software (C-EMS)

Computer Associates Unicenter Enterprise Management Software - Includes Security Management, Network Management, Event Management, Output Management, Storage Management, Performance Management, Problem Management, Software Delivery and Asset Management. In addition to these products there are many optional products, services and training available.

Contractor: ***Computer Associates International, Inc.*** (W91QUZ-04-A-0002); (800) 645-3042

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Citrix

Citrix - Provides a full range of Metaframe products including Secure Access Manager, Conferencing Manager, Password Manager, Access Suite & XP Presentation Server. Discounts range from 2-5 percent off GSA Schedule pricing plus spot discounts for volume purchases.

Contractor: ***Citrix Systems, Inc.*** (W91QUZ-04-A-0001);(301) 280-0809

Ordering Expires: 23 Feb 08

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Merant Products

Merant Products - Includes PVCS Change Management Software used to manage change processes in common development environments, release procedures and practices across the enterprise. All software assets can be accessed from anywhere in the enterprise. All changes can be entered, managed and tracked across mainframes, Unix or Windows platforms. The PVCS family also includes products to speed Web site development and deployment, manage enterprise content, extend PVCS to geographically dispersed teams and integrate PVCS capabilities into custom development workbenches.

Contractor: ***Northrop Grumman*** (N00104-03-A-ZE78); (703) 312-2543

Ordering Expires: 15 Jan 06

Web Link: http://www.feddata.com/schedules/navy.merant.asp

Microsoft Premier Support Services (MPS-1)

Microsoft Premier Support Services - Provides premier support packages to small and large-size organizations. The products include Technical Account Managers, Alliance Support Teams, Reactive Incidents, on-site support, Technet and MSDN subscriptions.

Contractor: ***Microsoft*** (DAAB15-02-D-1002); (960) 776-8283

Ordering Expires: 30 Jun 05

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

NetIQ

NetIQ - Provides Net IQ systems management, security management and Web analytics solutions. Products include AppManager, AppAnalyzer, Mail Marshal, Web Marshal, Vivinet voice & video products, and Vigilant Security and Management products. Discounts are 10-18 percent off GSA Schedule pricing for products and 5 percent off GSA Schedule pricing for maintenance.

Contractors: ***NetIQ Corp.*** (W91QUZ-04-A-0003)
Northrop Grumman - authorized reseller
Federal Technology Solutions, Inc. - authorized reseller

Ordering Expires: 5 May 09

Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Telelogic Products

Telelogic Products - Offers development tools and solutions which assist the user in automation in the development Life Cycle. The major products include DOORS, SYNERGY, and TAU Generation. Licenses, maintenance, training and services are available.

Contractors:
Bay State Computers, Inc. (N00104-04-A-ZF13); Small Business Disadvantaged; (301) 306-9555, ext. 117

Northrop Grumman Computing Systems, Inc. (N00104-04-A-ZF14); (240) 684-3962

Ordering Expires: 29 Jun 07

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/telelogic/telelogic.shtml

Enterprise Resource Planning

Digital Systems Group

Digital Systems Group - Provides Integrated Financial Management Information System (IFMIS) software that was designed specifically as federal financial management system software for government agencies and activities. The BPA also provides for installation, maintenance, training and professional services.

Contractor: ***Digital Systems Group, Inc.*** (N00104-04-A-ZF19); (215) 443-5178

Ordering Expires: 23 Aug 07

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_software/dsg/dsg.shtml

Oracle

Oracle - See information provided under Database Management Tools on the first page of contracts.

PeopleSoft

PeopleSoft - Provides software license, maintenance, training and installation and implementation technical support.

Contractor: ***PeopleSoft USA, Inc.*** (N00104-03-A-ZE89); (301) 581-2212

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/peoplesoft/peoplesoft.shtml

SAP

SAP Software - Provides software license, installation, implementation technical support, maintenance and training services.

Contractor: ***SAP Public Sector & Education, Inc.*** (N00104-02-A-ZE77); (202) 312-3571

Ordering Expires: Effective for term of the GSA FSS Schedule

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/sap/sap.shtml

ERP Systems Integration Services

ERP Systems

ERP Systems Integration Services - Provides the procurement of configuration, integration, installation, data conversion, training, testing, object development, interface development, business process reengineering, project management, risk management, quality assurance and other professional services for COTS software implementations. Ordering under the BPAs is decentralized and is open to all DoD activities. The BPAs offer GSA discounts from 10 percent to 20 percent. Firm fixed prices and performance-based contracting approaches are provided to facilitate more efficient buying of systems integration services. Five BPAs were competitively established against the GSA Schedule. Task orders must be competed among the five BPA holders in accordance with DFARS 208.404-70 and Section C.1.1 of the BPA. Acquisition strategies at the task order level should consider that Section 803 of the National Defense Authorization Act for 2002 requirements were satisfied by the BPA competition.

Contractors:
Accenture LLP (N00104-04-A-ZF12); (703) 947-1698
BearingPoint (N00104-04-A-ZF15); (703) 747-5442
Computer Sciences Corp. (N00104-04-A-ZF16); (856) 252-5583
Deloitte Consulting LLP (N00104-04-A-ZF17); (703) 885-6020
IBM Corp. (N00104-04-A-ZF18); (301) 803-6625

Ordering Expires: 03 May 09

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/erp_services/erp-esi.shtml

Information Assurance Tools

Network Associates, Inc.

Network Associates, Inc. (NAI) - This protection encompasses the following NAI products: VirusScan, Virex for Macintosh, VirusScan Thin Client, NetShield., NetShield for NetApp, ePolicy Orchestrator, VirusScan for Wireless, GroupShield, WebShield (software only for Solaris and SMTP for NT), and McAfee Desktop Firewall for home use only.

Contractor: ***Network Associates, Inc.*** (DCA100-02-C-4046)

Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.

Web Link: http://www.don-imit.navy.mil/esi/

Antivirus Web Links: Antivirus software available for no cost download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: http://www.cert.mil/antivirus/antivirus_index.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/antivirus_index.htm

Symantec

Symantec - This protection encompasses the following Symantec products: Symantec Client Security, Norton Antivirus for Macintosh, Symantec System Center, Symantec AntiVirus/Filtering for Domino, Symantec AntiVirus/Filtering for MS Exchange, Symantec AntiVirus Scan Engine, Symantec AntiVirus Command Line Scanner, Symantec for Personal Electronic Devices, Symantec AntiVirus for SMTP Gateway, Symantec Web Security (AV only) and support.

Contractor: ***Northrop Grumman Information Technology*** (DCA100-02-C-4049)

Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.

Web Link: http://www.don-imit.navy.mil/esi/

Antivirus Web Links: Antivirus software available for no cost download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: http://www.cert.mil/antivirus/antivirus_index.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/antivirus_index.htm

Trend Micro

Trend Micro - This protection encompasses the following Trend Micro products: InterScan Virus Wall (NT/2000, Solaris, Linux), ScanMail for Exchange (NT, Exchange 2000), TMCM/TVCS (Management Console - TMCM W/OPP srv.), PC-Cillin for Wireless, Gold Premium support contract/year (PSP), which includes six POCs.

Contractor: ***Government Technology Solutions*** (DCA100-02-C-045)

Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.

Web Link: http://www.don-imit.navy.mil/esi/

Antivirus Web Links: Antivirus software available for no cost download includes McAfee, Symantec and Trend Micro Products. These products can be downloaded by linking to either of the following Web sites:

NIPRNET site: http://www.cert.mil/antivirus/antivirus_index.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/antivirus_index.htm

Xacta

Xacta - Provides Xacta Web Certification and Accreditation (C&A) software products and consulting support. Xacta Web C&A is the first commercially available application to automate the security C&A process. The software simplifies C&A and reduces its costs by guiding users through a step-by-step process to determine risk posture and assess system and network configuration compliance with applicable regulations, standards and industry best practices, in accordance with the DITSCAP, NIACAP, NIST or DCID processes.

Contractor: ***Telos Corp.*** (F01620-03-A-8003); (703) 724-4555

Ordering Expires: 31 Jul 08

Web Link: http://esi.telos.com/contract/overview/

SecureInfo

SecureInfo - Enterprise Vulnerability Remediation (EVR) software allows IT managers the ability to automatically identify, track and correct vulnerability-related IT security material weaknesses. EVR distributes intelligence to the devices attached to the network to easily and quickly identify machines that require security fixes. With a single click of the mouse, administrators can confidently deploy patches that have been tested and approved to only the machines that need them.

Risk Management System (RMS) software offers organizations a highly automated certification and accreditation process that is customizable to meet the security requirements of enterprise networks. By utilizing extensive questionnaires, integrating specific requirements to exact standards and providing a straightforward intuitive user environment, RMS addresses the challenges experienced by C&A specialists throughout each individual phase including: security policies; test plans; security procedures; system posture and reports; and management documentation.

Contractor: ***SecureInfo Corp.*** (FA8771-04-A-0301); (210) 403-5610

Ordering Expires: 19 Mar 09

Web Link: http://www.don-imit.navy.mil/esi/

Office Systems

Adobe

Adobe Products - Provides software licenses (new and upgrade) and maintenance for numerous Adobe products, including Acrobat (Standard and Professional), Approval, Capture, Distiller, Elements, After Effects, Design Collection, Digital Video Collection, Dimensions, Frame Maker, GoLive, Illustrator, PageMaker, Photoshop and other Adobe products.

Contractors:
ASAP (N00104-03-A-ZE88); Small Business; (800) 248-2727, ext. 5303
CDW-G (N00104-03-A-ZE90); (877) 890-1330
GTSI (N00104-03-A-ZE92); (800) 942-4874, ext. 2224

Ordering Expires: 30 Sep 05

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe/adobe-ela.shtml

CAC Middleware

CAC Middleware - Provides Common Access Card middleware.

Contractors:
Datakey, Inc. (N00104-02-D-Q666) IDIQ Contract for DATAKEY products; (301) 261-9150
Spyrus, Inc. (N00104-02-D-Q669) IDIQ Contract for ROSETTA products; (408) 953-0700, ext. 155
SSP-Litronic, Inc. (N00104-02-D-Q667) IDIQ Contract for NETSIGN products; (703) 905-9700

Ordering Expires: 6 Aug 05

Web Link: http://www.it-umbrella.navy.mil/contract/middleware-esa/index-cac.shtml

Microsoft Products

Microsoft Products - Provides licenses and software assurance for desktop configurations, servers and other products. In addition, any Microsoft product available on the GSA Schedule can be added to the BPA.

Contractors:
ASAP (N00104-02-A-ZE78); Small Business; (800) 248-2727, ext. 5303
CDW-G (N00104-02-A-ZE85); (847) 968-9429
Hewlett-Packard (formerly Compaq) (N00104-02-A-ZE80); (800) 535-2563 pin 6246
Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 37010 or (512) 723-7010
GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI or (703) 502-2073
Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638 or (703) 469-3899
Softmart (N00104-02-A-ZE84); (610) 518-4000, ext. 6492 or (800) 628-9091 ext. 6928
Software House International (N00104-02-A-ZE86); Small Business Disadvantaged; (800) 477-6479 ext. 7130 or (703) 404-0484
Software Spectrum, Inc. (N00104-02-A-ZE82); (800) 862-8758 or (509) 742-2308 (OCONUS)

Ordering Expires: 30 Jun 05

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml

Netscape Products

Netscape Products - Netscape Communicator Client and a number of the Netscape Server products for use across DoD. Available for download at no cost. Customers must choose between the commercial version and the Defense Information Infrastructure Common Operating Environment (DII COE) Segmented Versions.

Licensed software products available from the Defense Information Systems Agency (DISA) are commercial versions of the software, not the segmented versions that are compliant with the DII COE standards. The segmented versions of the software are required for development and operation of applications associated with the DII COE, the Global Command and Control System (GCCS) or the Global Combat Support System (GCSS).

If your intent is to use a licensed product available for download from the DoD Download site to support development or operation of an application associated with the DII COE, GCCS or GCSS, you must go to one of the Web sites listed below to obtain the DII COE segmented version of the software. You may not use the commercial version available from the DoD Download site.

If you are not sure which version (commercial or segmented) to use, we strongly encourage you to refer to the Web sites listed below for additional information to help you to make this determination before you obtain the software from the DoD Download site.

DII COE or GCCS users: Common Operating Environment Home Page
http://disa.dtic.mil/coe

GCSS users: Global Combat Support System
http://www.disa.mil/main/prodsol/gcss.html

Contractor: ***Netscape***

Ordering Expires: Mar 05 – Download provided at no cost.

Web Link: http://dii-sw.ncr.disa.mil/Del/netlic.html

Operating Systems

Novell

Novell Products - Provides master license agreement for all Novell products, including NetWare, GroupWise and ZenWorks.

Contractor: ***ASAP Software*** (N00039-98-A-9002); Small business; (800) 883-7413

Ordering Expires: 31 Mar 07

Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/novell/novell.shtml

Sun (SSTEW)

SUN Support - Sun Support Total Enterprise Warranty (SSTEW) offers extended warranty, maintenance, education and professional services for all Sun Microsystems products. The maintenance covered in this contract includes flexible and comprehensive hardware and software support ranging from basic to mission critical services. Maintenance covered includes Sun Spectrum Platinum, Gold, Silver, Bronze, hardware only and software only support programs.

Contractor: ***Dynamic Systems*** (DCA200-02-A-5011)

Ordering Expires: Dependent on GSA Schedule until 2011

Web Link: http://www.ditco.disa.mil/hq/contracts/sstewchar.asp

Section 508 Tools

HiSoftware 508 Tools

HiSoftware Section 508 Web Developer Correction Tools - Includes AccRepair (StandAlone Edition), AccRepair for Microsoft FrontPage AccVerify for Microsoft FrontPage and AccVerify Server. Also includes consulting and training support services.

Contractor: ***HiSoftware, DLT Solutions, Inc.*** (N00104-01-A-Q570); Small Business; (888) 223-7083 or (703) 773-1194

Ordering Expires: 15 Aug 07

Web Link: http://www.it-umbrella.navy.mil/contract/508/dlt/dlt.shtml

Warranty: IAW GSA Schedule. Additional warranty and maintenance options available. Acquisition, Contracting and Technical fee included in all BLINS.

ViViD Contracts
N68939-97-D-0040
Contractor: Avaya Incorporated
N68939-97-D-0041
Contractor: General Dynamics

ViViD provides digital switching systems, cable plant components, communications and telecommunications equipment and services required to engineer, maintain, operate and modernize base level and ships afloat information infrastructure. This includes pier side connectivity and afloat infrastructure with purchase, lease and lease-to-own options. Outsourcing is also available. Awarded to:

Avaya Incorporated (N68939-97-D-0040); (888) VIVID4U or (888) 848-4348. Avaya also provides local access and local usage services

General Dynamics (N68939-97-D-0041); (888) 483-8831

Modifications

Latest contract modifications are available at http://www.it-umbrella.navy.mil

Ordering Information

Ordering Expires:
26 Jul 05 for all CLINs/SCLINs
26 Jul 07 for Support Services and Spare Parts

Authorized users: DoD and U.S. Coast Guard

Warranty: Four years after government acceptance. Exceptions are original equipment manufacturer (OEM) warranties on catalog items.

Acquisition, Contracting & Technical Fee: Included in all CLINs/SCLINs

Direct Ordering to Contractor

Web Link: http://www.it-umbrella.navy.mil/contract/vivid/vivid.shtml

TAC Solutions BPAs
Listed Below

TAC Solutions provides PCs, notebooks, workstations, servers, networking equipment and all related equipment and services necessary to provide a completely integrated solution. BPAs have been awarded to the following:

Control Concepts (N68939-97-A-0001); (800) 922-9259

Dell (N68939-97-A-0011); (800) 727-1100, ext. 61973

GTSI (N68939-96-A-0006); (800) 999-4874, ext. 2104

Hewlett-Packard (formerly Compaq) (N68939-96-A-0005); (800) 727-5472, ext. 15515

Hewlett-Packard (N68939-97-A-0006); (800) 352-3276, ext. 8288

Ordering Expires:
Control Concepts: 03 May 07 (includes two one-year options)
Dell: 31 Mar 05 (includes two one-year options)
GTSI: 1 Apr 05 (includes two one-year options)
Hewlett-Packard (formerly Compaq): 8 Oct 05 (includes two one-year options)
Hewlett-Packard: 28 Oct 05 (includes two one-year options)

Authorized Users: DON, U.S. Coast Guard, DoD and other federal agencies with prior approval.

Warranty: IAW GSA Schedule. Additional warranty options available.

Web Links

Control Concepts
http://www.it-umbrella.navy.mil/contract/tac-solutions/cc/cc.shtml

Dell
http://www.it-umbrella.navy.mil/contract/tac-solutions/dell/dell.shtml

GTSI
http://www.it-umbrella.navy.mil/contract/tac-solutions/gtsi/gtsi.shtml

Hewlett-Packard (formerly Compaq)
http://www.it-umbrella.navy.mil/contract/tac-solutions/compaq/compaq.shtml

Hewlett-Packard
http://www.it-umbrella.navy.mil/contract/tac-solutions/hp/hp.shtml

Department of the Navy Enterprise Solutions BPA
Navy Contract: N68939-97-A-0008

The Department of the Navy Enterprise Solutions (DON ES) BPA provides a wide range of technical services, specially structured to meet tactical requirements, including worldwide logistical support, integration and engineering services (including rugged solutions), hardware, software and network communications solutions. DON ES has one BPA.

Computer Sciences Corp. (N68939-97-A-0008); (619) 225-2412; Awarded 7 May 97; Ordering expires 31 Mar 06, with two one year options

Authorized Users: All DoD, federal agencies and U.S. Coast Guard.

Web Link: http://www.it-umbrella.navy.mil/contract/don-es/csc.shtml

Information Technology Support Services BPAs

Listed Below

The Information Technology Support Services (ITSS) BPAs provide a wide range of IT support services such as networks, Web development, communications, training, systems engineering, integration, consultant services, programming, analysis and planning. ITSS has four BPAs. They have been awarded to:

Lockheed Martin (N68939-97-A-0017); (240) 725-5950; Awarded 1 Jul 97; Ordering expires 30 Jun 05, with two one-year options

Northrop Grumman Information Technology (N68939-97-A-0018); (703) 413-1084; Awarded 1 Jul 97; Ordering expires 11 Feb 05, with two one-year options

SAIC (N68939-97-A-0020); (703) 676-2388; Awarded 1 Jul 97; Ordering expires 30 Jun 05, with two one-year options

TDS (Small Business) (N00039-98-A-3008); (619) 224-1100; Awarded 15 Jul 98; Ordering expires 14 Jul 05, with two one-year options

Authorized Users: All DoD, federal agencies and U.S. Coast Guard

Web Links

Lockheed Martin
http://www.it-umbrella.navy.mil/contract/itss/lockheed/itss-lockheed.shtml

Northrop Grumman IT
http://www.it-umbrella.navy.mil/contract/itss/northrop/itss-northrop.shtml

SAIC
http://www.it-umbrella.navy.mil/contract/itss/saic/itss-saic.shtml

TDS
http://www.it-umbrella.navy.mil/contract/itss/tds/itss-tds.shtml

Research and Advisory BPAs

Listed Below

Research and Advisory Services BPAs provide unlimited access to telephone inquiry support, access to research via Web sites and analyst support for the number of users registered. In addition, the services provide independent advice on tactical and strategic IT decisions. Advisory services provide expert advice on a broad range of technical topics and specifically focus on industry and market trends. BPA listed below.

Gartner Group (N00104-03-A-ZE77); (703) 226-4815; Awarded Nov 02; one-year base period with three one-year options.

Ordering Expires:
Gartner Group: Nov 06

Authorized Users:
Gartner Group: This Navy BPA is open for ordering by all DoD components and their employees, including Reserve Components (Guard and Reserve); the U.S. Coast Guard; other government employees assigned to and working with DoD; nonappropriated funds instrumentalities of the DoD; DoD contractors authorized in accordance with the FAR and authorized Foreign Military Sales (FMS).

Web Link: http://www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml

The U.S. Army Maxi-Mini and Database (MMAD) Program

Listed Below

The MMAD Program is supported by two fully competed Indefinite Delivery Indefinite Quantity (IDIQ) contracts with IBM Global Services and GTSI Corp. The program is designed to fulfill high and medium level IT product and service requirements of DoD and other federal users by providing items to establish, modernize, upgrade, refresh and consolidate system environments. Products and manufacturers include:

	IBM Global Services	GTSI
Servers (64-bit & Itanium)	IBM, HP, Sun	Compaq, HP
Workstations	HP, Sun	Compaq, HP
Storage Systems	IBM, Sun, EMC, McData, System Upgrade, Network Appliances	HP, Compaq, EMC, RMSI, Dot Hill, Network Appliances
Networking	Cisco	Cisco, 3COM, HP, Enterasys, Foundry, Segovia

Ancillaries include network hardware items, upgrades, peripherals and software. Services include consultants, managers, analysts, engineers, programmers, administrators and trainers.

MMAD is designed to ensure the latest products and services are available in a flexible manner to meet the various requirements identified by DoD and other agencies. This flexibility includes special solution CLINs, technology insertion provisions, ODC (Other Direct Cost) provisions for ordering related non-contract items, and no dollar/ratio limitation for ordering services and hardware.

Latest product additions include Fortress Technologies, HP Overview, Remedy Websphere and DB2 Tools.

Awarded to:
GTSI Corp. (DAAB07-00-D-H251); (800) 999-GTSI
IBM Global Services-Federal (DAAB07-00-D-H252); CONUS: (866) IBM-MMAD (1-866-426-6623) OCONUS: (703) 724-3660 (Collect)

Ordering Information

Ordering: Decentralized. Any federal contracting officer may issue delivery orders directly to the contractor.

Ordering Expires:
GTSI: 25 May 06 (includes three option periods)
IBM: 19 Feb 06 (includes three option periods)

Authorized Users: DoD and other federal agencies including FMS

Warranty: 5 years or OEM options

Delivery: 35 days from date of order (50 days during surge period, August and September)

No separate acquisition, contracting and technical fees.

Web Link

GTSI and IBM: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Thanks to our customers for 16 great years!

The DON IT Umbrella Program offers a full range of IT services and solutions to meet any requirement, including software, hardware, information assurance, project management, security, engineering, training, data warehousing, consulting and research.

PROGRAM FEATURES

- *Pricing below GSA Schedule and manufacturer's retail*
- *Tens of thousands of IT products and services to choose from*
- *Pre-negotiated contracts with top IT manufacturers and resellers*
- *Meets the DOD initiative to streamline the acquisition process and provides best-priced, standards-compliant IT*
- *Convenient and flexible - order by phone, fax or online*
- *Decentralized ordering*
- *Customer support for large and small purchases*
- *The easiest acquisition solution and best prices available - anywhere*

www.it-umbrella.navy.mil

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN CHARLESTON
CHIPS MAGAZINE
9456 FOURTH AVE
NORFOLK VA 23511-2130
OFFICIAL BUSINESS

PERIODICAL
POSTAGE AND FEES PAID
SSC CHARLESTON
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988