CHIPS magazine

OCT-DEC 2005

ENGINEERING FORCENET

DEDICATED TO SHARING
INFORMATION
TECHNOLOGY
EXPERIENCE

Department of the Navy
Chief Information Officer
Mr. David Wennergren

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

Space & Naval Warfare Systems Center Charleston
Commanding Officer
Captain Cloyes R. "Red" Hoover

CHIPS magazine

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: http://www.chips.navy.mil/.

Features

"The Electronic Chart Display and Information System - Navy (ECDIS-N) is the single biggest advancement to navigation since the advent of radar."

Capt. Zdenka Willis
Deputy Navigator of the Navy

Steve Ehrler
Program Executive Officer
Information Technology

Special SPAWAR section featuring an interview with Rear Adm. Ken Slaght, Commander, Space and Naval Warfare Systems Command.

"We have aligned SPAWAR to ensure we can deliver FORCEnet capability within the Sea Power 21 vision."

Rear Adm. Kenneth D. Slaght
Commander, Space and Naval Warfare Systems Command

CHIPS Oct - Dec 2005

Volume XXIII Issue IV

On the cover. L-R: Capt. Tim Flynn, Rear Adm. Ken Slaght, Vice Adm. James McArthur, retired Vice Adm. Jerry Tuttle, Rear Adm. William Rodriguez, Rear Adm. Edward H. Deets, Mr. Dennis Bauman and the Honorable John Young. On this page: (Sept. 9, 2005) - The hospital ship, USNS Comfort in Pascagoula, Miss., assisting in Hurricane Katrina humanitarian operations. Photo by Photographer's Mate 2nd Class Michael B. Watkins.

Don't miss a single issue of CHIPS! To request extra copies or send address changes, contact CHIPS editors at chips@navy.mil or phone (757) 444-8704, DSN 564.

Editor's Notebook

The *CHIPS* and Department of the Navy Information Technology Umbrella Program staffs offer our deepest sympathy over the loss of life and property in the areas ravaged by Hurricanes Katrina and Rita. Our hearts and prayers are with you and our stricken shipmates and their families.

In response to the devastation, the military services are at the forefront of relief and recovery missions led by the Federal Emergency Management Agency (FEMA) in conjunction with the Department of Defense (DoD).

An active duty force joined the National Guard in search and rescue operations, aeromedical evacuation of critically-ill patients, medical assistance, building and repairing structures, debris-clearing, marine-salvage, damage assessment and more. There was rapid response from the USS Iwo Jima, USS Shreveport, USS Tortuga, USS Graple, USS Patuxent, USNS Comfort, Coast Guard cutters, and military aircraft and helicopters.

FEMA reported that DoD has delivered more than 24.7 million liters of water, 67 million pounds of ice and 13.6 million individually packaged rations to areas in Mississippi and Louisiana.

As of Sept. 21, 2005, DoD reported 54,426 military personnel on the ground or aboard ships supporting relief operations — 13,305 active duty and 39,037 National Guard. The recovery effort is ongoing.

Our theme for this issue is "FORCEnet Engineering," and we are proud to feature a special section on the FORCEnet chief engineer — SPAWAR. We are kicking off the section with an interview with Rear Adm. Ken Slaght, who has led SPAWAR through decisive transformational change for the last five years.

Welcome new subscribers!

Sharon Anderson

Civilian Personnel Leave Transfer Program

The Office of Personnel Management has established an emergency leave transfer program to assist civilian employees affected by Hurricane Katrina. Authorized by President Bush, the leave transfer program will permit employees to donate unused annual leave for transfer to employ ees who are adversely affected by Hurricane Katrina.

OPM's regulations on the administration of the emergency leave transfer program are available on its Web site at http://www.opm.gov/oca/leave/HTML/emerg.asp/.

OPM has set up a number for federal employees and retirees affected by the storm, 1-800-307-8298. Open 7 a.m. - 9 p.m. Central Time.

Most affected employees will be granted excused absence or receive other payments to cope with the immediate emergency. The emergency leave transfer program will be in place to assist approved leave recipi ents as the need for donated leave becomes known.

New Orleans (Sept. 24, 2005) – U.S. Navy Aviation Warfare Systems Operator 1st Class William Davis, assigned to Helicopter Anti-Submarine Squadron Light Four Eight (HSL-48), checks on a lowered search and rescue swimmer during a search and rescue mission over New Orleans. U.S. Marine Corps photo by Staff Sgt. Steven Williams.

New Orleans (Sept. 24, 2005) - U.S. Navy Builder 1st Class Daniel McKee, right, assigned to Naval Mobile Construction Battalion Four Zero (NMCB-40), hands-off a sandbag to another Seabee while repairing a levee. A 150-foot sandbag wall was completed in time to beat the high tide, protecting Plaquemine Parish residents from any further damage caused by flooding as a result of Hurricane Rita. U.S. Navy photo.

Biloxi, Miss. (Sept. 12, 2005) - U.S. Seabees assigned to Naval Mobile Construction Battalion One (NMCB-1), based out of Gulfport, Miss., organize bottled water to give to families at First Baptist Church Biloxi. The Red Cross is using the church as a distribution point for food, water and supplies to victims of Hurricane Katrina. U.S. Navy photo by Journalist Seaman Joanne De Vera.

DON CIO

Putting information to work for our people

As I write this column, another catastrophic hurricane nears landfall along our southern coastal areas, just weeks after Katrina devastated the same coastline farther east. As usual, our Sailors and Marines have stepped up to the challenge to help hurricane victims, though many are victims themselves. Reprinted in this issue of *CHIPS* is a Navy message from the Chief of Naval Operations, Adm. Michael Mullen, highlighting what our Sailors are doing to assist those impacted by Hurricane Katrina as well as the support the Department is providing to our Navy families needing assistance.

These recent events are harsh reminders of the importance of emergency preparedness, an issue that relates to all of us in the Department of the Navy (DON). Since Sept. 11, 2001, local and state governments, as well as the federal government, have been cautioning us to "be prepared." Though we usually think of such emergencies as terrorist related, the reality is that natural disasters are more likely to cause us harm than terrorist attacks. Regardless of the type of threat, the Department has been proactive in establishing processes and tools to protect our assets and people.

For example, one of our Web-enabled tools, the "DON Critical Infrastructure Protection (CIP) Program" course, includes information on continuity of operations planning within a comprehensive discussion of what constitutes effective CIP posture. The course is available to Department personnel via http://www.nko.navy.mil and http://www.marinenet.usmc.mil. Additionally, our CIP team has developed two planning guides to assist Navy and Marine Corps personnel. The "DON CIP Remediation Planning Guide" advises on recognizing, planning and executing effective remediation actions to protect critical assets against disruptive events. The "DON CIP Consequence Management Planning Guide" provides step-by-step guidance on developing and maintaining effective continuity of operations plans and procedures. Both are available in the products section of the DON CIO Web site (http://www.doncio.navy.mil).

The DON CIP initiative was established shortly after the 1998 Presidential Decision Directive 63 called for identifying and protecting critical infrastructures. Today, the DON CIP Team leads a comprehensive DON initiative to: (1) identify cyber and physical infrastructures essential to warfighting readiness and assess their vulnerability to loss from either man-made actions or natural disaster; (2) assist in remediating those vulnerabilities to acceptable levels of risk; (3) coordinate an information-sharing indications and warnings capability in order to respond effectively to imminent threats; and (4) establish integrated consequence management plans and processes to ensure the continuity of Navy and Marine Corps critical operations.

Across the Department and in our personal lives, there are opportunities to rededicate our efforts to ensure we have effective emergency plans in place.

Dave Wennergren

Special Message from the Chief of Naval Operations
Task Force Navy Family

Hurricane Katrina directly impacted an estimated 18,000 Navy families. In fact, many of the Sailors providing relief to local citizens are in need of relief themselves. Most have lost something; some have lost everything.

Throughout the crisis, even as our efforts to support the joint task force ramped up, we never lost sight of our responsibility to help Navy families get back on their feet. The Navy Personnel Command rapidly stood up an emergency call center in Millington, Tenn., to foster communications and answer questions. The number is 1-877-414-5358, and it is still active.

Naval Installations Command established community support centers at Naval Air Station (NAS) Meridian, NAS Joint Reserve Base New Orleans, Naval Station Pascagoula and Construction Battalion Center Gulfport to provide a broad range of services, including crisis intervention and spiritual counseling, housing referral, legal assistance and even basic medical care.

The Navy-Marine Corps relief society has already processed more than 4,000 cases, distributing over $1.5 million in disaster assistance funds. TRICARE dispatched additional staff to a large number of evacuee sites to provide face-to-face counseling for Katrina beneficiaries.

These are great efforts — necessary efforts — and they will continue. But we need to better organize and coordinate them. We need long-term solutions. That's why I ordered the establishment of Task Force Navy Family (TFNF). Led by Rear Adm. Bob Passmore, TFNF will conduct full spectrum community service operations to provide a rapid and coordinated return to a stable environment for our affected Navy family. That's the mission.

And when I say full spectrum, I mean it. As stipulated in naval message, CNO Washington DC 161133ZSEP2005, full spectrum community service operations will include but are not limited to: (1) Full accounting of affected Navy family members; (2) Availability of temporary housing; (3) Way ahead for permanent housing where authorized; (4) Financial assistance and counseling; (5) Return to school for children; (6) Transportation options for relocation, work and school; (7) Access to health care services; (8) Access to pastoral and family counseling services; (9) Access to child care; (10) Access to legal services, including claims support; and (11) Employment support.

Just to be clear, the Navy family consists of: Navy service members (active and Reserve, other service members assigned to Navy commands or tenants on Navy installations pending concurrence of their respective services) and their families; Navy retirees and their families; civilian employees of the Department of the Navy (DON) and their families; and may include certain extended family members (defined as parents, parents-in-law, guardians, brothers, sisters, brothers-in-law, sisters-in-law) of deceased, injured or missing Navy service members, Navy retirees or DON civilians within the joint operations area (JOA); family members in the JOA of Navy service members and civilians.

Rear Adm. Passmore is reporting directly to the Vice Chief of Naval Operations and will be supported by two deputies, Rear Adm. Robert Reilly *(military personnel issues)* and Ms. Debra Edmond *(civilian personnel issues)*. He will coordinate his efforts closely with other governmental and non-governmental agencies as appropriate, to include JTF Katrina, applicable Office of the Secretary of Defense, Navy Secretariat and Office of the Chief of Naval Operations staff, Department of Veterans Affairs, American Red Cross and the Navy Marine Corps Relief Society, just to name a few.

I want the net cast wide, and I want it hauled in often. There are people hurting out there — our people and their loved ones — and we will do all we can to alleviate their pain. I liken it to a man overboard. You shift the rudder over, go to flank speed, and pluck the Sailor out of the water. In my view, we've got nearly 45,000 people in the water right now, and we're going to pick them up.

We will need your help to do it. Whether you know someone hit hard by Katrina or not, please reach out. Give of your time and your talent to one of the many volunteer organizations contributing to the relief effort. Check on a friend. Check on a stranger. Get involved and stay involved. From this day forward, every person serving our Navy not directly impacted by the hurricane should consider themselves ADDU to TFNF. You are key members of the team.

The Navy is doing great work on the Gulf Coast. I've seen it firsthand and couldn't be more proud of the contributions we've made. But nothing we do, no matter how badly needed or sincerely appreciated it might be, is more important than caring for those who make those contributions possible in the first place.

Hurricane Katrina devastated cities and towns. It took lives. By damaging our bases in that region, it even chipped away at some of our combat capability. But it did not destroy the human spirit. It did not destroy the Navy family. No storm can wipe that out. We will stand by the Navy family as the Navy family has stood by us.

I know I can rely on your support.

Adm. Mike Mullen
Chief of Naval Operations

The CNO's message has been edited from NAVADMIN 236/05 CNO Washington DC 192346Z SEP 05.

CHIPS

Sea Warrior — a true revolution in training
Interview with Vice Admiral J. Kevin Moran
Commander, Naval Education and Training Command

Encore! Encore! When the CHIPS staff heard Vice Adm. Moran brief the Sea Warrior vision to the spellbound audience at the FORCEnet Engineering Conference in June, we had to ask the admiral if he would discuss some of the aspects of the Sea Warrior vision with CHIPS.

This interview is a follow-on to Vice Adm. Moran's interview in the Jul-Sep 2005 issue where he talked about Navy Knowledge Online serving the educational and training needs of today's Sailors.

CHIPS: What is the 5 Vector Model and what does it mean to Sailors? Can Sailors tailor it according to their career goals or is the 5VM standardized according to rating?

Vice Adm. Moran: It is flexible, and it is both standardized and tailorable. I call it the Sailor's resumé. It is a way of capturing the requirements for a position in the U.S. Navy, and it is a real resumé for a Sailor. For example, the professional vector for an electrician's mate was built by a Job Task Analysis (JTA) that asked, *'What it is this Sailor needs to know and when does he or she need to know it?'*

We worked with a company called SkillsNET® because its algorithm is linked to the Department of Labor statistics and standards. When you are done doing the JTA, you take that data and apply it to the algorithm and out comes a series of skill objects. Skill objects are simply a way of bundling knowledge, skills, abilities and training into small, manageable, chunks of human resource data.

Then you lay these skill objects out at the apprentice, journeyman and master levels on the vector and take it to the community in the fleet that has responsibility for that vector, in this case the Commander of Naval Surface Forces, to get the data verified. We would then ask the admiral and his staff, *'Do you think that this is in fact the requirements for electrician's mates in terms of what they need to know and when they need to know it throughout their careers?'* When he said *'Yes,'* it became the requirement for electrician's mates.

The professional vector is the requirement. Sailors who are electrician's mates build their resumés based on the requirement. That's why I say that the 5VM is both a requirement and a real resumé. Does the Sailor have control over it? Absolutely. When Sea Warrior comes to life, the Sailor's challenge is to improve that resumé to be ready for the next position.

CHIPS: In your brief you talked about how commanding officers will have the ability to view a Sailor's 5VM to make sure he or she is the right fit for the job. Would the commander only look at the professional development vector or would personal development be viewed as well? For example, *if someone took the initiative to learn a foreign language or some other useful skill would that be of interest?*

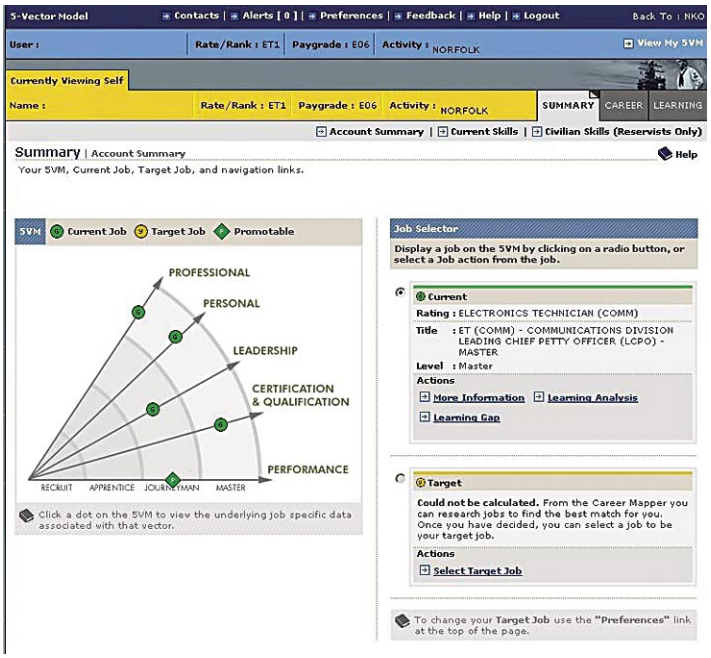
Vice Adm. Moran: Let me first say we are not quite there yet. We have two of the three databases we need to be able to do exactly what you describe in the question, and we are just starting the third one now. We need that third database for the gaining command to be able to see the requirements versus the Sailor's resumé.

Vice Adm. J. Kevin Moran at the FORCEnet Engineering Conference briefing the Sea Warrior vision June 28, 2005.

You can go on Navy Knowledge Online today and look at 5 Vector Models for Sailors, but all the 5VMs are not fully populated. We are not detailing by the 5VM yet. We have to complete that third database to do the interactive detailing you just asked about. If that third database were operational, the gaining command would be able to see that someone could, for example, speak a foreign language, although that may not be relevant for the position that individual is interested in. In the vision we have today for Sea Warrior, the gaining command will be able to look across the 5 Vectors of the model to see if the individual fits the position.

CHIPS: It appears that Sailors will need to be self-motivated to make this training approach work. Is mentoring or leadership help available through Sea Warrior to keep Sailors motivated?

Vice Adm. Moran: You are absolutely right. Right now our training and development process in the Navy is a push system. You get orders — we are pushing you to the next command — and we are pushing you through the training in the development piece. Sea Warrior is a pull system, so Sailors will be able to



Computer screen showing the 5 Vector Model module.

improve their resumés to get ready for the next position. Realistically, we know there will be folks who are like General Colin Powell and General Douglas McArthur who will stick out like a sore thumb, and mere mortals like most of us that will have some holes in our resumés, and we know there will always be those individuals that will be a bit of a challenge.

Along with building Sea Warrior, the folks at Navy Personnel Command (NPC) have been working on a new performance and mentoring process to work with Sea Warrior to help Sailors to succeed. I would defer to them for a more definitive definition of the new mentoring program they are working on, but the short answer is yes.

CHIPS: How does the 5VM impact manning?

Vice Adm. Moran: Sea Warrior will be the process to manage our Human Capital Strategy to deliver readiness so the 5 Vector Model, that resumé, will be the integral part of the entire manning process.

CHIPS: You mentioned the third database being built for interactive detailing. Are Sailors able to send a resumé to apply for job openings?

Vice Adm. Moran: Not at the current time. We need the third database to be built in order to do a gap analysis between the SkillObject™ requirements for a position and what is actually in the Sailor's resumé. The JCMS, JASS (Job Advertising Selection System) Career Management System, which is the current online interactive detailing tool, is a spiral-developed process. It is a more robust way of detailing than we've been able to do in the past, but we are still moving toward Sea Warrior functionality, so we are not there yet. We are actually in an interim step. Sailors can't compare their resumés yet, but they can compare parts of their profiles to see how well they fit a position.

CHIPS: So when Sea Warrior is fully developed will it allow Sailors more independence in making career choices?

Vice Adm. Moran: Absolutely!

CHIPS: We talked a little bit about training requirements. For example, how do you know that an E-6, Information Systems Technician on a carrier has the right skills to do the job?

Vice Adm. Moran: There are really two parts to that answer. First, you have to look at what an IT needs across the entire continuum and somewhere in that continuum are the knowledge, skills and abilities needed for that E-6 IT position on the aircraft carrier. We already have built SkillObjects to capture that requirement. Then when you actually build that position on that aircraft carrier, you move the SkillObjects with the knowledge, skills and abilities requirements in the database to define that position.

It's stubby pencil work; you build the requirement for all ITs and somewhere in there is a SkillObject for a particular chunk of knowledge, skills and abilities. You look at those positions in the fleet and move SkillObjects into that positional map so that you capture the requirement for that particular job on a particular unit. For example, a 1st class electrician's mate on a carrier would need different skills than a 1st class electrician's mate on a DDG.

CHIPS: Do you have feedback on how Sailors rate the 5VM?

Vice Adm. Moran: Yes, we have. A 3rd class master-at-arms from Sigonella, Sicily, wrote: *'I just want to say that of all the time that I spend [spent] on this site, this 5VM is just fantastic!!! It helps me tremendously! Fantastic Job! Love the new look! Thank you so much!'*

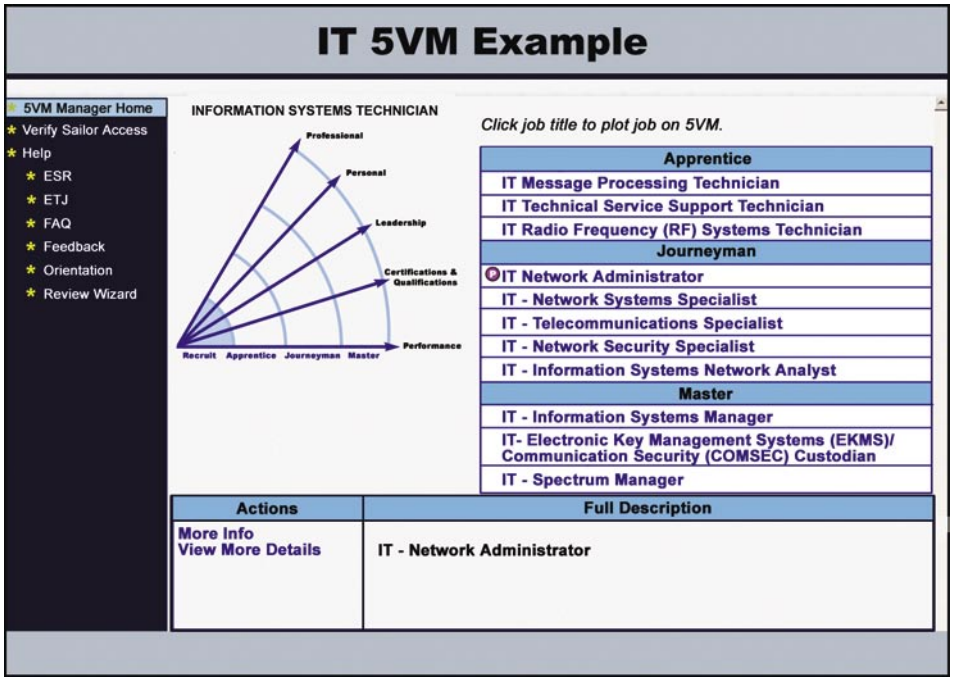
A 1st class aviation electrician's mate from the Fleet Aviation Specialized Operational Training Group (FASO) wrote: *'The new layout looks good.'*

On a recent survey question posted on Navy Knowledge Online (NKO) that had 2,337 total responses we found the following responses. Question: 'I need more information about...'
·How to use my 5VM … 44.0 percent of respondents agreed
·How the 5VM will affect advancement … 48.2 percent of respondents agreed (this was the top response).

The 5 Vector Model FAQ page has received more than 23,000 hits since January 2005. The 5VM FAQs are available on the Naval Personnel Development Command Web site at https://www.npdc.navy.mil, and are also available via NKO at https://www.nko.navy.mil.

CHIPS: Does the 5VM work the same way for all enlisted ratings?

Vice Adm. Moran: Yes, the vision is that the 5VM will work the same for all of the ratings. It is a recipe so it will work the same. We are in the process now of building the SkillObjects for officers. Right now the recipe is the same, but it could change based on our continuing work. The 5VM is also in a spiral-development process.



CHIPS: A lot of young people join the service for educational benefits. Is Sea Warrior being used as a recruiting tool?

Vice Adm. Moran: It is interesting that you mentioned that. It is not in the recruiting part of our business yet; but we are discussing it.

CHIPS: Sea Warrior is exciting to me because if a Sailor chooses to leave the Navy after four years, he or she would have marketable skills and the experience of learning from a multifaceted learning environment. Sometimes you hear a young person who has been in the service say that he or she didn't learn skills that are marketable in industry (other than military bearing and discipline).

Vice Adm. Moran: You're right. I think it will resonate well on the deckplate and in the fleet. I think it will resonate well as a marketing tool; although that is just my opinion at this point. We really are going to give Sailors a resumé when they leave the service. That 5VM, that electronic training jacket (ETJ) will be their resumé.

We are already beginning some of the basic steps at the recruiting level even though we aren't marketing it. We have given everyone a Navy Knowledge Online account that has raised their hand and taken the oath. The Navy has a delayed entry program, which means that there is a waiting period until recruits are sent to boot camp. Sometimes that wait is substantial, so while they are waiting we have given them an NKO account.

What we eventually want to do is push content to them through NKO so they can be learning. What they add to their resumés early in their career may be something that we won't have to deliver later on in the training pipeline. For instance, we have begun the process of understanding, in some of our aviation ratings, where individuals are going earlier in the selection process. So for those in the delayed entry program using NKO, we could do something like: *'Mr. Smith, welcome to the U.S. Navy. We understand that yesterday you raised your hand and took the oath. Welcome to the greatest Navy the world has ever seen. We understand that you are going to be a jet mechanic, and that you are going to be assigned to the F-18 squadron in Oceana, Va. Here is Oceana, why don't you take a virtual tour of Virginia Beach and see one of the nicest vacation areas on the East Coast. And by the way, this is an F-18. By the time you report to boot camp we expect you to have all the parts of the F-18 engine memorized.'*

So we can deliver content to somebody who has yet to begin official training. Everything he or she can remember about those parts and the location of those parts we won't have to deliver later in the pipeline. That's the vision for Sea Warrior.

CHIPS: You want to keep recruits engaged so they will maintain that level of excitement about joining the Navy during the delayed entry period.

Vice Adm. Moran: Absolutely. It makes better use of their time and saves us time and helps us roll out the training more efficiently and effectively. The money we save by using this early training can be used for other things.

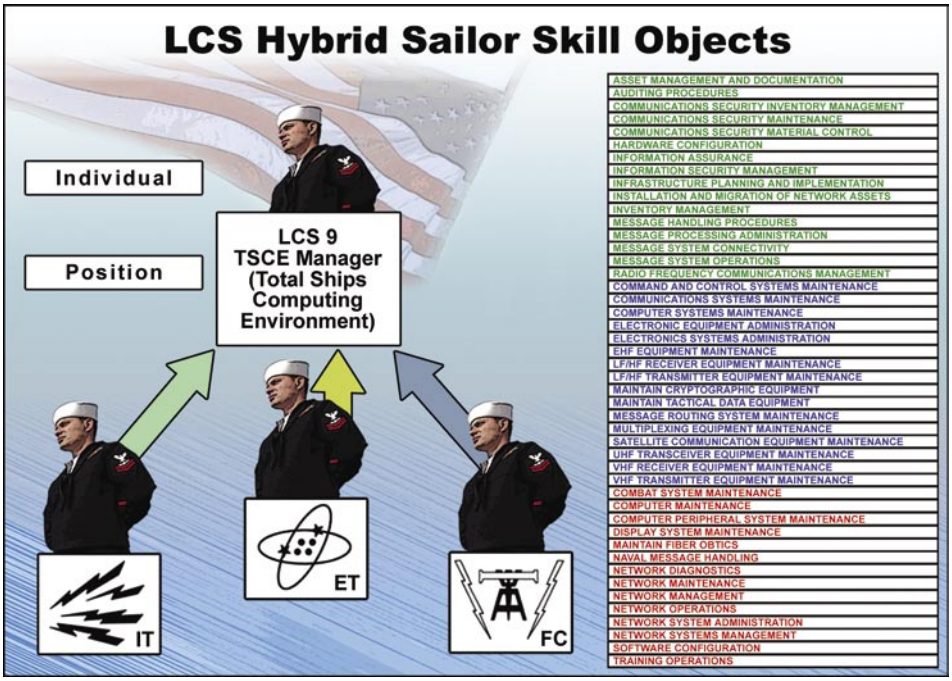
CHIPS: What is the mix of Sailor training now? For example, how much training is done in schoolhouses, online, on-the-job and self-instruction?

Vice Adm. Moran: We have converted about 36 percent of our "A" school training to online courses of instruction, and we are continuing to convert more. As of July 2005 approximately 12,000 Sailors have completed some online training, and they have completed that training in about half the time it used to take. We have 52 percent of our Sailors under instruction at "A" schools using online courses.

CHIPS: Can you talk about the hybrid Sailor and the impact it will have on training?

Vice Adm. Moran: It will certainly be different because what we are doing is developing a Sailor differently. The training will be basically the same, but we are picking different parts of the training to deliver to different Sailors. Because of the SkillObjects we know what skills they will need, but who we deliver them to is the issue with the hybrid Sailor. Under the old way, we would deliver all IT SkillObjects to ITs; we would deliver all jet mechanic SkillObjects to jet mechanics. In the future, we will be delivering IT SkillObjects not only to ITs, but to other ratings in order to better fit an individual for a position. Since we are more effectively utilizing our manpower, we can then optimally man our units.

This is the concept we are using right now to prepare the crew for the Littoral Combat Ship. We are continuing our examination of the hybrid Sailor model for other parts of the Navy as well. So



the methodology that we used to build the crew for the Littoral Combat Ship we are now beta testing in an F-18 squadron to see what it shows us about how to man that squadron. What we learn from this effort will determine what else we do with that model.

CHIPS: A smaller fighting force could mean less opportunity for advancement. The data you collect in the 5VM could be used as a rating approach to a performance-based system to reward top performers. Is Navy looking at different ways to create incentives for top performers?

Vice Adm. Moran: What you are getting into now is the Navy's Human Capital Strategy, which you will be able to lay on top of this recipe to build incentive packages. Capt. Scott Van Buskirk [now Rear Adm. Buskirk] is working the Navy's Human Capital Strategy for the Chief of Naval Operations. What they come up with remains to be seen. But clearly, you can see how this recipe can be used in terms of compensation and other human resources tools to tailor the force.

CHIPS: Is Sea Warrior technology flexible enough to continue to evolve?

Vice Adm. Moran: There are a couple answers to that question. One of the challenges we will have is technology. To stay flexible and relevant, we will have to have governance over these databases to change the data that links to the requirements. Then we in the training and education business must be able to change content in our school houses in order to deliver the knowledge, skills and abilities needed by the Sailor going to key positions that effect readiness.

Commander, Fleet Forces Command is working on the governance that we will have to lay over the top of these databases. Common things like who can make changes and when can changes be made are critical issues. Then you'll need an IT system that can cover the vision. The IT system needs to be robust, it needs to be ubiquitous, and it needs to be able to scale.

We are on a journey, and we are still in the crawling stage, but there is a lot of stuff coming together. What I'm working on is building the foundation, getting the databases built and trying to get my hands around the challenges of building an IT system capable of meeting the vision. Then the CNO will decide what Navy Human Capital Strategy to lay on top of this Sea Warrior architecture.

CHIPS: In your previous interview we talked about the NKO portal. Is the intent for Sailors to "live" in that enclave to do their work?

Vice Adm. Moran: Clearly, there is a lot of daily work that will not be in the NKO environment. The vision is that NKO is linked to a reach back tool that will help a Sailor do his or her job in terms of troubleshooting and reach back to technical assistance. We partnered with Distance Support, a program run by the Naval Sea Systems Command, because the Sea Warrior vision fits nicely within the Distance Support program.

When we get a new weapons system in the Navy, we also get a technical pub and training program. We would like that from day one to be delivered in a format that we can put into our metadata library and use as a tool to deliver content in the schoolhouse or online as a product that helps Sailors trouble-shoot equipment and ensures that they are looking at the same piece of content they saw back in the schoolhouse.

In terms of the workday, I'm always concerned about how much we can fit into a standard workday. The vision for this self-improvement was not to give us a 10-hour workday and go home and do six hours of homework. We want to get this vision into a Sailor's workday. We know that some hard-chargers will do that extra work and it's OK, but for us mere mortals, we have to fit this in the standard workday. We are trying to understand the complexity of this issue. We have done some work on a couple of ships trying to understand how much we can fit in with this kind of a vision.

CHIPS: I was going to ask how Sailors would be able to fit this responsibility in with all the operational duties they have.

Vice Adm. Moran: It is not just workload, you have to have the devices available, and they have to be linked to the content. Then it is a policy decision on how you fit it into the workday. When you do settle the policy piece, then you think about how many devices of what kind do we need for the ships so that each Sailor has access to do what we just talked about. It's an important issue that we need to come to grips with. But even if I get all of this 30 or 40 percent right, you won't recognize the United States Navy. It is that dynamic of a vision. CHIPS

INTERVIEW WITH CAPTAIN ZDENKA WILLIS DEPUTY NAVIGATOR OF THE NAVY (CNO-N7/CN)

On July 26, the Navy announced a revolutionary change to the traditional paper chart method of navigation that has been used by the surface and submarine fleet for more than 50 years. The Navy will go to an all-digital nautical navigation system by October 2009. Under the Electronic Chart Display and Information System - Navy (ECDIS-N), the Navy expects to increase safety, accuracy, reliability and accountability during deployments.

The ECDIS-N system interfaces with the ship's Global Positioning System receivers and other navigation sensors to give the ship's watchstanders a computerized real-time view of the ship's position and movement on an electronic-chart display. It also provides an automated capability for route planning and Digital Nautical Chart® correction to include the latest "Notice to Mariners" information.

CHIPS asked the deputy navigator of the Navy, Capt. Zdenka Willis, to explain the features of ECDIS-N and its impact on the Navy's warfighting mission.

CHIPS: Why have you called ECDIS-N, "the single biggest advancement to navigation since the advent of radar."

Capt. Willis: ECDIS-N, in conjunction with the Global Positioning System (GPS) and Digital Nautical Chart, provides superior navigation capabilities using an interactive computer system. For instance, in traditional navigation there is a time delay between taking a navigational position, plotting it on a chart and comparing it to the planned route. During this time the ship is normally moving, so the plot represents where the ship was at the time the position was taken, not where it currently is. But ECDIS-N, using a secure GPS connection, instantaneously updates and displays the ship's position. In a dangerous combat situation, or even a crowded seaway, this can provide a huge advantage.

ECDIS-N will also increase accuracy. A majority of navigational errors are human in origin. The most common mistakes are made in adding, subtracting and manually plotting the position on a chart. ECDIS-N will greatly enhance the safety of navigating at sea. Another common problem that affects safety is the difficulty in manually updating paper charts with new information and ensuring that the ship's chart inventory is current. ECDIS-N allows automated updating of the digital charts, via Net download or mailed compact discs. This will significantly decrease the tedious workload of correcting charts.

One of the most powerful tools of ECDIS-N systems is the automatic grounding avoidance feature found in route planning and route monitoring. Automatic grounding avoidance correlates the ship's position, draft and safety ellipse with the chart and generates alarms if the system detects potential hazards along the ship's track. The system also provides a full set of alarms if the system is malfunctioning.

CHIPS: What is revolutionary about ECDIS-N?

Capt. Willis: The most important aspect of this system is the integration of the GPS and other positional sensors, with radar and 'smart' charting databases to provide a continuous plot of where the ship is, any hazards to that ship and the location of other vessels in the area. GPS is a significant advancement, but without ECDIS-N, a petty officer would read the GPS position, go to a chart and plot the position, then figure out where the ship is

Deputy Navigator of the Navy, Capt. Zdenka Willis, in her office at the U.S. Naval Observatory in northwest Washington, D.C. Over her shoulder is a portrait of Lt. Matthew Fontaine Maury, known as the "Pathfinder of the Seas." With his love of plotting the seas, Maury studied navigation, meteorology and currents. In 1842, Maury was named superintendent of the Depot of Charts and Instruments. The Depot of Charts and Instruments later became the U.S. Naval Observatory and, in 1844, Maury served as its first superintendent.

in relationship to the planned inertial movement of the ship. It was a time consuming process and by the time you were done a couple of minutes had passed. So when you went to the officer of the deck and said here is our position, it really wasn't your position because the ship was moving. In a tight navigation or combat situation where seconds are precious, this is automated; there is no room for error. This is the biggest change for the Navy.

CHIPS: How long has ECDIS-N been in testing?

Capt. Willis: Navy began testing ECDIS-N with Voyage Management System software on submarines and surface ships in 2003. The VMS software is Windows-based. The same software is used on commercial ships. The databases used by ECDIS-N are the Digital Nautical Chart® (DNC) and a companion product called Tactical Ocean Data (TOD). TOD provides military and classified bathymetric data required by the Navy. These are produced by

the National Geospatial-Intelligence Agency (NGA) in the DoD standard format called Vector Product Format (VPF).

The VPF is a standard format, structure and organization for large geographic databases that are based on a georelational data model and are intended for direct use (i.e., you do not need to translate the data into another format to use). VPF allows application software to read data directly from computer-readable media without prior conversion to an intermediate form. VPF uses tables and indexes that permit direct access by spatial location and thematic content and is designed to be used with any digital geographic data in vector format that can be represented using nodes, edges and faces. VPF defines the format of data objects, and the georelational data model provides a data organization within which the software can manipulate the VPF data objects.

The software then reads the DNC and TOD data, both in VPF, and displays the data to a screen, so that it looks like the paper chart that the mariner is used to seeing. There are three sets of displays within ECDIS-N, the base layer, or the minimum amount of data that must be displayed; the standard layer, looks most like the paper charts, and then mariner overlay display that allows the mariner to add additional information needed for operations.

The software has tools that allow the watchstander to adjust the display to ambient light. There is a color scheme for bright sunshine and one more suited to evening hours. There is also a night-time color scheme because the bridge of a ship is in darkened mode. A computer screen that shows a lot of white would be blinding when you look outside at the dark night. Another feature of the software allows the watchstander to turn on and off layers of information to make the presentation on the screen most useful to him or her. Most significant, is that even if the data such as the soundings are turned off, the software continues to interact with the database and sounds an alarm if there is an impending danger to the vessel.

CHIPS: Which members of the ships' crew will use ECDIS-N?

Capt. Willis: Displays are available to the commanding officer, executive officer, and all of the watchstanders on the navigation bridge and in the combat information center. All the watchstanders (enlisted and officer) will be using ECDIS-N. The navigation team, prior to getting underway, will plan the ship's route and have the route approved by the commanding officer. While underway each of the watchstanders monitors the ECDIS-N system along with the real-time situation and the mission of the vessel. If the route needs to be changed for safety or mission requirements the watchstander can easily change the ship's voyage plan to meet the emerging needs. Procedures are in place to ensure that the appropriate approvals are obtained prior to making these changes. What ECDIS-N does is to automate the planning process and by querying the smart DNC and TOD data ensures that the route planned is a safe route.

Prior to ECDIS-N, voyage planning could take weeks to days. With ECDIS-N, planning is reduced to less than five hours, changes are easy to make, and 'what if' routes can be easily explored. Everybody has the ability to access the data on the system and make a query to look at the information behind the database. For example, if you have a buoy, one can query that buoy and find out everything there is to know about it.

Earlier this year as part of a fleet-wide program to upgrade the Navy's surface ships and submarines with ECDIS-N systems, ECDIS-N was installed on the Aegis guided-missile cruiser USS Cape St. George. On the St. George, for a routine underway watch there are three individuals on the bridge. The officer of the deck has overall responsibility for the safety of the ship, and there is a conning officer (trained in ship handling) and helmsman. ECDIS-N is used by each of these watchstanders to ensure the ship safely executes its mission.

Meanwhile in the combat information center, watchstanders are responsible for executing the mission of the ship. With ECDIS-N, they no longer have to plot the ship's position, required for many tactical evolutions, but now use the ECDIS-N to understand the ship's location and voyage plan. This frees up a watchstander who previously was required to plot the ship's position, improves accuracy since everyone is on the same sheet of music and allows the watchstanders to concentrate on mission execution.

CHIPS: What effect will the ECDIS-N have on warfighting capability?

Capt. Willis: Instantaneous plots will provide a tactical advantage in a combat situation, where seconds count. But ECDIS-N also allows the ability to overlay tactical data on the display, including the ship's surface search radar plot. We call this enhanced situational awareness; that is, knowing exactly where you are, where your assets are and where the enemy is. This will not only facilitate precise navigation but also other tactical applications.

CHIPS: What are some of the other components of ECDIS-N?

Capt. Willis: Radar overlay, as mentioned earlier, ECDIS-N allows the watchstanders to 'hook' tracks on the surface search radar and overlay them onto the DNCs. This allows a ship to have better situational awareness and better ability to manage the contact picture.

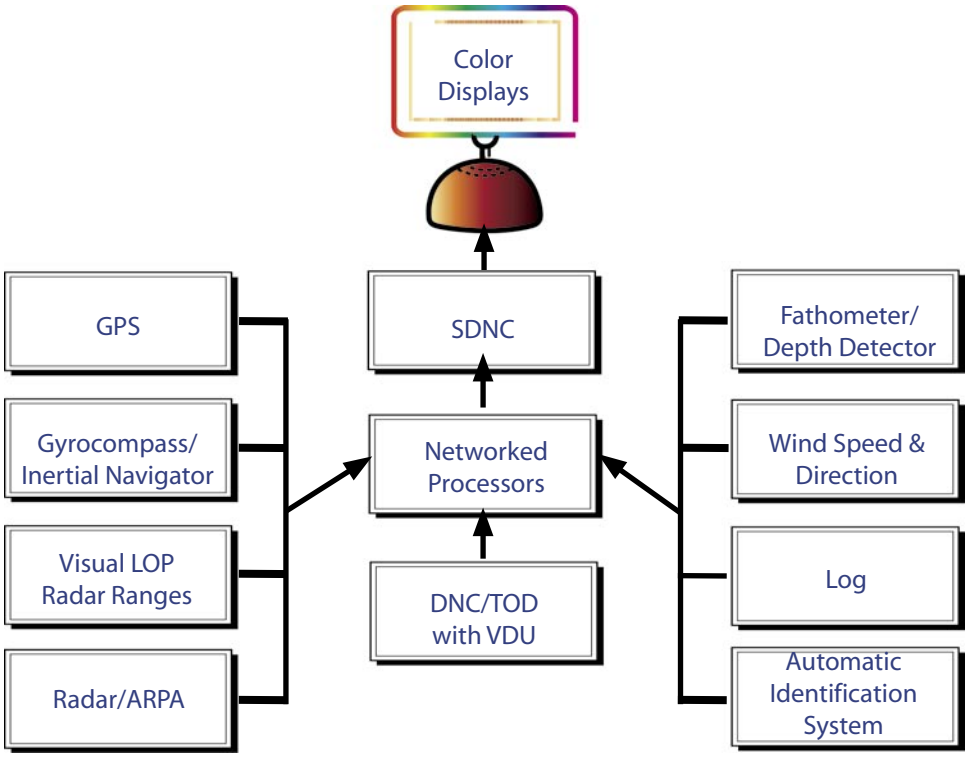
Shared awareness with the integration of digital charts, text material, alarms and danger queries, have increased the accessibility from two manually plotted displays to seven automated, interacting consoles. Aside from the manpower savings, this puts everyone on the same sheet of music on the bridge and in combat. No longer is everyone huddled around two different plots – one on the bridge and one in combat. ECDIS-N also associates visual and radar fixes with GPS positions, providing much better situational awareness in low visibility.

Playback feature is a significant step forward for training and assessment of the voyage. ECDIS-N provides what many consider a 'black box' recording for a vessel's track. In addition to the obvious legal use, it is useful for retracing a ship's course in the case of a man overboard situation and can be used as a training aid. External track steering mode allows the ship to be automatically driven without input from the ship's watchstanders. This

"ECDIS-N is the single biggest advancement to navigation since the advent of radar …. ECDIS-N, in conjunction with the Global Positioning System and Digital Nautical Chart®, provides superior navigation capabilities using an interactive computer system."

- Capt. Zdenka Willis
Deputy Navigator of the Navy

ECDIS-N COMPONENTS



functionality allows the deck watchstanders to act more as lookouts and safety observers, and it saves the Navy money by being fuel-efficient. The ECDIS-N system is constantly updating position, so precision anchorage can drive the ship to the precise anchorage point. ECDIS-N allows a user to input the swing and drag circles and activates an alarm if the anchor begins to drag or another ship is about to move within the danger circle.

The query function capability allows the navigation team to drill down for more than the normal displayed data. For instance, a Digital Nautical Chart of a harbor approach will show bathymetry and land data, approved navigation lanes, buoy and channel marker information, established landmarks for navigation fixes, hazards to navigation, etc. Hot links will allow easy access to additional information including photographic views of these features.

It also provides information about the reliability of the chart data. Ocean bottom data are critical to safe navigation, but only 60 percent of the ocean is surveyed to navigation standards and only 10 percent is surveyed to GPS standards. Many charts, by necessity, provide the only data currently available, which may be from very early or partial surveys. Because of this, it is critical for the watchstander to understand the data he or she is navigating from, and DNCs provide text information on the source and reliability of the survey data.

CHIPS: What do you mean "everyone will no longer be huddled around two different plots – one on the bridge and one in combat?"

Capt. Willis: Without ECDIS-N, petty officers on the bridge and in the combat information center are both plotting the position and trying to keep track of the entire situational picture. In the high tempo of combat operations this can lead to errors as multiple individuals are trying to read and plot the ship's position on more than one plot in two separate locations. The other watchstanders would crowd around the chart table on the bridge or in combat to execute the tactical mission or to navigate. Space was limited to those who could fit around the chart table, and the potential always exists that two different plots exist. Now with the distributive nature of ECDIS-N, the same navigation picture is displayed on multiple consoles both on the bridge and in combat — allowing everyone to see the same picture.

CHIPS: Can ECDIS-N capture uncharted data?

Capt. Willis: The technology exists within the system to accept and record input from the ship's position and fathometer systems. At this point, the fathometer information is not routinely collected. We are evaluating the feasibility and viability of this data and how we might send this data to the National Geospatial-Intelligence Agency and Naval Oceanographic Office for input to DNC and TOD databases.

The Navy has seven oceanographic survey ships that are in continuous use, basically driven 365 days a year to collect survey data. The NOAA, the National Oceanographic and Atmospheric Administration, surveys inside U.S. waters; the Navy surveys outside U.S. waters. Additionally, many other countries have survey vessels, and there are many agreements in place to share this data. Even with this global effort, only 40 percent of the world's oceans have been surveyed to hydrographic standards.

CHIPS: Why would a ship use external track steering mode?

Capt. Willis: The external track steering mode is an additional

capability for those ships that have a fully integrated bridge system. You can think of external track steering mode akin to cruise control in a car that also knows your route and keeps you on that route. It is most often used in long transits and while most of Navy operations are not of this nature, this feature can be used during transits. The St. George drove more than 900 miles to Nassau, the Bahamas in external track steering mode. This capability not only keeps the ship on track; it keeps it within 15 yards of its desired course. As well, the St. George transited in 'best fuel' mode and saved fuel on transit. This saved money and allowed the watchstanders to act more as safety observers than hands-on operators.

CHIPS: Does precision anchorage eliminate the need for a ship to request a harbor pilot to pull into port?

Capt. Willis: No. It is still standard practice for a ship that is coming into the harbor to use a harbor pilot. With the electronic systems onboard, the commanding officer and the harbor pilot will work together to bring the ship in. What ECDIS-N does is make this a much easier evolution. The harbor pilot has a lot of local knowledge.

The chart information is as good as we can have it. But on any given day in and out of port, there could be, just like on a highway, local construction that is transient in nature, so it doesn't show up on the chart. Coming into port you have traffic separation schemes on the water just as on the road. Bringing a harbor pilot onboard is a requirement of the port.

CHIPS: Is ECDIS-N based on commercial standards?

Capt. Willis: The Safety of Life at Sea (SOLAS) convention, initiated in 1914 and later administered by the U.N. International Maritime Organization (IMO), states that all commercial ships must carry up-to-date navigation charts. When the SOLAS convention was adopted, paper charts met the requirement. In November 1995, the IMO issued a resolution entitled Electronic Charting Display and Information System (ECDIS) that set the requirements that commercial vessels had to meet to safely replace paper charts with digital charts displayed on interactive computer systems.

The Navy determined that it was in our best interest to take advantage of what had been done in the civil sector. After all, ECDIS represented a 10-year worldwide effort that had been tested at sea. Further, the number of commercial SOLAS bound vessels (30,000) significantly outnumbers the Navy's inventory. Although DoD is not bound by U.N. conventions, it makes sense from both a safety and business perspective for Navy to follow the ECDIS performance standard as closely as possible.

When we reviewed the civil specifications, we determined that we could use it with only minor modifications that included: (1) Use of DoD standards for digital charting data – Digital Nautical Chart for surface operations and Tactical Ocean Data for underwater operations; (2) The ability to plot lines of positioning and to navigate the ship using dead reckoning; (3) Greater system reliability in a combat environment. These additions were made to the ECDIS resolution for the Navy variant, known as Electronic Charting Display Information System – Navy, or ECDIS-N.

CHIPS: Is there a transition plan to deploy the ECDIS-N to the fleet?

Capt. Willis: Yes, CNO (N6/7) is funding the ECDIS-N capability under several programs of record. The submarine fleet is receiving this capability under a radar upgrade program and surface ships from various modernization programs. New construction ships will receive the ECDIS-N capability as they are delivered to the fleet.

CHIPS: Who was involved in the development of the ECDIS-N?

Capt. Willis: This was a team effort that involved: the Office of the Oceanographer/Navigator of the Navy; various components of the Chief of Naval Operations staff; the Program Executive Office for Integrated Warfare Systems; the Program Executive Office for Ships; the Naval Surface Warfare Centers; the Space and Naval Warfare Systems Command; the Operational Test and Evaluation Force; and Northrop Grumman's Sperry Marine Division. This partnership extends to the fleet from the fleet commander who oversees the procedures, tactics and training, down to the commanding officer and crew of the ships and submarines who embrace the new technology.

CHIPS: Will ECDIS-N change the way navigation is taught?

Capt. Willis: Absolutely. A training plan is in place for installed systems and will be updated based on lessons learned. Overall responsibility for formal Navy school courses rests with the Naval Education and Training Command. Training of midshipman is already being provided at the U.S. Naval Academy and in a few ROTC units. In addition, Surface Warfare Officers School has incorporated ECDIS-N training into the curriculum and changes to the enlisted quartermaster school curriculum are being evaluated.

To address the needs of operational ships, training courses and associated electronic classrooms have been established at fleet concentration areas for both surface ships and submarines, with supplemental training provided as part of initial system installation or system upgrades. Changes are being incorporated into course material as lessons learned are provided by the fleet users. To make training material available to a broader audience and on an as needed basis, computer-based training is nearing completion and should be available in the near future.

CHIPS: Is ECDIS-N more difficult to learn than paper plotting?

Capt. Willis: The interface between the human and machine will make the process easier. We have found that most Sailors, with their computer backgrounds, take really quickly to the system. Understanding the basics of the system is pretty easy. The training gets to be how to be an expert on the system. We have to continue to teach basic seamanship because that does not go away. It will be awhile before we make the complete transition.

So Sailors are being taught to plot on paper, so they understand the mechanics behind what the computer is doing. I expect over the next three years that will be phased out, but we will still teach the navigation principles of how the computer is making the plots. CHIPS

Taking an Enterprise View of IT

By Steve Ehrler
Program Executive Officer for Information Technology

The Department of the Navy (DON) continues to evolve and improve how it is forging cohesive and integrated management of business and enterprise information technology. Progress is being made across the board, from the details of how to assess the utility of individual applications, to instituting new robust governance structures at the strategic level, and in between, where IT management is working to provide leadership insight, oversight and the reins to guide an agile IT enterprise.

This management effort has not been made explicit and is still evolving in response to external pressures, the need to address fiscal realities, evaluation of industry IT management models, benefit projections and coordination among key IT leadership. The enduring impetus from challenges identified through the systematic implementation of the Navy Marine Corps Intranet (NMCI) is fostering a longer view of IT management at the corporate level. Management involves more than what is probably perceived through press reports as just executing IT initiative by initiative. The purpose of this article is to provide insight into how one might view the evolving DON IT management construct.

The Challenge and the Imperative

The Government Accountability Office (GAO) has cited numerous inadequacies in IT management across the Department of Defense. Many of these reports consistently state that insufficient steps have been taken to properly support business reform DoD-wide with an integrated approach. *(See the Reference Links text box for a list of GAO reports and policy documents.)* Missing has been a clear expression of management responsibility, accountability and control over IT-related activities and resources.

In addition to the need to support business reform and solid business practices, industry also tells us there are fiscal and other benefits enabled through robust IT management. Industry experience supports recent Navy leadership messages on the need to maximize or optimize the utilization of the systems we have today. Industry data cited in Figure 1 show that rigorous IT management enables dramatic improvements in the cost-effectiveness of IT operations, ranging from 5 percent in improved software licensing, 20 to 30-percent improvement in data center cost and other cost-saving initiatives.

Given the scale of DON IT operations, potential savings could range upward of hundreds of millions of dollars annually from implementing corporate IT life-cycle management measures and approaches. DON senior leadership has issued several critical mandates recently that place an emphasis on improving cost-effectiveness, doing so through the reduction of the Department's IT base and continued improvement through solid IT management. A few examples include:

Data/Server Consolidation

- 20-30% reduction in data center operation costs[1]
- 10-20% reduction in IT infrastructure budgets during 2-year period[2]

Enterprise Asset Management

- 5% in license fees, first year, 2-3% in ensuing years; potentially 10% per year by identifying poorly managed assets[3]

Enterprise Content Management

- Most content managers and planners report a 12-month to 18-month pay back for an average midsize installation[4]

Enterprise Systems Management

- 10% savings per year[5]

[1] *AMR Data Center Consolidation*
[2] *Gartner*
[3] *Gartner - IT Management Reduce Costs and Minimize Risks*
[4] *Gartner - You Can Document ROI for Web Content Management*
[5] *Gartner - IT Management Reduce Costs and Minimize Risks*

Figure 1.

• Assistant Secretary of the Navy, Research, Development and Acquisition (ASN (RDA)) Memo – Purchase of Servers and Application Hosting Services of Nov. 12, 2004 – direction on review and approval of purchase or lease of server or application-hosting services for CONUS ashore use.

• ASN (RDA) Memo – DON Acquisition Policy on Mobile (Cellular) Phone and Data Equipment and Services of March 7, 2005 – providing for increased centralized visibility into and control of mobile communications usage.

• SECNAV Washington DC 111413Z Jan 05 (ALNAV 003/05) – SECNAV-issued naval message defining DON IT Objectives for 2005.

The evolution of the Department's perspective on IT management can be seen in the details of the Secretary of the Navy IT objective, as stated below:

I. Information Technology (IT): Transform the Enterprise Business IT functions of the Navy.

(1) Achieve 100 percent cut over to NMCI.

(2) Begin to turn off legacy networks and consolidate legacy servers.

(3) Reduce the number of applications through the Functional Area Manager's application rationalization and migration processes.

(4) Develop methods for enhanced life-cycle management and visibility of IT assets to reduce total cost of ownership.

The first several subobjectives are fairly intuitive, though not to say easy, and target completing corporate efforts previously initiated (NMCI seat rollout) and reducing and consolidating IT assets (applications, networks, servers, etc.). The fourth subobjective bears additional discussion because it calls for evolving to a Department-wide IT life-cycle management construct. What might this construct look like given what is underway today?

Models for Viewing the Whole

In response to the Secretary of the Navy IT objective, a plan was generated utilizing the basic tenets of acquisition life-cycle management. Although not inclusive of every Department initiative that would contribute to accomplishment of the objective, this framework can be used to relate many of the Department's corporate IT initiatives.

Simplistically, the life-cycle steps making up the framework are:

- *Identify what IT assets you have, and analyze for improvement.*
- *Reduce the inventory to the extent not dependent on more long-term activities, such as generating a top-down, business-to-business process for business IT mappings and improvements.*
- *Make use of real operational data, economies of scale and smart buying to support the IT asset base required.*
- *Achieve additional efficiencies in operations, including centralized management of IT assets or alternative business approaches providing for the efficient use of IT, such as IT services or commercial hosting.*
- *Support continued evolution of DON enterprise business IT through responsive management of the IT portfolio.*

How current efforts fall into these steps and the degree they are interrelated can be seen in Figure 2.

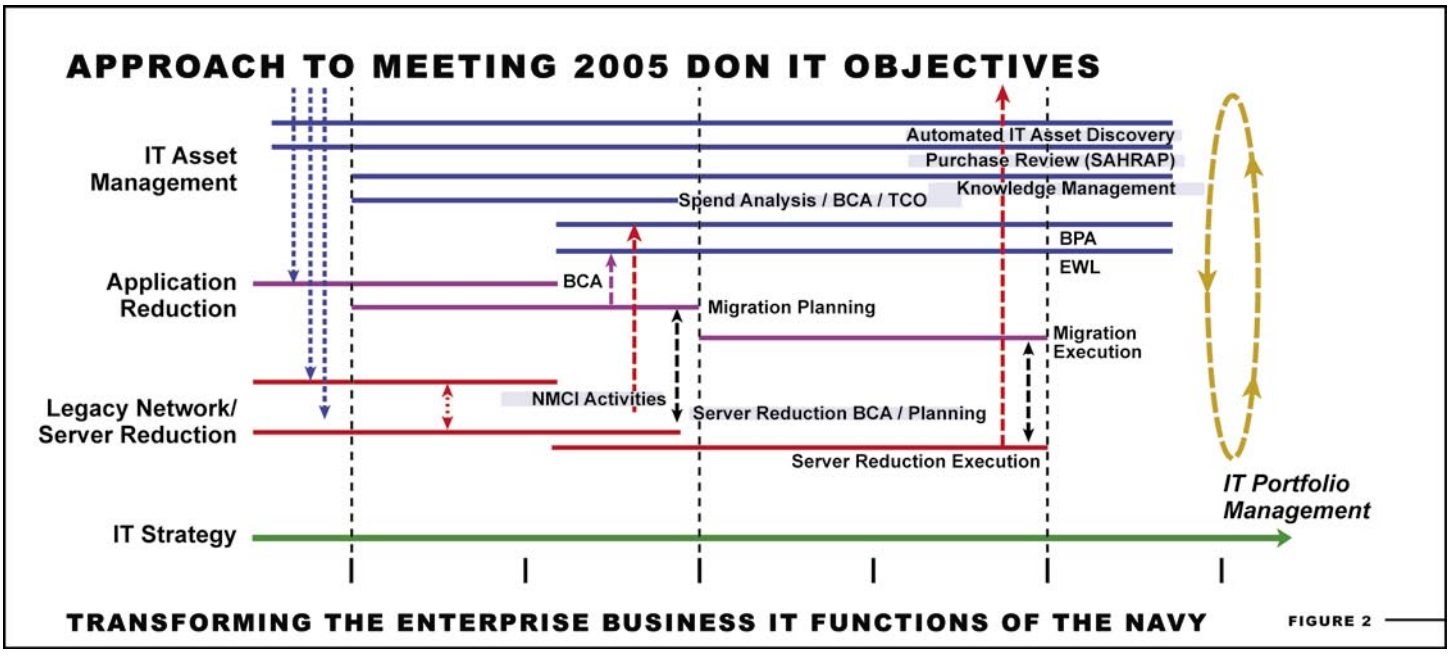
Steps of the life cycle are shown vertically on the left, and individual IT efforts under each are shown in the time lines. Although the time line is not scaled, it does give a sense of the amount of coordination required among all these activities. The vertical dashed arrow lines illustrate dependencies among the individual efforts. For example:

- *Automated asset discovery efforts currently underway will be used to assess the number and utilization of current server assets and to support a corporate business case for server consolidation.*
- *Server purchase and application-hosting reviews link hardware procurements to application reduction and approval efforts by Command Information Officers (CIO) and Functional Area Managers (FAM), thereby strengthening the Department's overall governance structure through information sharing.*
- *Application reduction, asset management and server procurement information support legacy network reduction and resolution of other issues impeding the rollout of NMCI seats.*
- *The FAM process (consisting of functional analysis, requirements setting, acquisition and portfolio management) yields requirements for enterprise-wide software licensing while asset discovery supports the scope of the required license.*

Obviously, centralized coordination of all these activities and the supporting processes are required if the promise of business and enterprise IT is to come to fruition. The need for rigor in establishing centralized management also becomes apparent when the impact of individual IT management initiatives on other management processes is shown. Let me use asset discovery mentioned above to illustrate.

Anecdotal evidence from DON efforts to estimate its application server population has shown, with remarkable consistency, that server counts from automated scanning yield about twice the number of servers in use compared with data call results, and about four times the typical offhand estimate. Although

Figure 2.



intuitively it makes sense to have the most accurate data on IT assets, the criticality becomes even clearer when one maps the dependency of other IT life-cycle processes on asset discovery information.

The next illustration, Figure 3, shows a composite view of various commonly utilized IT and IT infrastructure management standards, broken out into life-cycle phases: plan, deliver, operate, monitor and evaluate. Notice that of the 51 subelements of this IT management construct (each supported by auditable processes and procedures derived from industry standards) 23 subelements or 45 percent of the total are in whole or in part dependent upon asset discovery data (white blocks).

The take-away is that it is absolutely paramount to have accuracy and rigor in building the management framework if one expects to provide for rigorous enterprise IT management and; thereby, obtain the benefits of having an enterprise.

Challenges to Adopting an Enterprise Approach

So, besides rigor and accuracy in integration, what other challenges does the Department face in establishing business and enterprise IT management? Many issues can be cited and most are interrelated but at the top of the hit parade are arguably: scope, prioritization, centralized funding models and governance to support aggregation.

Scope

The scope of this effort is daunting:

•$3.8 billion in annual expenditures for DON IT (not including National Security Systems)

•More than 30,000 fielded applications

•An application rationalization process with over 9,000 approved or approved-with-restriction applications, each requiring some measurable migration plan and resourced execution

•Over 18.3 million Internet Protocol (IP) addresses and 285,000 network devices cataloged to date.

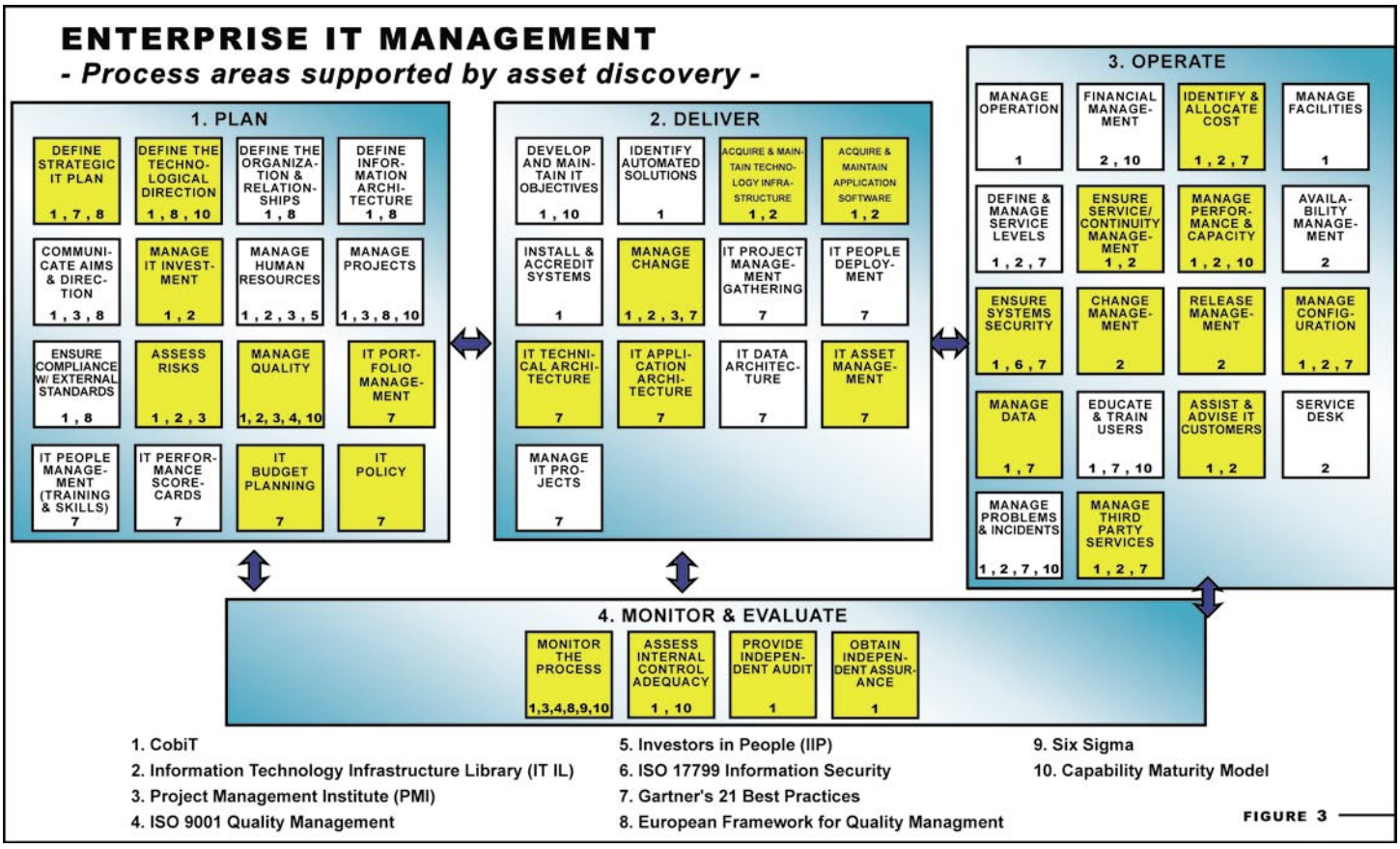
By comparison, although certainly not trivial by any stretch of the imagination, the widely discussed FORCEnet effort to baseline and assess systems is currently contending with a database of over 400 predominately C4I systems in its FORCEnet Implementation Baseline (FIBL) process, according to a July 12, 2005, press release issued by the Naval Facilities Engineering Command.

Prioritization

Placing a priority on business and enterprise IT is difficult in that it is arguably somewhat disadvantaged at the budget table in comparison to C4I systems and certainly to weapons systems.

The issue is comparing the value, of what are viewed in some camps as, "back-office" systems with "warfighting" systems — the veritable "guns and butter" comparison. Not to say that there aren't ways to do that comparison. For instance, OPNAV N6/N7 has invested heavily in modeling to assess the value balance between physical and information assets: ships, weapons and C4I. But the linkage between business systems and these models is currently tenuous at best.

Figure 3.



Program Executive Officer for Information Technology, Steve Ehrler, (left) and U.S. Senator David Vitter (R-LA) at the DON Enterprise IT Industry Symposium, New Orleans, La., Aug.10, 2005. The senator was one of several guest speakers at the conference.

Central Funding

Centralized or corporate funding of enterprise initiatives is more difficult than it might at first seem. There is a common perception that some of these initiatives are "self-funding" meaning the payback of the investment in IT consolidation is recouped from the resulting reduced costs within the same execution year. So why don't these efforts take off?

The stumbling block is with "priming the pump." There has to be funding to initiate the effort to generate the savings to pay back the investment. First, there are no IT funds that aren't already being used to support ongoing activities. Therefore, funds for new corporate initiatives have to come from existing sources. Second, even self-funding activities require cash flow to get them started — and sometimes "it ain't flowing." Third, even given the availability of funds, there is still an investment decision to be made and consideration of other priorities.

Fourth, the IT asset-owning organization accrues a return on investment (ROI) that consists of strategic and efficiency gains not easily translated into immediate cash savings. Further, real cost reduction yields little "spendable" cash and is often a fraction of the total benefits derived from the initiative. Because only spendable cash can be passed back to corporate Navy to pay back a corporate investment, centralized funding of IT initiatives in a federated environment is hard to justify.

Support for Aggregation

Lastly, the hard-working folks who have done an exceptional job keeping the Department's IT running and evolving are likely to be skeptical of anyone offering "to help," and they usually have legitimate concerns for continuity in operations that need to be addressed.

As with any change, a solid exchange on concerns, approaches and options, facilitated by an institutionalized governance structure, is required to provide the needed momentum and support to the enterprise initiative.

Reference Links

GAO, DoD Business Systems Modernization: Long-Standing Weaknesses in Enterprise Architecture Development Need to Be Addressed, GAO-05-702 (Washington, D.C., July 22, 2005). http://www.gao.gov/new.items/d05702.pdf.

GAO, DoD Business Systems Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments, GAO-04-731R (Washington, D.C., May 17, 2004). http://www.gao.gov/new.items/d04731r.pdf.

GAO, DoD Business Systems Modernization: Billions Being Invested without Adequate Oversight, GAO-05-381 (Washington, D.C., April 29, 2005). http://www.gao.gov/new.items/d05381.pdf.

GAO, DoD Business Systems Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability, GAO-04-615 (Washington, D.C. May 28, 2004). http://www.gao.gov/new.items/d04615.pdf.

GAO, High-Risk Series: An Update, GAO-05-207 (Washington, D.C., January 2005). http://www.gao.gov/new.items/d05207.pdf/.

ASN (RDA) Memorandum - Purchase of Servers and Application Hosting Services of 12 Nov 04. http://www.peo-it.navy.mil/HomePageContent/SAHRAP/ASNRDAMemo.pdf.

ASN (RDA) Memorandum - Department of the Navy Acquisition Policy on Mobile (Cellular) Phone and Data Equipment and Services of 7 Mar 05. http://www.peo-it.navy.mil/HomePageContent/Mobile_Phone_Policy/Signed_memo.pdf.

SECNAV WASHINGTON DC 111413Z Jan 05 (ALNAV 003/05), Department of the Navy Objectives for 2005. http://www.npc.navy.mil/ReferenceLibrary/Messages/ then choose drop down menu for Message Type "ALNAVS for 2005."

"Navy's Virtual SYSCOM Transforming Business Processes: NAVAIR, NAVSEA, SPAWAR, NAVSUP, NAVFAC Team Up to Enhance Performance, Reduce Costs and Gain Efficiencies," July 12, 2005, Press Release. https://portal.navfac.navy.mil/pls/portal/APP_PAO.PRESSRELFULL_DEV_DYN.show?p_arg_names=newsid&p_arg_values=1485/.

Summary

The Department of the Navy has demonstrated aggressive, progressive leadership with initiatives such as adoption of Enterprise Resource Planning systems, infrastructure service contracts with specified performance and application, and other IT asset management. Past efforts have set the stage for establishing an enduring, effective, centralized management structure to support and guide DON IT execution in a federated manner. Business and enterprise IT management is a challenging and exciting arena. Stay tuned for further evolution! CHIPS

Interview with PEO-IT Project Director Capt. Chris Christopher

CHIPS asked Capt. Christopher to explain the significance of the Department of the Navy (DON) business information technology enterprise initiatives that are underway just a few days before the DON Enterprise IT Industry Symposium August 8 - 11, in New Orleans.

CHIPS: What is your role in the Program Executive Office-Information Technology organization?

Capt. Christopher: I have two projects under my direction, one is the Enterprise IT Asset Management Program and the other is the Department of the Navy Enterprise IT Symposium, which takes place August 8 through 11 in New Orleans. The 2005 symposium is a successor to and builds on the IT symposiums we did in 2003 and 2004. Those focused on the Navy Marine Corps Intranet, which was appropriate, since the NMCI was the first big step in implementing the Navy's decision to start moving away from a locally owned, locally managed and operated IT inventory, and toward an enterprise IT portfolio wherein IT assets are planned, budgeted and acquired centrally.

This direction will require a change in behavior in the Department of the Navy, where we spent the last 35 years buying IT at the base, post or station level without a lot of control or oversight from the enterprise level. DON leadership wants to turn this around and exercise much more control and make more decisions at the enterprise level. That changed behavior, in which the NMCI has played a part, is going to require a change in behavior on the part of the IT industry. Basically, industry will have to change the way they market to the Navy because we are changing the way the Department buys IT.

The industry symposium was born from the need of understanding what that future DON IT marketplace is going to look like. The first years our focus was the NMCI because NMCI was the big driver of activity in this realm. But after last year's symposium, we decided we needed to zoom out and take a look at the larger scope of all enterprise IT, of which the NMCI is a part, but certainly not the only part.

This year's symposium is taking a look at the broad range of things; how the Navy actually budgets for IT and how the Navy is going to acquire IT in the future. We are looking at industry. Large companies over the last decade have made this transition from local management to enterprise IT management. We want to reach into their successes and learn from them so the Department can make the same transition smoothly.

The industry symposiums are intended to be a dialogue. We talk and industry listens; industry talks and we listen. This annual event is a way to keep ourselves in synchronization as we move into the future and try to make the IT marketplace more efficient for us, the buyers, and the sellers.

CHIPS: Is the symposium geared more toward industry rather than government and Navy personnel?

Capt. Christopher: As I said, it is a conversation, a dialogue, between government and industry. We have had about a 60-40 split of industry and government attendees, and that seems appropriate. We hope it stays that way in the future. Vendors can understand what we are doing so they can adapt their behaviors to match ours. From our side, we can ask industry what they are doing, so we can take advantage of their lessons learned. It is also an opportunity to look at technology. Technology shouldn't be the driver, but it is important to know what is changing, what's emerging. So it is an opportunity for vendors to show us their new, cool stuff and, for us, an opportunity to tell industry what we need in the future.

CHIPS: Is it appropriate for average users to attend since they would not be involved in the executive-level decision process for acquisition or policy?

Capt. Christopher: It is highly appropriate for them to attend. They need to understand, in the same way industry needs to understand, how IT acquisition and management is changing in the DON. We haven't figured out exactly how the future is going to work. We have a sense of what the end state is, what we are driving toward, but how we get there and what happens while we are getting there is very much still up in the air.

There is important information that the average end user brings to the table that helps decision makers in the Department of the Navy and in industry. There aren't a lot of opportunities to hear these voices. It's an opportunity for an average user to sit down and have a conversation with the CIO from Sun Microsystems, for example. It's an opportunity for the end user to say these are the challenges I have, this is the way I see my mission evolving in the future. Having those kinds of conversations are very important. We certainly want the individual, average user to be there as well as the CIO and the technology officer.

CHIPS: Critics of the NMCI and centrally managed IT assets say that there is no room for an individual to make improvements.

Capt. Christopher: There is some merit in that discussion. What we need to do is figure out how to preserve space for innovation inside the context of the larger enterprise. I'm sure that we in the DON going through the first throes of this decision aren't the first to look at the different sides of this conundrum. On the one hand, we want to get those economies and efficiencies of being more centrally managed, but on the other hand keeping a space for that innovation and that new, cool stuff while making sure we are not buying ourselves into a technology straitjacket.

Entergy, for example, is one of the big corporations that

"The data from the networks we have so far [from the Enterprise IT Asset Discovery and Management project] are interesting, surprising and, in some cases, even alarming."

– Capt. Chris Christopher

made this decision. Entergy's CIO will be talking to us at the symposium. How did companies that made this decision ensure that user voices are heard? There have always been challenges to our various enterprise initiatives, and we want to look to other organizations to see how they ensured that grassroots concerns were elevated to the enterprise level and had impact on the decision process.

I always tell my daughters that while it's important to learn from your own mistakes; it's even better to learn from someone else's mistakes. So that's really what we are doing, learning from the people in other organizations and industries that are as large or close to the Navy in scope, so we can take advantage of what they did and do even better.

I am personally very interested in ensuring that there is a constant incorporation of innovation and new ideas into what we do. But how we do it is the kind of thing that I want to discuss at the symposium.

One of the things we have added this year is a whole track on venture capital and that's a good example of just the innovation problem you asked about. Venture capitalists bankroll a huge amount of the cutting-edge technology in our country. A lot is developed by large companies, but a whole lot is funded by venture capitalists, investing in something like 'Joe's Pizza & Software' as he works in his garage on a good idea that will change the IT marketplace in 18 months.

Venture capitalists expect to make money over a certain period of time, but the Navy is tied to the POM cycle, which means new money is almost always three years away, so it takes a long time to get that cutting-edge technology. The Navy budget cycle isn't aligned to the market's 18-month product cycle.

So we want to explore if there is some way for us to bridge that gap, to work with the venture capital world to get that technology into the enterprise more quickly. I don't know if there is or isn't, but this year we are going to open that discussion with key venture capitalists to see if there is some way we can get there so that new, slick technology doesn't get passé before Navy users get a crack at it. We also want to make sure the best buy is available to the Navy on that new technology.

CHIPS: Let's talk about your other program.

Capt. Christopher: That is the Enterprise IT Asset Discovery and Management project. What was interesting and not very clear when we implemented the NMCI in 2001 and 2002, is that we really didn't know or have a good understanding of what was in the Department's IT inventory. The NMCI contract is a paradigm shift; it was let as a service contract — not a stuff contract. We turn all our stuff over to the contracted company, and it sells services to us.

Part of the challenge for the DON was understanding what we had, what we were turning over, and what we were retaining. We began looking in 2001 and 2002 for something that could go out and find what was out there on our networks. We finally found it in 2003 with BDNA Corp.'s Enterprise IT Asset Management capability, which can explore the DON Internet Protocol address ranges, and discover and identify the hardware and software residing on our networks. It identifies anything that has an 'IP heartbeat' on the network, like workstations, servers, switches, routers — anything that is alive on the network. The tool is agentless, and enables scanning across all the enterprise networks from a central location.

We had been doing market research looking for something like this; so when we found it; we did some initial testing with the Marine Corps at Quantico and with the Navy at the Naval Sea Systems Command, and the results were very promising. So we looked at initiating the project for 2004. The Director of NMCI, who was at the time Rear Admiral Munns, the N6, who was Rear Admiral Zelibor at the time and the DON CIO, Dave Wennergren, all concurred that we should go forward.

In the summer of 2004, the PEO-IT agreed to execute the project, and in September a service contract was placed with BDNA Corp. to initiate the Enterprise IT Asset Discovery and Management project, an effort to actually get our arms around everything we have in our IT inventory.

The project is very interesting. What we are doing is analogous to the Lewis and Clark Expedition: We are sending our team to go out and find what's out there in the same way that Lewis and Clark were sent to discover what was in the Louisiana Purchase. The people in 'D.C.' knew the country now had this big uncharted territory, a whole lot of land, but nobody knew what it contained. So Lewis and Clark went and looked.

So we have begun scanning the DON network portfolio on a network by network basis, discovering a variety of information about the configuration of the network and what is on the network and pulling that all together into an enterprise repository. This is allowing us to draw metrics about the state of our enterprise to make the kind of important future business decisions we need to make.

CHIPS: Don't we already know what's on the NMCI?

Capt. Christopher: The current service contract covers all Naval shore networks — unclassified, non-tactical, CONUS and OCONUS, Alaska, Hawaii — both government-owned and contractor-owned networks, so it certainly includes the NMCI. It includes all networks that support the Department of the Navy. We have completed initial scanning for the Marine Corps' NMCI and legacy networks, and the Navy's NMCI network. We are making a slow march through the Navy's legacy networks.

I mentioned earlier how IT has always been acquired, managed and operated in a decentralized fashion, and we are discovering that certainly holds true in the organization and operation of our networks. Each one is a little different and each one has presented unique challenges to getting access to it and the various devices on the network itself.

The data from the networks we have so far are interesting, surprising and, in some cases, even alarming. For example, we have discovered a whole lot more Windows NT than we thought we would be finding. The large amount of Windows NT still in use has caused the DON CIO to stand up an NT Migration Working Group. Based on the data we have, we can take an enterprise approach to get us off the old NT stuff and migrated to new and supported server operating systems.

We are discovering that a single vendor has a large majority of Unix application servers on the networks that we have looked at. This suggests a couple of things. One, since we are so heavily invested in its servers, we ought to be very interested in that company's health, because we are so dependent on them; and two, since we are obviously such a good customer for them, we need to start looking at getting an enterprise price based on total ownership. All those servers were bought locally by a program manager, base, station, etc., but no one ever got a Department of the Navy price on those servers because they were all bought in relatively small lots.

As that example illustrates, when we make future enterprise IT decisions, such as, for example, server consolidation, we can make those decisions based on what we actually own and are operating, rather than estimates or data calls, which are notoriously inaccurate. BDNA's asset discovery and management capabilities enable a process that is highly accurate, rigorous, and repeatable. It enables the management of all IT assets (hardware and software) from a DON enterprise functional and financial view. The results of the scans provide visibility, analysis and accountability. Detailed analysis reveals data on utilization, standards compliance, obsolescence and possible overexposure to a certain vendor's product.

We are moving toward a monthly scheduled scan of our networks, so we have a constantly upgraded picture of what's on the networks, and also trends to see how our networks are changing. For instance, we are seeing more Linux in the environment than we thought would be there. That suggests we may need to have a Department-level policy about Linux usage. We haven't really been in a position to speak about these types of things before because we didn't have a good understanding of what was out there. As we continue to develop this portfolio inventory, it's going to allow us at every level — policy, management and acquisition — to do things smarter.

CHIPS: When you alluded to the inaccuracies of data calls, I thought of the data calls prior to implementing the NMCI. There turned out to be many more legacy systems than were reported.

Capt. Christopher: One of the things that comes at the end of my standard IT asset management briefing, is a slide with the words 'data call' with a red circle and bar over them – saying 'No more data calls' for IT asset management. We don't want to have people out there counting stuff.

Industry doesn't do business that way any more. In fact, Gartner Group says that doing a manual inventory costs $35 to $75 per device — if you hire a professional to do it for you. Using your own people could cost twice as much. If you apply that unit cost to tens of thousands of devices, and multiple data calls, you can see the impact. And a data call is a snapshot. What we are doing with an automated process is more like a stop-motion video. We can spot changes and trends, which are important to understand.

CHIPS: Data calls are a burden to the organization. They are a disruption to productivity, and in the end no one is happy with the results.

Capt. Christopher: You are completely correct. We are hoping that this is going to eliminate the necessity for data calls in most cases. We can't identify what base or building a machine is in, but almost everything about the machine physically itself we can collect, including the software. The system uses what's called 'fingerprints,' which when you think about it, is how people are positively identified. Similarly, BDNA uses fingerprints to identify hardware and software on machines by identifying unique characteristics that identify specific devices and applications.

Over time, we will develop fingerprints for all the different applications that the Navy has. We have fingerprints for virtually all the COTS applications. As we develop fingerprints for all the GOTS applications, it's going to be of great assistance to, for example, the FAMs (Functional Area Managers) to know exactly how many copies of a given software are running out there. They will be able to make decisions about what software to approve or disapprove for running on Navy networks, based on what is actually installed across the enterprise.

The FAMS can go to the IT asset management repository and look at the redundant application choices there, and really dive into a specific application to see how many users it has, for example. This analysis will help support business decisions without having to task individual people to go around and search for this information, which, again, avoids data calls which are repetitive and very expensive to do.

In summary, what we are doing with Enterprise IT Asset Discovery and Management positions the DON to make key business decisions, based on a solid, auditable understanding of the Department's IT Asset portfolio. Enterprise IT asset management gives rigor and structure to our understanding of what we really have in our IT asset inventory, and this supports rigor in all areas of IT acquisition and management.

We cannot do this with manual processes or data calls. We need the support of an automated, consistent, repeatable capability, currently being provided by BDNA. Considering the size of our IT enterprise, this process is critical to have; and having it now, we need take advantage of it and get on to the next steps. CHIPS

Air Dominance

By Air Force Lt. Gen. William M. Fraser III
Vice Commander, Air Combat Command

Air Force Lt. Gen. William M. Fraser III

Winston Churchill once said, *"There is nothing wrong with change, if it is in the right direction. To improve is to change, so to be perfect is to change often."*

Transformation is a reality; however, transformation isn't just change for change's sake, it's change in the right direction. Reality usually prompts ideas and innovation. An effective partnership between operators and industry carries ideas into true transformation.

Today's reality is that there are unique challenges facing our warfighters — some obvious — some not so obvious. If we look at where our Airmen fight, and their contributions, perhaps we can uncover some challenges that need to be addressed.

Airmen are providing air dominance over Afghanistan and Iraq, allowing us to operate in any capacity as an effective joint and coalition force with zero risk of enemy aggression from the skies. This air dominance is enabled by network-centric operations. If it flies, hovers, drops or orbits, it is part of a larger joint network that needs to be developed by us in partnership with industry — if we're going to continue air dominance into the future.

We fly combat air patrols in a different way than we did 20 years ago. Legacy bombers have become multi-role strike platforms with deadly precision. They carry versatile weapon loads in orbits over critical ground engagements and allow a level of precision never before achieved.

Who would have known that a year ago a B-1 crew would be flying a close air support (CAS) mission? This is a great example of how airpower has changed. The crew received a tasking from the CAOC (Combined Air Operations Center) to "respond to troops in contact." There was a humvee taking fire from a ridgeline in northeast Afghanistan, and there was no qualified joint terminal attack controller (JTAC) present to clear the B-1 crew to release weapons — he was 15 minutes away. The Soldiers under fire gave their coordinates, bearing and range for the enemy fire. The B-1 crew found the target with synthetic aperture radar, received clearance from the JTAC to engage, and the crew released two Joint Direct Attack Munitions (JDAM). The first JDAM destroyed the threat.

You can see how airpower has transformed. The B-1 has its origin in the Cold War, but we've transformed its employment to meet the challenges of today's combat. This is a common story across the Air Force today.

Air dominance allows more deliberate, persistent and penetrating intelligence, surveillance and reconnaissance (ISR). Joint networks enhance our capability to perform ISR. We place ISR assets where and when the joint force needs them. Airmen provide persistent, dynamic and nontraditional ISR that benefits the entire joint team.

ISR is everyone's job. This means even fighters, strike aircraft and ground units are involved in building the battlespace picture using on-board sensors connected to command and control nodes through networks.

Today's ISR is unbelievably effective and timely. In November 2004, we were fighting the battle of Fallujah II. We flew just over a 1-to-2 ISR sortie to strike sortie ratio. This means we had one ISR platform up for every two fighters. Only a year earlier, that ratio was 1-to-12. During that battle, we had aircraft orbits stacked in layers above the city.

We achieved constant, dynamic battlespace awareness which allowed a one-two punch. Air strikes hit one house holding insurgents, and then hit a second, smaller house where survivors had fled. You can see this was a level of persistent, real-time ISR that allowed instant responsiveness to ground operations.

In addition to providing air dominance, Airmen contribute expeditionary air power. Most people don't know Airmen are on the battlefield alongside Soldiers and Marines. Expeditionary Airmen are Airmen who deploy forward. Examples include engineers, communicators, surgeons and contracting troops. They are equipped with basic force-protection competencies to protect themselves and the base.

Expeditionary Combat-Airmen encompass those who, because of their missions and tasks, actively conduct operations "outside the wire" and beyond the protection of the expeditionary air base perimeter. Good examples are contingency response groups and security forces and combat convoy operators. Expeditionary Combat Airmen also perform convoy duty.

We have trained more than 2,500 Air Force transportation troops who are serving alongside Army Soldiers driving convoys. They are trained at Camp Bullis, Texas, for combat convoy duty transporting aircraft fuel, medical supplies and munitions. Airmen have been escorting convoys in Iraq since day one of Operation Iraqi Freedom.

Battlefield Airmen are the tactical air control parties (TACPs), pararescue, battlefield weather, combat control teams, special tactics officers and combat rescue officers. These Airmen directly assist, control and execute operational air and space power. They operate independent of an established air base or its defenses. They truly embody jointness and interoperability.

The perfect example of our battlefield Airmen is the TACP assigned to Army units. The Airmen who make up these groups

provide agile combat capability to prosecute air operations in a mutually-supportive environment. TACPs are more robust, mobile and survivable — they're using Stryker armored vehicles from the Army retrofitted with TACP radios and equipment. The TACP skill set is truly a joint endeavor. The Air Force is training Army officers to be JTACs at Nellis Air Force Base (AFB), Nev. There are currently six Army officers in the course.

Airmen are providing air dominance in a joint and network-centric environment. Airmen fly multi-role platforms with extremely versatile capabilities providing persistent, near real-time, nontraditional ISR that evokes rapid combat responsiveness. Airmen are fighting on the ground and in the air.

Given the current budget challenges, we're developing new and better ways to practice and train as a joint force. Distributed Mission Operations is the perfect tool for training. DMT/DMO (distributed mission training/operations) lets us build a virtual battlespace by linking simulators and live assets into a shared interactive network.

DMO allows us to integrate as a joint force without the risk and expense of flying actual sorties. We can train jointly and in combined operations. DMO extends aircraft life and seasons our pilots more rapidly. DMO also integrates ISR assets and shooters in real-time rehearsals; it enables us to create a realistic threat environment in exercises such as Joint Red Flag.

We've just completed Joint Red Flag 2005. This exercise exploited DMO to a grand scale with great success. Joint Red Flag combined three exercises into one to train like we fight: Joint Red Flag, Virtual Flag and Roving Sands. It was one of the largest distributive exercises in U.S. history.

Joint Red Flag provided training for more than 9,000 people using more than 40 different sites across the CONUS connected through DMO. It combined live, virtual and constructive training. It's basically like making movies — blending live warfighters and a virtual background of settings and scenarios. Networks and jointness were the key. This was the first Joint Red Flag integrating the Air Force, Army, Navy and Marines. It was the perfect opportunity to practice combat interoperability and interdependence.

We also pursue transformational capabilities in partnership with industry through our battlelabs. The labs are joint and transformational by nature. ACC owns three of the seven battlelabs: the Information Warfare Battlelab at Lackland AFB, Texas; Air Warfare Battlelab at Mountain Home AFB, Idaho; and the Unmanned Aerial Vehicle (UAV) Battlelab at Indian Springs, Nev., now renamed Creech AFB. They rapidly identify and prove the worth of ideas which enable and enhance joint warfighting. I'll list two of many current air warfare battlelab initiatives.

First, is the Alert Data Embedded Passive Tag (ADEPT). This is a joint endeavor with the Army. Using radars, it allows airborne platforms to identify friendly ground forces (wearing tags); it will help us to eliminate fratricide.

Second, is the Stabilized Portable Optical Target Tracking Receiver (SPOTTR). SPOTTR binoculars allow JTACs to identify precisely what ground-based and airborne lasers are targeting to verify that the designated target is the proper one. The result will be the ability to hit targets faster.

Some of our transformational capabilities are organizational. Many of you are familiar with the Air and Space Expeditionary Force (AEF) concept. Our warfighters use newly developed ideas, such as those from the battlelabs, practice new capabilities at exercises, such as Joint Red Flag, and then deploy revived and transformed every time the next AEF drum beat sounds.

Those are just some of the ways that we as warfighters have transformed our training thanks to a strong operator-industry partnership. In addition to its first look, first shot, and first kill capability, we are working to give the F/A-22 the capability to find, fix, track, target, engage and assess a moving target — putting a cursor on a target sooner.

The F/A-22 combines capabilities onto a single platform. Without a strong partnership between industry and the warfighter, it would have been impossible to transform a space-age stealthy fighter into the ultimate multi-role, peerless air dominance machine.

Industry teamed with the warfighter to give the F/A-22 supersonic SIGINT or signals intelligence. No other fighter will be able to process and collect signals like the Raptor. We developed a fighter-bomber with multiple sources of passive surveillance, a nontraditional ISR developed partly due to the powerful sensor suite on the Raptor. Because of its capability to gain fast, deep-penetrating ISR, it's the perfect complement to traditional collection platforms like the U-2, RC-135, EP-3 and AWACS (airborne warning and control system) aircraft.

Industry is improving the Raptor's capability with development of the small diameter bomb (SDB). With its 250-pound warhead and wing kit, it can fit in the internal weapons bay of the F/A-22 (and the Joint Strike Fighter) and be released 50 miles from its target. The SDB was a technological innovation born from real necessity.

Another great example of technological innovation from industry is the WDL or weapons data link. When developed fully, it will give us the ability to in-flight retarget some weapons. This means we can update target location data to our weapons as they fall and increase the probability of hitting a moving target.

Just as impressive, is that the WDL combines three radio capabilities into one: Link-16, SATCOM and UHF, and dramatically shrinks the component to fit into an Mk-series weapon. We will be able to hit a moving target, or even a target that is stationary at weapons release but attempts to escape as the weapon is in-flight.

The ROVER III or Remote Operations Video Enhanced Receiver receives data from transmitters on Predator and fighter and bomber targeting pods and displays the data to a laptop computer or other viewing device. In the future, Army patrols and Special Operations Forces will depend on ROVER-type technology to be their eyes. This technology is indeed transformational when you consider how Soldiers previously gained imagery — by e-mail at best or by runners carrying pictures in the battlefield.

The new ROVER III version allows reception from Army and Marine Corps small, tactical UAVs. In June, ROVER was used by an Air Force JTAC assigned to a Marine unit near Al Qaim, Iraq. The team was taking fire from an enemy mortar position. The JTAC and the Marines located the mortar position using ROVER and cleared the Predator UAV crew to launch a Hellfire missile to destroy the mortar site and eliminate hostile fire.

UAVs are the perfect example of how technological change supported by industry fundamentally transformed the way we do business. We used to fly many sorties and put our Airmen at extreme risk to attain imagery, signals or other intelligence. Now UAVs do a great deal of that collection and much more.

The MQ-1 Predator and MQ-9 Predator B provide us with remote and long-loiter intelligence and surveillance capabilities and allow us to strike with weapons like the Hellfire antitank missile. The RQ-4 Global Hawk is the ultimate surveillance machine. It provides a versatile sensor load (electro-optical, infrared and radar) and loiters for extremely long sorties — 24 hours-plus. The Global Hawk exploits global networks and data links.

The Joint Unmanned Combat Air System or J-UCAS is a transformational program in its infancy. J-UCAS will develop combat UAVs for suppression of enemy air defenses, electronic attack, precision strike and more.

The steady interaction among industry, defense labs and operators is the catalyst to healthy transformation — to not have it is a barrier to healthy, directional change. That directional change can't happen without continuous operator involvement with industry and well-defined transition plans to take technology from ideas all the way to deployment.

I challenge you to turn more ideas into reality for the warfighter. Let's develop dynamic, networked kinetic weapons. We still need a reliable ability to hit any moving target on the water or on land — in all weather conditions. New technology like the WDL tells us we're well on our way.

We need to develop nonkinetic weapons such as directed energy. We've learned nation building is costly; if we can deactivate a target without destroying it, we can rebuild faster and cheaper.

Balad Air Base, Iraq – Airmen 1st Class Sarah Oliver, (left), Phillip Coswell, (back left) and Joseph Oliver, process 20 mm rounds for an F-16 Fighting Falcon. They are munitions system journeymen assigned to the 332nd Expeditionary Maintenance Squadron. All three are deployed from Aviano Air Base, Italy. U.S. Air Force photo by Senior Airman Tim Beckham.

I challenge you to evolve our information operations (IO) capabilities. IO is gaining momentum. We have the Information Warfare Battlelab, a new IO range at Nellis AFB, to be used in joint exercises and a structured process for taking IO innovation to operational combat power. Information dominance is essential for combat success. This means optimizing the concepts we now use in information warfare and developing more great ideas so we stay ahead.

Compatible and interoperable networks offer one of the most important opportunities to transform. Jointness means we must have a warfighting network that is truly plug-and-play for everyone. New technologies from industry must create, update, maintain and support these networks for use by everybody and everything: fighters, bombers, tankers, reconnaissance, UAVs, space assets, CAOCs and ground forces.

It should be effortless. The last thing the warfighter needs is another black box that does something really neat, but takes a million-dollar fix to share data on a network. When a Navy F-18 shows up over Iraq, that airplane should automatically check-in, update its data, sensors and weapons from the joint network with no effort from the pilot. And when it leaves, the network should know it automatically.

The House of Representatives just passed a bill to address the increasing costs of weapon systems. That bill introduces provisions that restrict the DoD from buying immature weapon systems or developing single service weapons. I've listed some areas that outline where we need to go with transformational technology, but we obviously need to do it with cost in mind and in the spirit of jointness.

In early June near Karabilah, Iraq, Air Force F-16s dropped five GBU-12s (guided bomb units) and two GBU-38 JDAMs against armed anti-Iraqi forces hiding in small buildings in a suburb outside the city. The insurgents were engaged with U.S. Marines. The enemy threat was eliminated in a matter of minutes and there was no collateral damage.

This type of precise, timely and dominant warfare would be impossible without a strong industry-warfighter partnership that's never been more important than it is today. Agility is the key for the future force. We need to continue to transform our ability to rapidly respond so we can be successful in the future.

The success of our Airmen and the rest of our military can be seen in the faces of 53 million Afghan and Iraqi citizens — now free from tyranny — who now have the opportunity to determine their own futures. You are part of that success.

Editor's Note: Lt. Gen. Fraser's article has been edited from his remarks at AFCEA Transformation TechNet 2005, June 22, 2005. For more information about Air Combat Command go to http://www.acc.af.mil/. CHIPS

Special SPAWAR Bonus Section

RADM Kenneth D. Slaght

Interview with Rear Admiral Ken Slaght COMSPAWAR

Rear Adm. Slaght has been the hard-charging, innovative commander of the Space and Naval Warfare Systems Command for the last five years. On the eve of his retirement, Nov. 3, 2005, with 35 years of naval service, CHIPS asked the admiral to talk about some of SPAWAR's initiatives, challenges and triumphs during his command.

CHIPS: What are some of the SPAWAR achievements that you consider most important?

Rear Adm. Slaght: First and foremost has been FORCEnet becoming the central focus of everything we do. We have aligned SPAWAR to ensure we can deliver FORCEnet capability within the Sea Power 21 vision.

We have worked hard to define FORCEnet with our customers, stakeholders, the fleet and industry. The result has been dramatic in a number of areas. We have seen FORCEnet capability pay off in Operation Iraqi Freedom and Operation Enduring Freedom in Afghanistan where it enabled warfighters to conduct their missions much more effectively and efficiently than they have ever been able to do in the past. Everything from putting more Tomahawks on target because of more rapid tasking that came through a FORCEnet system to the ability to prepare and conduct missions collaboratively over FORCEnet systems.

When the former Chief of Naval Operations (CNO), Admiral Vern Clark, visited a couple of years ago, we showed him a capability called 'Composeable FORCEnet' that allowed an operator or commander to reconfigure warfighting capability on the fly. He was impressed, particularly with how the Navy could use it with some of the antisubmarine warfare (ASW) challenges it has in the Pacific fleet. I think the CNO's final comment was, 'We need that and we need it now.' Six months later it was delivered to the CTF 74 Operations Center in the Pacific fleet, ready to start performing a mission. So a capability that was very much needed and delivered in a very rapid cycle is a testament to what SPAWAR has been able to achieve in its focus on FORCEnet.

When the USNS Mercy was called to provide relief in the Far East and other areas hit by the tsunami, she needed to be upgraded with FORCEnet-like capabilities so she could perform command and control missions to support humanitarian assistance. We were able to quickly get her up to speed in support of that mission.

One of the most important areas has been a collaboration process across the Navy and up to the joint world — across all the elements that participate in delivering FORCEnet. Starting with the systems commands and the Program Executive Offices (PEO), there has been a significant effort in what is termed the Virtual SYSCOM to tie together all the elements to create FORCEnet capability. This is one of the things that we have all been very proud of: The ability to collaborate broadly across the systems commands, OPNAV and the fleet to pull together the requirements, the resourcing and the technical solutions that in the end create FORCEnet.

CHIPS: Where do you envision the Virtual SYSCOM heading in the future?

Rear Adm. Slaght: What's really evolved out of the Virtual SYSCOM is that it has become more than just a SYSCOM effort. One of the challenges we realized early on is that unlike building a ship, plane or submarine, this was a much broader exercise and collaboration. As I've said many times, it's an amazing collaborative event when you build a network. I think we can all relate to that when we look back to how the Internet evolved. It was not a single company or entity that created the Internet; it was many entities across academia, industry and government. The result of that collaboration is that there is the amazing capability that we call the Internet.

Truly, when we talk about net-centric operations and net-centric warfare, the key to creating this net-centric capability is the collaboration environment that has to take place. We started the Virtual SYSCOM within a systems commands arena where we were able to collaborate across PEOs and across all the different programs, but then we brought in systems engineers across all the systems commands and started a system of systems.

We've engaged at the SYSCOM commander level, but probably the most important level has been bringing it together under the Assistant Secretary of the Navy Research, Development and Acquisition (ASN (RDA)), Mr. John Young and what he calls his EXCOMs, his executive committees, that bring to the table all the other stakeholders for a given functional area. Mr. Young recognized the power of FORCEnet and stood up a FORCEnet EXCOM. We were able to get OPNAV and the fleet, in the form of the Naval Network Warfare Command, and Secretary Young at the table. Now you have all the parts of the triangle that create capability for the Navy. You have the fleet with its requirements and priorities, you have OPNAV with its resourcing, and then you have the acquisition community and the ability to deliver on the requirement.

The Virtual SYSCOM effort has expanded into almost a Virtual Navy in terms of bringing all the parts that must be brought together to create anything for the Navy: the fleet, OPNAV and the acquisition community. The Virtual SYSCOM will continue to be a broad effort across the Navy as part of Sea Enterprise that really addresses more than just FORCEnet. I think we will start to address more and more of the challenges of Sea Power 21, starting with the pillars — Sea Strike, Sea Basing and Sea Shield — and doing it in the kind of environment that started with FORCEnet.

CHIPS: Can you talk about the synergy between the PEO C4I and Space, PEO Space Systems and the SPAWAR Enterprise?

"It has been a pleasure working with Rear Admiral Slaght. The vital working relationship between NETWARCOM and SPAWAR has been significantly strengthened during his tour. This complementary relationship has enabled us to provide improved, consistent and more reliable service to the fleet.

Rear Admiral Slaght is a visionary leader and with him and the SPAWAR team as chief engineer for FORCEnet we have made great steps forward. These advancements will bring improved mission effectiveness and deliver on network-centric warfare and Sea Warrior."

Vice Adm. James D. McArthur Jr.
Assistant Chief of Naval Operations for Information Technology
Commander, Naval Network Warfare Command

Rear Adm. Slaght (left) with Vice Adm. James McArthur, Assistant Chief of Naval Operations for Information Technology and Commander, Naval Network Warfare Command at the FORCEnet Engineering Conference, Norfolk, Va., June 28, 2005.

Rear Adm. Slaght: It's been interesting. As you recognized, the stand up of PEO C4I and Space and PEO Space Systems has been relatively new compared to the stand up of the other PEOs in the rest of the Navy and the Department of Defense. We are newcomers and there is some good and bad news attached to that newness. There was certainly some catch up to do, but being newcomers we took a fresh look to how to create the synergy that you mentioned.

It is still a work in progress, but we have started to hit on all the cylinders that will drive FORCEnet. We've done this by creating a connection across the SPAWAR Enterprise that does the filing. When you visualize it, it's like a car radiator where you have elements that go vertical and horizontal across the organization. The vertical elements that we have, which we've always had, are the product lines: communications, sensors, ISR, business systems and so on. The horizontal parts of the radiator chart that support those product lines are where we have created the synergy. Some of those have been the traditional ones like contracting, logistics and legal, but we have added some new critical pieces to be able to create something like FORCEnet.

Systems engineering, for instance, has been integrated horizontally across the enterprise. We use resources in each of the organizational elements to support systems engineering. We have systems engineers from Code 05, the Chief Engineer, the headquarters' piece of SPAWAR, each of the PEOs and systems engineers from each of the specific functional areas in the field to really leverage the size and power of a 7,000-person organization.

In this way, we can take advantage of bringing together all the different levels of systems engineering that you need to tackle a big challenge like FORCEnet. That's been the power of the alignment effort of the last several years — the ability to work the horizontal issues across the organization to deliver, at the end of the day, a FORCEnet capability and not just a 'series of boxes.'

CHIPS: What roles do the SPAWAR Space Field Activity and National Reconnaissance Organization Group play at the enterprise level?

Rear Adm. Slaght: The Space Field Activity and the NRO Group are part of that functional product line, the vertical piece that addresses the space piece of building FORCEnet. They are the whole reason we have the name 'space' in Space and Naval Warfare Systems Command. They are the connection, not only for us, but more importantly for the Navy, into space. We recognize that space has tremendous capability for us today and into the future. It is very important for us to be engaged in all fronts for how space is going to support us and help us perform our mission in the future.

The Space Field Activity, which is basically integrated into the NRO, is that connection where we connect the dots within the Navy into space. We have most recently stood up PEO Space Systems, and it is responsible for the MUOS (Mobile User Objective System) program, which is the next generation of narrowband satellites. MUOS will consist of a space segment and multiple ground segments. These segments will provide the communications medium and services for all users. Space and ground segments will include a network of advanced narrowband satellites and the ground infrastructure necessary to manage the information network, control the satellites and interface with other systems of the Global Information Grid.

CHIPS: The first FORCEnet Engineering Conference generated phenomenal energy. The buzz in the working and general sessions was indicative of the huge success of the conference.

Rear Adm. Slaght: This conference is one of the tools that will help take the team down the field. It got industry, OPNAV and the fleet together in the room. The reason we held it in Norfolk, Va., was that we wanted to make sure we had fleet involvement. The next one will be held in San Diego, Nov. 15 through 17, so there will be a fleet-centric focus to the conferences. The conferences are designed to get all three parts of that triangle together — the acquisition community, OPNAV and the fleet — in the room with the systems engineers.

I want to emphasize all the words in the title of this conference. It's about FORCEnet, and it's about engineering FORCEnet so there is a lot of technical detail. We want to get people in the room so they can roll up their sleeves, understand the problem, contribute and have a dialogue about the problem, which is why

"Rear Admiral Slaght has been a valuable member of my team at a crucial time for the C4I community. He led the Navy to a leading position in network-centric warfare over the past few years working hard with our PEOs, to help push FORCEnet from a strategic concept to an acquisition strategy. His vision will continue to positively effect our organization long after Ken's retirement, and we're already using his strategies to design and build net-centric capability for the warfighter.

Ken excelled as the SPAWAR commander. I was particularly impressed with his introduction of the FORCEnet Implementation Baseline (FIBL). This really provided my acquisition team the opportunity to work with requirements and resource stakeholders to scrub programs for capability gaps and redundancies. I'll miss his leadership and wish him well in the future."

The Honorable John J. Young Jr.
Assistant Secretary of the Navy Research, Development and Acquisition

L-R: Mr. Dennis Bauman, PEO C4I and Space, the Honorable John J. Young Jr., ASN (RDA) and Rear Adm. Slaght.

we think it is appropriate to have two to three days to be able to do this.

I agree with you, the buzz was very positive for the first FORCEnet Engineering Conference. We are working through our feedback to make the next one even better. We are going to hold a conference every six months because this is one of the very important tools you need to have to create the collaborative environment to deliver FORCEnet.

CHIPS: I think one of the key success factors was that the conference attracted fleet operators.

Rear Adm. Slaght: I appreciate that feedback. It was especially great having Vice Admiral Kevin Moran, Commander, Naval Education and Training Command, there. I'm not sure that people had connected the Sea Warrior initiative with FORCEnet. Yet, when you think about it, if we are really thinking net-centric all these initiatives connect in the end. So it was great to see Vice Admiral Moran beginning to brighten light bulbs with all that is going on with Sea Warrior and how much Sea Warrior is going to rely on the connections of FORCEnet to be able to deliver on the Navy Human Capital Strategy. Admiral Moran's presentation was a very powerful element of the conference.

CHIPS: What is the status of the FORCEnet Implementation Baseline?

Rear Adm. Slaght: The FIBL is now institutionalized within the Navy. I'll take that up a notch. On July 14, Secretary Young signed the Department of the Navy Policy for Acquisition Community Support to Implement FORCEnet Capabilities. I think this will be one of the cornerstone documents that is going to take us forward. Keep in mind that we have these three elements of the triangle — OPNAV, the fleet and acquisition community — and each one of those now has a directive, something in writing.

This is important because early on many people kept asking the question, what is FORCEnet? One of the important parts of defining FORCEnet is getting things in writing at the appropriate level, so people can point to how the parts of the Navy enterprise define FORCEnet and intend to implement it.

So each of the elements in the triangle now have a defining document for FORCEnet, starting with the fleet and NETWARCOM. NETWARCOM issued the FORCEnet conceptual document, which defines the operational framework for FORCEnet in the future. OPNAV has created what it calls the FORCEnet check-off compliance list, which it will use as it develops the NCDP, the Naval Capability Development Process that is going to feed the POM.

OPNAV is using that compliance check-off list to certify systems from an operational and, to some extent, technical view so that there is a screen that says if the Navy is going to implement and fund these programs in the future that they fit the bill for FORCEnet compliance. For those of us on the acquisition side, the most important one is the document that Secretary Young signed in July. That document, put together by his chief engineer Carl Siel, gets into the detail that will help us define our work plan for the next several years, maybe even longer, to take FORCEnet forward.

There is specific direction in that document for the FORCEnet Chief Engineer, which is SPAWAR. Specifically, the document says, 'In collaboration with ASN (RDA) CHENG, Marine Corps Systems Command and other stakeholders, the FORCEnet chief engineer will develop and manage the FORCEnet database and associated processes ensuring efficiency, effectiveness and minimal workload on the program managers.'

The FIBL is the database that the document refers to, so now we have a tasking to go do it. But there is also a caution there that says this has to be valuable, efficient, and we have to carefully manage it so that it is not another whole series of redundant data calls on the program managers. The FIBL has been institutionalized. We are ready to take it to the next level, which is to baseline FORCEnet for the future, which will then become a valuable authoritative data set to be used by the Secretary as he goes through milestone reviews. It will feed the NCDP and the FORCEnet compliance part that OPNAV will use as it develops the POM cycle.

It will truly become the authoritative database and, if we do it right, not only will it start to answer Navy questions about the

capabilities that are going to comprise FORCEnet, but then we can start to feed it into OSD and the joint arena to answer GIG compliance questions.

CHIPS: How have the requirements for FORCEnet been gathered?

Rear Adm. Slaght: This is a very intricate dance that takes place between NETWARCOM and OPNAV. Going back to the triangle, NETWARCOM, as the fleet representative for FORCEnet, sets the stage for requirements and priorities, and they work closely with OPNAV to create the roadmap for those requirements and priorities. As that is developed, it helps prioritize what we need to evaluate as part of the NCDP, so we collect the data and evaluate each of the elements of FORCEnet.

We can look at projecting capabilities into the future like space-based radars. As these technologies evolve into the future, we ask how many nodes and what kind of packages should the Navy request the Air Force to put up in the sky, so we can perform our mission of maritime domain awareness, i.e., keeping track of all maritime shipping worldwide as part of the global war on terror. That intricate synchronization has to take place between the fleet and fleet sponsors.

The other aspect is the Sea Trial process led by NETWARCOM in the FORCEnet arena and driven by the fleet commanders and the Naval Warfare Development Command. Using Sea Trial to experiment and prototype capabilities from industry, putting these in the hands of the warfighter and getting warfighter feedback, then using real data from that process helps us quantify which capabilities we should accelerate and support. The key challenge is the golden rule that has not changed: There are not infinite resources to create each of the pillars of Sea Power 21, including FORCEnet. You have to measure and compare across all the warfighting capabilities to decide what is the right balance, what is the right mix.

OPNAV has brought in a number of modeling tools that has allowed us, for the first time, to balance the right mix across Navy resources. How many nodes to the network do we need, i.e., planes, ships, submarines, and how much of the network do we need to protect. So when the POM is created, we have maximized the spread of our limited resources to the maximum extent possible. That is the real key to how the information is gathered and validated making sure that each of the principals — the fleet, OPNAV and the acquisition community — have input. Then input is rolled into a modeling process to compare. As we used to say in the old days, how do you measure a pound of C4I? I think we have truly gotten our hands around that for the first time.

CHIPS: How would you rate the importance of business IT to the success of FORCEnet?

Rear Adm. Slaght: I think it is absolutely critical. From day one, we have talked about a FORCEnet continuum. I would describe it this way: There is a business end to FORCEnet. I don't think our early thinking about FORCEnet really addressed this; it was always about warfighting systems and C4I at sea. But business IT and tactical systems are all very intricately interrelated. For example, the Sea Warrior piece that we talked about earlier with Vice Admiral Moran is a great example of that business IT part. It literally impacts the Navy's ability to perform its mission by using FORCEnet tools to help evolve the warfighter in conjunction with the Human Capital Strategy in real-time in terms of where we want to be in the future.

So the business end of FORCEnet — the infrastructure, NMCI, and all the software systems that train and educate our Sailors, pay our Sailors, and the logistics that support the warfighting systems — all those business elements are going to be an integral part of FORCEnet in the future. FORCEnet has to be a universal network. There may be subsets and layers, but in the end the goal is this global network, the GIG. We should all be marching toward this goal.

There is another end of the continuum from business to the more pointed end of the spear and warfighting, and that is the combat systems. This will be another challenge for FORCEnet in the future. How do we align and integrate across the warfighting systems, literally into fire control loops. There is a significant effort going on right now in the combat systems arena called open architecture. I think originally when FORCEnet was defined people just equated it to C4I. It is much broader than that from a technical view; it includes business systems and combat systems to some extent. It's a Venn diagram; it doesn't include all combat systems, but it certainly includes a great part of them.

Keep in mind that the center of FORCEnet is the warfighter. It's not unlike what Vice Admiral Jerry Tuttle came up with when we started to evolve C4I when he talked about the construct of Copernicus that put the warfighter in the center of the universe. This is another step in that direction that keeps us focused on keeping the warfighter in the center of this equation. That is the reason why when the acronym was created for FORCEnet, the 'n' for the network has always been a small n because it's not so much about the technology as it is about the warfighter.

CHIPS: Any predictions for the future of C4I?

Rear Adm. Slaght: Without question C4I is a critical area that will continue to grow for the Navy, DoD and this nation. We're starting to connect more and more to homeland defense and security. So as the Navy wrestles with the Quadrennial Defense Review and the global war on terror, in addition to major combat operations and balancing force posture to achieve success, there's incredible leverage you get from this capability we call FORCEnet.

CHIPS: Any predictions for the future of Ken Slaght, Rear Admiral, U.S. Navy (retired)?

Rear Adm. Slaght: Well, it's been an incredible ride, an incredible journey. I hope to continue to contribute in some way, maybe on the industry side of the equation. I really find this business extraordinarily rewarding with lots of challenges to be addressed. I would like to continue to contribute in some way because it's one of the most important things we're doing for the Navy and this nation. CHIPS

Interview with Captain Tim Flynn

The Space and Naval Warfare Systems Center San Diego is the U.S. Navy's research, development, test and evaluation, engineering and fleet support center for command, control and communication systems and ocean surveillance. SSC San Diego provides information resources to support the joint warfighter in mission execution and force protection.

CHIPS asked Capt. Flynn, former commanding officer of SSC San Diego and acting SPAWAR vice commander to talk about the exciting mission of SSC San Diego.

Capt. Flynn has been nominated for appointment to the rank of rear admiral.

CHIPS: Can you talk about some of the initiatives SSC San Diego has in building FORCEnet?

Capt. Flynn: SPAWAR's instantiation of FORCEnet is to use a composeable approach to net-centric publishing and subscribing in a services-oriented architecture. The architecture is based on open, commercial standards. The operational impact of FORCEnet is the ability to support changing mission needs, to increase a commander's situational awareness, to give the commander the ability to 'geo-collaborate.'

The ability to actively share information and collaborate on a map (what we call 'map chat') is one of the unique capabilities that reduces the decision-cycle time for 'speed to decision,' and provides the commander a reconfigurable decision center. Many command centers are going to be around for years. As the missions flex and commanders change, the current commander will want to be able to reconfigure his or her command center.

In delivering FORCEnet capabilities, SSC San Diego's primary contribution is Composeable FORCEnet or 'CFn,' which basically provides the capability or services for the warfighter to obtain information from local and remote locations through a 'publish and subscribe' mechanism.

Users are not constrained to just C2 (command and control) information that their units develop nor are they constrained to depending on other users sending them information. CFn enables information to be organized into knowledge then shared with other local or remote users through map chat collaboration. Map chat also enables virtual teaming. It started in the fleet as text chat. Now taken to the next level, map chat enables geospatial collaboration.

We also provided Web patron services through which CFn translates data from multiple sources into a format that is accessible to any user on that domain. This will enable integration of multiple data types into a single view, including data sources that are outside the domain of the WebCOP or GCCS-M (Global Command and Control System—Maritime) program. You can actually subscribe to PC IMAT (Personal Computer Interactive Multi-Sensor Analysis Training) or AREPS (Advanced Refractive Effects Prediction System) or GALE Lite for the signal intelligence piece of the puzzle.

Soon METOC (weather) information will be available as a subscriber service. Users sitting at existing workspaces, such as the theater ASW (antisubmarine warfare) watch floor at CTF-74 (Commander, Task Force 74) are now able to view data from non-GCCS-M systems and other data sources via a browser with a CFn plug-in. These are the key capabilities. There are three views. First, there is the geospatial view, a three-dimensional view of the objectified area of interest to the combatant commander. There is a temporal view which allows commanders to archive, replay and reconstruct much like a videocassette recorder.

There is also the functional view. This is the Knowledge Web or the portal piece. Included within the client capabilities is the ability to collaborate by map chat. From the services side, the capabilities include an information broker, a translation service, a bandwidth management capability and intelligent agent technologies that allow commanders to actually launch intelligent agents to data-mine and bring back information of interest. There are also some legacy system interfaces.

With Composeable FORCEnet, you can use databases that are not normally accessible. This is done through coding or scripts that allow users to access databases by publishing XML (Extensible Mark-up Language). In this way, the XML tags can be subscribed to over the Internet in a CFn environment.

CHIPS: Has the FORCEnet vision changed ocean and littoral surveillance and reconnaissance systems and technology?

Capt. Flynn: It is changing as we speak. SSC San Diego has been in ocean surveillance work for more than 40 years. Maritime C4ISR is the biggest part of our mission. In the area of ocean surveillance, the focus for decades has been on off-board and distributed sensors and systems. SSC San Diego's expertise includes building sensors, and — most importantly — integrating those sensors across multiple platforms that operate from the seabed to space. This is not only for the Navy but for the joint warfighter and other agencies. The FORCEnet vision is not platform-centric. Distributed sensors and capabilities, including unmanned systems and manned platforms, are all nodes on the network.

We see an increased emphasis in networking ISR systems across domains (undersea, surface, air and space) and also across

functional areas (such as acoustics, electromagnetic, radar, electro-optical and infrared). From a technology point of view, this has driven an increased emphasis in areas such as intelligence fusion and correlation. We have also seen an increased emphasis in rapidly deployable systems. For example, on the Littoral Combat Ship, you will see the ADS (Advanced Deployable System) as part of its lightweight off-board sensor capability.

FORCEnet requires adherence to an open architecture with commercial standards that will enable surveillance and reconnaissance systems to publish their information so that users can easily subscribe to that information. This will enable the warfighter to get the right information where it is needed most. It will also enable the insertion of new technology more rapidly without the massive reengineering and integration efforts that we have experienced in the past.

CFn enables the warfighter to 'plug-and-play' or as Admiral John Nathman (Commander, U.S. Fleet Forces Command and Commander, U.S. Atlantic Fleet) called it, 'plug-and-fight.' We are actively supporting the development of the FORCEnet architecture for ocean surveillance and other mission areas.

CHIPS: CHIPS published an article about the Composeable FORCEnet Human Systems Integration (CFnHSI) Laboratory (http://www.chips.navy.mil/archives/04_summer/Web_pages/FORCEnet.htm) last year. What are some of the new developments in HSI?

Capt. Flynn: Human Systems Integration work is core to the development of every C4ISR capability. Our design work is less about technology insertion and more about first understanding the operator's processes end-to-end, then working alongside the operator to reengineer processes and leverage state-of-the-art technologies to enhance situational awareness and enable 'speed to decision.'

You really see the return on investment when you first evaluate the processes, eliminate unnecessary workload, then exploit the best of breed technology. The biggest cost-driver across the design-life of a ship is the cost of manpower. We see the same thing in command centers. There is a real need to minimize the workload on the operator. This will enable a corresponding reduction in the crew size. Our human factors and knowledge management scientists are at the forefront of this for Navy and joint C4ISR.

CHIPS: Is San Diego doing any work with IPv6?

Capt. Flynn: We have been working on IPv6 since 2001, conducting research as a result of our major involvement in coalition interoperability. In 2001, the Communications and Information Systems Department was tasked by ONR (Office of Naval Research) to lead an international group of scientists and engineers from the United Kingdom, France, Germany, Canada and Italy to investigate international interoperability with IPv6 networks. Our program is called the Interoperable Networks for Secure Communications Group.

As part of this program, SSC San Diego has participated in IPv6 demonstrations with NATO countries. We have extensive experience with solving IPv6/IPv4 heterogeneous wide-area network problems.

SSC San Diego employees working in the Composeable FORCEnet Human Systems Integration (CFnHSI) Laboratory.

Our tasking includes work in: architectures, quality of service, routing, mobility, management, security, etc. Some of our recent IPv6 tasks include next generation IP naming and addressing and work on the Global Information Grid (GIG). Recently, in support of SPAWAR 05 Office of the Chief Engineer, which is the Navy's lead for IPv6 transitions, we are now writing the Navy's part of the Department of Defense Transition Plan to IPv6.

At SSC San Diego, Dr. Albert Legaspi is leading a cross-SPAWAR team to develop the Navy's IPv6 technical transition strategy. This team has participated in many DoD working groups and has had a major influence on DoD's IPv6 transition strategy. Lastly, we currently have two of our scientists, Dan Greene and Robert Kolesar, developing IPv6 test tools for OSD (Office of the Secretary of Defense).

CHIPS: Last summer CHIPS published an article about NETWARS and network warfare simulation (http://www.chips.navy.mil/archives/04_summer/Web_pages/NETWARS.htm). Are there any new developments in this area?

Capt. Flynn: Network Warfare Simulation or NETWARS is the Navy's networking, modeling and simulation tool based on optimized networking, populated with validated communications and network models from all the services. The complex set of NETWARS tools is used to accept the new network architectures and determine performance of any modifications made or proposed to existing networks.

Recently, NETWARS has been federated with the Naval Simulation System (NSS). This is a high-level tool that assumes limited communication models. It is used to determine courses of action, campaign directions, experiments, etc.

With the fidelity of NETWARS communications, coupled with the high-level campaign direction of NSS, the Navy has a much better

"FORCEnet is really the focus, not only of SSC San Diego but also of the SPAWAR enterprise. FORCEnet is not just Navy — it's joint."

– Capt. Tim Flynn

understanding of how to allocate its resources for the highest return-on-investment. Some NETWARS tools are now being used by OPNAV N71.

CHIPS: What are some of the ways that SSC San Diego has contributed to fleet readiness?

Capt. Flynn: SSC San Diego contributes to the fleet, specifically readiness, in three areas. Our Distance Support Office is our first line of support. It manages requests for technical assistance very similar to a customer support office at a product manufacturer.

These requests for assistance come in from around the world by message, e-mail and sometimes telephone. So far this year, our office has responded to more than 7,200 distance support requests. If a shipboard or shore facility equipment casualty can be resolved by this office, money does not have to be spent to fly a technician or team of technicians to the affected ship or shore facility. In the event a technical issue cannot be resolved by e-mail or telephone, one of our technicians will have to be sent to correct the problem.

Our Fleet Support Office manages the technical support effort that requires sending technicians to the ship or shore facility. So far this year, this office has provided more than 170 on-site technical assists worldwide. The third part is the Installation Management Office, which manages the installation of C4ISR systems on ships, submarines and Navy shore facilities both in CONUS and Hawaii, Japan and Guam. The office will complete between 400 and 500 C4ISR system installations and upgrades each year.

CHIPS: Is there any other SSC San Diego project you would like to talk about?

Capt. Flynn: FORCEnet is really the focus, not only of SSC San Diego but also of the SPAWAR enterprise. FORCEnet is not just Navy — it's joint. Efforts are ongoing to align with the Air Force's C2 Constellation and eventually with the Army's LandWarNet. It is the Navy's implementation of the GIG. All the services are converging on the GIG.

FORCEnet is in line with U.S. Joint Forces Command's Joint Command and Control (JC2) vision. We fully expect FORCEnet to expand to include our coalition partners and other agencies. We have some challenges to overcome with multi-level security, joint information domain exchange and the ability to move data from NIPRNET to SIPRNET to JWICS (Joint Worldwide Intelligence Communications System).

Composeable FORCEnet is currently deployed in 7th Fleet. Last year, CFn was installed on the watch floor of CTF-74 in Yokosuka, Japan. Installations at Kadena and Misawa and aboard USS Blue Ridge and USS Kitty Hawk followed.

This August, SSC San Diego is installing CFn aboard USS Ronald Reagan. For the first time, CFn, installed as part of GCCS-M, will be able to subscribe to combat systems data from the ASW module. In our Interactive Multi-Sensor Analysis Training Lab, Fleet ASW Command just completed training the Destroyer Squadron Seven watchstanders on their new CFn capabilities. With PEO C4I and Space and PEO Integrated Warfare Systems, SSC San Diego is breaking new ground here.

Thus far, CFn has primarily (and appropriately) focused on the warfighter, particularly in the ASW mission area. Because of its composeable nature, CFn can also transform other warfighting mission areas as well as warfighter support areas, such as logistics, training, manpower, disaster recovery, etc. The potential is far-reaching. CHIPS

Captain Tim Flynn is the former commanding officer of the Space and Naval Warfare Systems Center, San Diego. He has been nominated for appointment to the rank of rear admiral.

Capt. Tim Flynn received his commission upon graduating from the U.S. Naval Academy with a Bachelor of Science degree in marine engineering in 1979 and completed nuclear propulsion plant operator training in 1980. He was later awarded Master of Science degrees in National Security Affairs (technical intelligence) and mechanical engineering from the Naval Postgraduate School.

Captain Flynn's sea assignments include service as damage control assistant in USS Truxtun (CGN 35), First Lieutenant and Reactor Training Assistant in USS Arkansas (CGN 41), operations officer in USS Paul F. Foster (DD 964), chief engineer in USS Texas (CGN 39), and chief engineer in USS Harry S. Truman (CVN 75). He qualified as a Surface Warfare Officer and was designated as "Qualified for Command at Sea." He became an Engineering Duty Officer in 1992.

His shore assignments include special projects officer at Joint Task Force Five; assistant project officer for New Construction Aircraft Carriers at Supervisor of Shipbuilding, Conversion and Repair, Newport News, Va.; assistant program manager for In-Service Carriers, including Smart Carrier, at Aircraft Carrier Program Office (PMS 312) at Naval Sea Systems Command, Washington, D.C.; and Director of Shore C4ISR Installations; followed by executive assistant at Space and Naval Warfare Systems Command, San Diego. He assumed command of Space and Naval Warfare Systems Center, San Diego, on 2 May 2002.

Capt. Flynn is the acting SPAWAR vice commander.

His decorations include the Meritorious Service Medal (four awards), the Joint Commendation Medal, the Navy Achievement Medal (three awards) and multiple unit commendations.

The FORCEnet Engineering Conference

Synchronizing FORCEnet's Engineering Future

By Sharon Anderson and Steve Davis

The first FORCEnet Engineering Conference provided a dynamic collaborative environment for FORCEnet stakeholders and the naval engineering communities to exchange information and "synchronize FORCEnet engineering efforts." The event, sponsored by the Space and Naval Warfare Systems Command, was held in Norfolk, Va., June 28-30. The conference gave working-level engineers and fleet operators an opportunity to meet with program officials, resource sponsors and users in a structured forum.

According to Craig Madsen, technical director for SPAWAR's Office of the Chief Engineer, the conference came at just the right time. *"It became apparent that in the absence of engineering-level guidance from the government, many private activities were attempting to fill the void in engineering detail with their own version of what the Navy means,"* Madsen said. *"This conference and the anticipated follow-on conferences in the FORCEnet engineering series are designed to fill that engineering detail void with an official government position."*

The conference format was a mix of general sessions with featured speakers, panel discussions and working sessions covering all the components of FORCEnet. Broad topic areas included: the FORCEnet Toolset; Engineering-Services-Oriented Architecture Environment; Communications/Networks; Experimentation and Demonstration; Combat Systems/Hull, Mechanical & Electrical Equipment; Implementation/Test/Certifications; Aviation Systems Assessments; and Command and Control (C2).

"The goals of the initial conference were specifically to bring together and identify the 'FORCEnet engineering community' with the anticipation that this collective community could then get on with the business of realizing the FORCEnet vision," Madsen said.

Representatives from the engineering communities for C2; communications; networks; business information technology; intelligence, surveillance and reconnaissance; information operations; assessment and experimentation; human systems integration; and architecture/certification engaged in spirited discussions in the working sessions regarding the future of FORCEnet.

"Individual working sessions were structured to allow a variety of topics and viewpoints to be presented. Flag sessions were created to allow the senior level FORCEnet vision to be provided to the audience of engineers and program managers. All the major acquisition commands were there to participate," Madsen said.

A significant indicator of the conference's success was the strong participation from fleet operators. Their enthusiasm was evident in their interaction with colleagues and Navy and Department of Defense leadership during the working and general sessions.

SPAWAR Chief Engineer Rear Adm. William Rodriguez, with executive assistant Tricia Ward, welcomes attendees to the FORCEnet Engineering Conference, held June 28-30, 2005.

Retired Vice Adm. Jerry Tuttle and Vice Adm. J. Kevin Moran, Commander, Naval Education and Training Command.

"The conference was very informative and there were so many great working sessions going on simultaneously that it was hard to choose which ones to attend. At future conferences I look forward to hearing about implementation success stories from many of the ideas discussed," said Cmdr. Danelle Barrett, communications officer on the Carrier Strike Group Twelve staff.

Working sessions were led by subject matter experts, program office representatives and resource sponsors. SPAWAR Commander Rear Adm. Ken Slaght said he wanted attendees to "roll up their sleeves" and work on moving FORCEnet forward. Attendees from fleet operators right up to the Department level were eager to do just that.

"Capt. David Prater (PMW 780, PEO C4I and Space) and his team's brief on the Battlespace Networking Initiative was detailed, informative and clear. It demonstrated that we can work across all the Navy systems commands," said Capt. Scot Miller, commanding officer of the Navy Center for Tactical Systems Interoperability (NCTSI), San Diego, Calif.

Another conference success factor was the enthusiastic mix of leadership, users and engineers represented from the Naval Sea Systems Command, Naval Air Systems Command, Naval Network Warfare Command, Marine Corps Systems Command, Defense Information Systems Agency, Program Executive Officer (PEO) Information Technology, PEO C4I and Space, SPAWAR and OPNAV.

"The right people are in the room," said Rick Paquin, head of SPAWAR Systems Center Charleston FORCEnet Engineering and Technology Support Branch.

In addition to Rear Adm. Slaght, other featured speakers included Rear Adm. William Rodriguez, SPAWAR Chief Engineer; Vice Adm. J. Kevin Moran, Commander, Naval Education and Training Command; Vice Adm. James D. McArthur Jr., Assistant Chief of Naval Operations for Information Technology and Commander, NETWARCOM; and Mr. David Weddell representing OPNAV N6/7 – Warfare Requirements and Programs. Moderators were retired Vice Adm. Jerry Tuttle and retired Rear Adm. Bob Nutwell.

"I was impressed with the number of top leadership who came out. They were very approachable when I asked for clarification or additional information concerning anything from the fundamentals to the functional concept of FORCEnet," said Sandy Mieczkowski, manager for SPAWAR Systems Center (SSC) Charleston Tidewater Node of the FORCEnet Composeable Environment.

Participants agreed that the conference gave them a clearer idea of FORCEnet's design, purpose and impact. Information from the FORCEnet Toolset session included technical and operational views to help the user as well as the engineering community visualize what FORCEnet capabilities the Navy envisions.

The toolset includes a collaborative environment, called the Naval Collaborative Engineering Environment (NCEE), which will be used to implement FORCEnet engineering practices. The session, hosted by Barbara Vaughn, NCEE technical director, of the Assistant Secretary of the Navy Research, Development and Acquisition Chief Engineer's office, described the roles for key players and milestone events in building and refining the NCEE.

"The FORCEnet Engineering Conference was a great opportunity for sharing FORCEnet efforts across our entire community, including C4ISR and combat systems, OPNAV and the SYSCOMs (systems commands), and the acquisition and operational communities of interest," said Capt. Cloyes "Red" Hoover, SSC Charleston commanding officer.

The Sea Warrior brief by Vice Adm. Moran was one of the conference highlights. The admiral meticulously mapped out the links between the Navy's Human Capital Strategy, Sea Warrior, Sea Power 21 and FORCEnet — the links that lead to warfighter readiness.

Conference attendee, Capt. Scot Miller, commanding officer of the Navy Center for Tactical Systems Interoperability, San Diego, Calif.

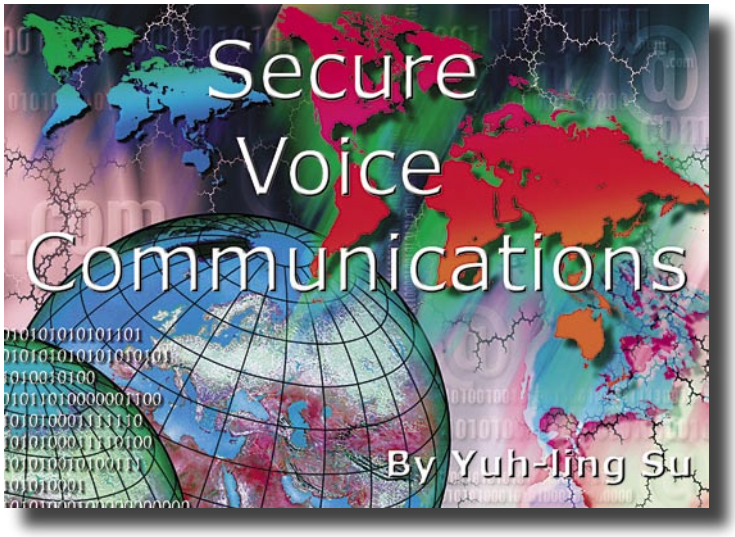
Cmdr. John Hearne, Carrier Strike Group Ten (CSG-10) knowledge manager (left) and Lt. Cmdr. James H. Mills, CSG-10 flag communications officer, participated in the FORCEnet Engineering Conference.

Perhaps the ultimate factor to the conference's success was that solid partnerships were formed and conference participants took on a feeling of ownership for making FORCEnet a reality.

"The next conference will continue to expand and build upon the positive relationships built at the initial meeting," Madsen said. *"Attendees can be expected to walk away with specific, engineering-level actions for their particular community as they help create the FORCEnet vision."*

The next FORCEnet Engineering Conference will be held Nov. 15-17, 2005, in San Diego. The theme of the San Diego conference will be "Integrating Interests/Finding Common Ground." The upcoming conference will explore a variety of topics, including interaction at the "joint warfighter tactical edge," data structures used as net-centric warfare doctrine and processes to enhance the capabilities of a fully netted force. Go to http://www.nconfs.com/fnengineeringconference/index.htm for information.

Sharon Anderson is the CHIPS senior editor. She can be reached at chips@navy.mil. Steve Davis is a media officer and policy review manager in the SPAWAR Office of Public Affairs. CHIPS



The need for secure data and secure voice is increasing dramatically with new threats and the global war on terrorism …

Military units require a full spectrum of communications capabilities to ensure that all elements of command and control (C2), *(battle orders, planning, logistics, medical, personnel, etc.)* are communicated effectively. Secure communication systems may be considered the lifeline of C2 on the battlefield and must be available to U.S. forces at all levels, from strategic to tactical.

FORCEnet will enable the integration of secure voice with data and sensor networks within the Global Information Grid (GIG). Integration of secure voice within FORCEnet is enabled by the rapidly maturing Voice over Internet Protocol (VoIP). In the last decade, circuit-switched technologies (used for voice communications) are transitioning to packet-switched integrated networks that support both data and voice.

The need for secure data and secure voice is increasing dramatically with new threats and the global war on terrorism. Today's warfighter must be able to use both secure voice and secure data simultaneously for effective collaboration. The future of end-to-end secure communications will be driven by Department of Defense (DoD) requirements, including joint and coalition collaboration, and the growing need to interoperate through the full range of federated operations involving U.S. government organizations such as the Department of Homeland Security, state and local government and others as directed. The convergence of voice and data in secure VoIP is a cost-effective enabler for these missions.

The Navy Secure Voice Team of the PEO C4I and Space, PMW 160, with technical expertise from SPAWAR Systems Center San Diego Code 2877, St. Julien's Creek, Va., is developing the Naval Advanced Secure Voice Architecture (NASVA) that identifies the future of secure voice communications in the sea, land and air warfare missions of the Department of the Navy. The NASVA describes an acquisition process that will leverage the spiral development process. It also provides the guidance necessary to integrate policies, requirements and technologies to successfully move from today's "as is" architecture to the future "to be" secure voice architecture.

The Secure Voice Team will leverage industry technologies and innovations, and rely on a comprehensive assessment of capabilities required by users. The team will also conduct continuous, in-depth examinations of emerging technologies that may deliver those capabilities. It is hoped that this approach will energize the development of technology to achieve immediate gains in capability under a rapid insertion scenario.

The Navy secure voice team is using a four-pronged approach to capture user requirements and help guide development efforts to meet users' needs:

√ Review the Joint Mission Essential Task List (JMETL) and Naval Mission Essential Task List (NMETL) to determine documented requirements.

√ Develop a Web-based questionnaire for recently deployed fleet, Marine Corps, joint and special warfare forces to collect a continuing flow of anecdotal or empirical information about equipment and user desired improvements or features.

√ Follow up with interviews of returning strike groups and special warfare units to capture the "real story" of system performance and solicit new ideas. Candid feedback to the online survey and fleet liaison visits are critical to the collection and analysis of requirements.

√ Consult industry to leverage emerging communications and network technologies. Selected technologies will be tested during Sea Trial events (*e.g., Trident Warrior series exercises)* for suitability.

Requirements gathering starts below decks with interior communications systems and extends through the "last mile" all the way to the "foxhole" in support of Army and Marine Corps units. The Secure Voice Team is investigating the full spectrum of technologies with an eye toward future net-centric requirements.

Major technological issues, technology mandates, security concerns, and integration and interoperability requirements all provide a catalyst for close partnership with industry to produce the next generation of secure communication devices.

The technological challenges of secure voice integration are many and complex. The convergence of voice and data presents a significant challenge for the prioritization of packets and managing traffic flow over an IP network while also meeting the quality of service requirements for voice, combat systems and other mission critical systems.

Interoperability issues are driven by DoD mandates, compelling the adoption of new features or security schemata that can cause interoperability problems (in particular with legacy

equipment). For instance, the Joint Tactical Radio System has been mandated as the joint standard for the future of radio frequency (RF) communications in DoD, and secure voice devices must accommodate this emerging standard. Another mandate is for IP migration to an IPv6 capable architecture for all communications and data systems by 2008.

In order to meet the net-centric secure voice requirements, the Secure Voice Team is pressing for the following initiatives:

√ Secure Communication Interoperability Protocol *(SCIP, previously known as Future Narrowband Digital Terminal, FNBDT)* Voice Gateway compresses voice signals to enable transmission over tactical links. This gateway is crucial to ships underway due to limited bandwidth on the battlefield and aboard ship.

Voice is critical for reach back to headquarters and remote medical and technical expertise — even more critical as manpower is reduced. In addition, the SCIP Voice Gateway will convert traditional telephony voice into IP packets that can be routed by the Advanced Digital Network System from and to the tactical links, maximizing use of available tactical bandwidth rather than requiring dedicated voice links.

√ Variable Data Rate (VDR) Voice Encoder enables 28 instantaneous data rates (2.4 kbps to 32 kbps) to optimize use of IP bandwidth while maintaining voice quality. It also provides narrowband to wideband interoperability. The dynamic VDR arbitrator enables the VDR voice encoder to set the data rate on the fly based on the network traffic conditions.

√ Secure Voice Core Technology supports voice encoding, encryption and instantaneous variability (using VDR) over a wide range of data rates, ensuring best voice quality over a challenged network. The encryption will include Type-1 and Advanced Encryption Standard (AES) algorithms.

√ Universal Voice Terminal (UVT) is a multifunctional, software configurable voice terminal that uses Secure Voice Core Technology. It will interface with VoIP and telephony systems, support new waveforms to meet future requirements, be compatible with existing RF components, and interoperate with legacy equipment via gateways. Land-based UVT can be used as a relay hub for the Personal Secure Telephone to provide worldwide secure voice coverage. The UVT could replace all current tactical secure voice crypto devices, dramatically reducing integrated logistics support, training and maintenance costs.

√ Personal Secure Telephone (PST) is a small, lightweight, multimedia, rugged, handheld wireless terminal that uses Secure Voice Core Technology. It will provide short-range tactical secure voice communications, interface with the UVT to extend tactical secure voice over the horizon and provide the Global Positioning System (GPS) reporting and targeting. Furthermore, the PST will use access controls, biometrics and a personal identification number (PIN) for authorization and authentication.

An important lesson learned from Operation Iraqi Freedom was that many situations preclude the use of Type-1 devices, and that the Navy required a small, wireless AES device for secure communications. A device supporting both Type-1 and AES encryption can also be used for DoD and homeland defense first-responder personnel.

A comprehensive secure voice architecture, well-defined fleet requirements, industry involvement and implementation of the secure voice initiatives are essential to ensure the superiority of secure voice communications …

√ Tactical Shore Gateway (TSG) is being installed at Naval Computer Telecommunications Area Master Stations to provide wireline/wireless telephone to tactical radio interoperability.

√ TSG for VoIP interoperability will combine the TSG and VoIP systems to provide an interface to an external connection that merges legacy secure voice systems, commercial telephony systems and IP networks with a tactical capability for Secure Voice over IP (SVoIP). This effort paves the way for tactical SVoIP capability, the first step toward integrating legacy secure voice systems and modern commercial telephony.

A comprehensive secure voice architecture, well-defined fleet requirements, industry involvement and implementation of the secure voice initiatives are essential to ensure the superiority of secure voice communications. Furthermore, benefits extend beyond the Navy, supporting the joint services and homeland defense missions.

Secure voice technologies will continue to evolve to integrate voice and data within FORCEnet into the GIG. Implementation of the planned architecture described in the Naval Advanced Secure Voice Architecture will extend superior situational awareness, which is heavily dependent on secure voice and data — all the way to the tactical edge.

The PEO C4I & Space, Networks, Information Assurance and Enterprise Services Program Office (PMW 160) provides all common network services and commodities used by multiple programs. PMW 160 consolidates network services in all classified domains to support cross-domain and coalition operations.

For more information about the PEO C4I & Space go to the SPAWAR home page at http://enterprise.spawar.navy.mil/.

Yuh-ling Su is the assistant program manager for the Navy Secure Voice Team (PEO C4I & Space, PMW 160).

CHIPS

SPAWAR Develops Innovative Approaches to Human Systems Integration

By Dee Quashnock

The Space and Naval Warfare Systems Command (SPAWAR) is exploring a number of innovative approaches for achieving greater mission effectiveness while maximizing the Navy's workforce capability. Leading this effort, is the SPAWAR Human Systems Integration (HSI) team in the Office of the Chief Engineer. This headquarters team directs a corporate-wide team comprised of teams located in SPAWAR field activities.

Figure 1.

HSI integrates human capabilities and limitations into system definition, design, development and evaluation to optimize total system performance in operational environments. It is part of the total systems engineering approach to analysis, design, development and testing. Figure 1 shows the elements of the operational environment.

FORCEnet is the Navy's road to transformation for network-centric warfare. It integrates warriors, sensors, command and control, platforms and weapons into a networked combat force. FORCEnet is the key enabler of Sea Power 21; it provides the foundation for Sea Basing, Sea Shield, Sea Strike, Sea Warrior, Sea Trial and Sea Enterprise.

The FORCEnet Functional Concept, which was approved by the Chief of Naval Operations and the Commandant of the Marine Corps, characterizes the FORCEnet environment as collaborative, decentralized and agile. "FORCEnet is all about command and control, and HSI provides the focus on the warfighter," said Capt. Rick Simon, FORCEnet Coordinator at the Naval Network Warfare Command (NETWARCOM).

One result, since the issuance of the FORCEnet Functional Concept, is new constructs such as distributed staffs. Members may be embarked on forward-deployed units supported by a shore-based staff of domain specialists available to provide technical support via Web-based, service-oriented information systems using an agile semantic framework for dealing with disparate data.

This functional concept draws attention to several HSI issues, including distributed decision-making, shared situational awareness, system-of-systems training, reliable collaboration tools and displays to promote effective command and control. HSI has played a significant role in supporting the decomposition and expansion of the FORCEnet Functional Concept to ensure that cognitive and decision processes are adequately represented.

The Marine Corps Combat Development Command, NETWARCOM and the Office of the Chief of Naval Operations (OPNAV) Resources, Requirements and Assessments (N81) have supported SPAWAR's efforts to incorporate HSI considerations into the documentation that articulates the FORCEnet concept as part of the Defense Department's Joint Capabilities List.

Transforming the Navy into a decentralized, more distributed, agile workforce demands effective HSI efforts that address not only the traditional HSI disciplines of manpower, personnel, training and human factors but also such disciplines as organizational psychology and even cultural anthropology.

Organizational psychology is very much a part of HSI. HSI is about the interaction of human operators with the technologies they use. It includes how operators communicate, coordinate and collaborate information with other humans in the system. Cultural anthropology offers insights and a discipline for studying and comparing organizational constructs among and within organizations.

Trident Warrior 2004, an annual FORCEnet Sea Trial experiment led by NETWARCOM, initially examined FORCEnet concepts. Experimentation in Trident Warrior improved tactical situation awareness, provided speed to capability, a rapid fielding of improved FORCEnet command and control warfighting capability to the fleet, and supported the development of tactics, techniques and procedures to optimize new technologies for the execution of naval operations.

During Trident Warrior 2004, the HSI team collected data from a wide range of FORCEnet technologies designed to support operational mission capabilities, such as ISR (intelligence, surveillance and reconnaissance), targeting and tactical operations in a complex global war on terrorism scenario.

In TW04, the HSI team found a good shared understanding of exploited imagery and ISR products afloat and ashore; effective collaboration with no loss of service via the Distributed Chat Architecture; and an accurate understanding of network status via a new Advanced Digital Network System technology.

FORCEnet is the key enabler of Sea Power 21; it provides the foundation for Sea Basing, Sea Shield, Sea Strike, Sea Warrior, Sea Trial and Sea Enterprise.

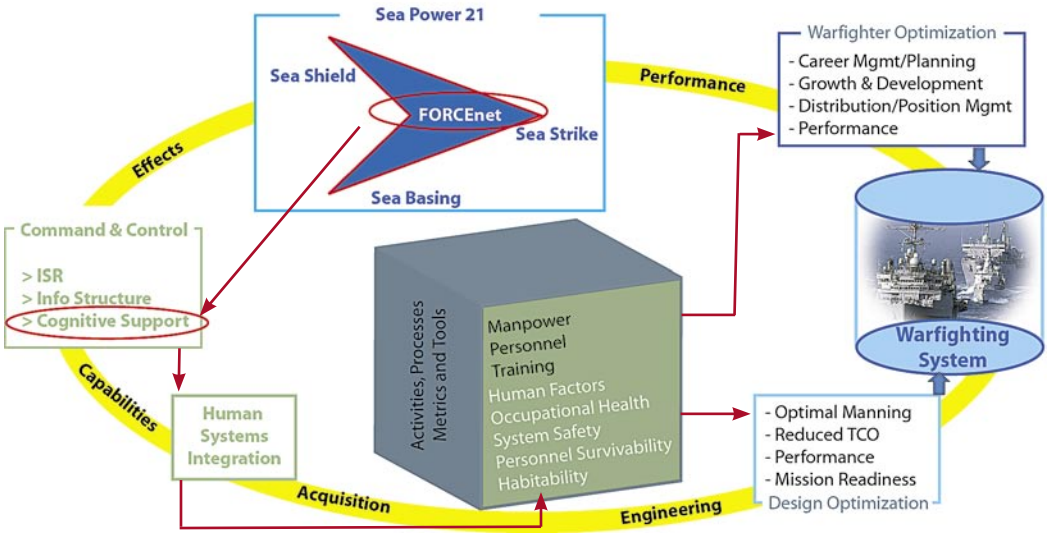


Figure 2. HSI Enterprise Architecture.

We used the results to make recommendations for the Military Utility Assessment (MUA) to request continued development for the programs associated with these technologies to further improve warfighting capabilities.

The HSI team collected data on operator performance, situation awareness and system usability. The HSI findings were influential in the Operational Agent's Assessment and the MUA to make decisions regarding acquisition programs based on how well operators and mission performance are supported by advanced FORCEnet technologies. Both the HSI methods and the Trident Warrior results have been very well received by military and system engineering groups in the United States and abroad.

The SPAWAR HSI team continues to take a significant leadership role in the analysis of FORCEnet systems in Trident Warrior 2005. In coordination with other initiative areas including joint and coalition organizations, HSI is providing comprehensive quantitative and qualitative human performance data related to a variety of systems, including chat tools, network visualization tools, information operations, Voice over Internet Protocol /video teleconferencing over IP, cross-domain solutions and information management plans.

In addition, HSI is spearheading the development of an improved concept to update commanders as part of the regular battle rhythm and to form a response in crisis situations. Each of these efforts demonstrates the impact that HSI has had on moving the emphasis from technology-based assessment to mission-based analysis. Mission-based analysis considers how effectively human operators and decision makers are integrated with information technologies and networks.

SPAWAR is part of the Human Systems Performance Assessment Capability (HSPAC), a Navy infrastructure that will allow individual and system-level human performance to be assessed and certified. The Usability and Engineering Research Lab and the Composeable FORCEnet Human Systems Integration (CFnHSI) Lab in Point Loma, Calif., will be a key part of this distributed capability. HSPAC will enhance fleet readiness and operational effectiveness at the lowest total ownership cost by providing personnel, expertise, equipment, connectivity, tools, models, environments and alliances necessary to measure, analyze, assess and certify Sailor performance in warfighter systems across all life-cycle phases. Figure 2 shows the HSI enterprise architecture.

SPAWAR 052 is working closely with the Virtual SYSCOM HSI Working Group to define a common taxonomy of human performance measures and metrics that can be shared and applied to a broad array of systems analysis tasks. SPAWAR's efforts led to the rapid implementation of an initial taxonomy accessible in flexible formats via an HSI ontology software application that has now formed the basis for a continuing metrics effort by HPC and Virtual SYSCOM working groups.

SPAWAR recognizes that there are several key features for an effective distributed workforce and has taken the lead in integrating these features into its systems. These features include:

√ *Common operational picture (coordinating representation) and collaboration tools (feedback);*
√ *Shared understanding of team roles, capabilities, goals, deadlines and priorities;*
√ *Operating tempo aligned across distributed teams;*
√ *Technology and reliable communications with a high degree of usability;*
√ *Consistent, current and easily accessible data;*
√ *Training and procedures for how to employ technologies in a system-of-systems approach.*

These HSI efforts directly support initiatives to transform the Navy's Human Capital Strategy through Sea Warrior. The strategy is focused on a distributed, capable workforce that uses FORCEnet to realize the vision of distance support teams, composeable systems capability and agile forces to rapidly execute the Navy's missions.

Dee Quashnock is the director, architecture and human systems in the SPAWAR Office of the Chief Engineer.

CHIPS

SPAWAR Systems Center New Orleans Customer Support Center Finalist for Government Customer Support Excellence Award

By Maria LoVasco Tolleson, Public Affairs Officer

The Space and Naval Warfare Systems Command (SPAWAR) Systems Center (SSC) New Orleans, Customer Support Center (CSC) was named one of the top three customer support centers in the area of customer focus at the Government Customer Support Conference in May.

The CSC competed with top support centers around the nation, which included all levels of local, state and federal government. Other finalists included the Social Security Administration, Utah State Government and NASA.

The Government Customer Support Community of Practice (GCSCoP), nominated the SSC New Orleans Help Desk for the award. The GCSCoP is a federal help desk forum created to promote excellence in supporting government internal and external customers. Currently, several thousand organizations from all three levels of the U.S. government (and some foreign governments) participate in the GCSCoP.

The CSC is a critical part of SSC New Orleans providing information technology services and support to the Department of the Navy and Defense Department.

"Our vision is to increase business opportunities by providing superior capabilities, perseverance and outstanding customer support," said Mr. Jamie Passaro, SSC New Orleans director of customer services. "We view challenges as opportunities, and we strive to adjust to ever changing requirements without changing our core customer support principles."

SSC New Orleans, an echelon III field activity under SPAWAR, consists of about 1,100 military, civilian and contractor personnel who provide a full range of information technology products and services from requirements identification and analysis, systems and production engineering and telecommunications support, to architecture design, quality assurance, Navy human capital development and homeland security.

Additionally, SSC New Orleans supports the Program Executive Office for Information Technology (PEO-IT) in the development of the Defense Integrated Military Human Resources System (DIMHRS) and other military human resources information technology programs.

The help desk provides support 24 hours a day, 365 days a year for nine systems and includes: the Navy Standard Integrated Personnel System (NSIPS); Navy Reserve Pay Helpdesk; Navy Reserve Order Writing System (NROWS); Job Advertising and Selection System (JASS); Medical Readiness Reporting System (MRRS); Inactive Manpower and Personnel Management Information System (IMAPMIS); Reserve Headquarters Support (RHS); Reserve Standard Training Administration and Readiness Support (RSTARS); Health Professions (HP); local base operations; electronic data warehousing (EDW); and Corporate Data Maintenance (CDM), formerly known as the Personnel Pay Assistance Center (PPAC).

Through these systems, the center supports a customer base of 537,000 personnel from every Naval activity, including fleet units. The center also provides support to the Air National Guard and Marine Corps.

Fifty customer service engineers with backgrounds in functional and customer support staff the center. In the last 12 months, they have fielded more than 215,000 calls and already this year have responded to 67,000 service requests.

With an annual volume of more than 225,000 calls and total service requests in excess of 260,000, SSC New Orleans is the largest source of support in the Navy reporting to the Global Distance Support

"We've been successful because we have developed true partnerships with our Navy customers …"

- Jack Walbridge, help desk manager

Customer Support Center employees, Ms. Joan Baham (standing) and Ms. Felicia Smith.

Leonard Ball, help desk pay technician (left) and Mike Redoutey, Navy Standard Integrated Personnel System (NSIPS) tech lead.

Help Desk personnel receive instruction in the training room. Jack Walbridge, help desk manager, is at the podium.

Center (GDSC), formerly known as the Navy Integrated Call Center. The CSC is part of the SPAWAR Distance Support Community.

In addition to the central facility in New Orleans, there are waterfront support groups located in Norfolk, Va., and San Diego, Calif., which provide NSIPS, quality of life and training support directly to fleet units. These units are comprised of both Sailors and civilian personnel who can respond quickly to emergent fleet requirements.

Mr. Jack Walbridge, a STI-certified (industry certification) help desk manager, heads the Customer Support Center. Ninety percent of the staff has 20 or more years of support experience with Navy quality of life applications. A large percentage of the staff are retired from military service, with 75 percent from military pay and personnel backgrounds and 67 percent from travel order preparation backgrounds.

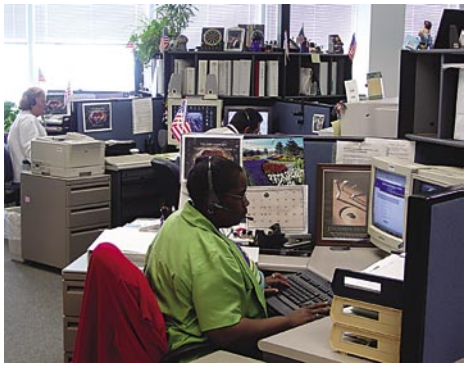
Because of their military experience, the Customer Support Center staff have seen the entire range of pay and personnel problems in the fleet, and they understand the importance of rapidly solving quality of life issues.

The CSC teams with systems and production engineers to ensure successful support early in the program life cycle. They work directly with program managers for testing, validation and training.

According to Mr. Tom Ledet, program manager for the Navy Reserve Order Writing System, the SSC New Orleans Help Desk has a significant impact on the NROWS reputation. "The group consistently provides accurate and timely responses to all questions and problems reported by the field users. It is truly one of the best teams I have worked with," Ledet said.

Prior to his assuming command as commanding officer of Naval Air Station Joint Reserve Base, Fort Worth, Texas, Capt. John McCormack served as the Commander, Naval Reserve Forces program manager for NROWS.

"The SSC New Orleans Help Desk is a shining example of doing business right," McCormack said. "The professionalism and dedication displayed by the team is unmatched in any support center I have ever dealt with. I have never before experienced the kind of ownership the SSC New Orleans Help Desk took in our program, it made all the difference in the world."



Ms. Velvet Knight, Navy Reserve Order Writing System (NROWS) subject matter expert (foreground) and Ms. Susan Stringfield, NROWS tier 1 technician.

A look at the latest metrics on the Distance Support Content Central Web site *(http://www.anchordesk.navy.mil/CntMgmt/CntCentral.htm)* reveals that SSC New Orleans serviced more calls in the past month than the other top 10 help desks combined.

"I'm very pleased with SSC New Orleans' participation in the Sea Warrior Help Desk Integration with the Distance Support initiative," said Ms. Terri Clark, supervisory program analyst in the Functional Integration Directorate at the Naval Personnel Development Command.

"The SSC New Orleans representatives are providing their help desk operations expertise, as well as their leadership skills, to support our transition to an integrated Sea Warrior Help Desk system with Distance Support," Clark said.

The CSC developed and implemented a customer service request system that is based on the Remedy Action Request System application. The center uses Remedy Distributed Server Option for transferring service request data to SPAWAR San Diego for statistical reporting. Crystal Reports is used to develop customized reports for customers. Using the Remedy system, personnel can generate, update and track service requests. The system also creates knowledge-based solutions for common problems.

Escalations and notifications are generated based on defined rules. Escalations are originated for a service request when it has been waiting too long in a queue. When this occurs a notice is sent to a supervisor or manager to take action.

The center has automated service request generation capabilities using an interface between a Computer Associates application called, Unicenter Network and System Management, and Remedy. When a monitored server has a threshold that has been exceeded a service request is automatically generated in Remedy and routed to the appropriate technician for resolution.

This methodology allows personnel to track and report issues related to the availability and performance of a system. In addition, personnel use Asset Management and Performance Management components to inventory the hardware and software loaded on a server.

For telephony, the center has a private branch exchange (PBX) Avaya G3R with a full range of call management capabilities.

"We've come a long way in a relatively short period of time. Over the last five years, we've grown from a staff of 10 to a staff of 50," Walbridge said.

To be recognized as one of the top three Customer Support Centers in the federal government for customer focus is a testament to the professionalism of our entire staff and to the seriousness with which SPAWAR views quality of life issues for our Sailors and their families.

"We've been successful because we have developed true partnerships with our Navy customers and government leadership. We're part of SPAWAR's Strategic Vision which means that the importance of providing great support is not just a function of the CSC, it's a total commitment from SPAWAR," Walbridge said.

Due to the effects of Hurricane Katrina, SSC New Orleans is temporarily closed. CHIPS

Interview with Cmdr. Tony Parrillo Director of the FORCEnet Execution Center

Recently appointed Deputy Director of Naval Network Warfare Command, Mr. Mark Honecker, Cmdr. Tony Parrillo, director of the FORCEnet Execution Center and Capt. Chris Abbott director of FORCEnet Innovation and Experimentation Division cut the ceremonial ribbon celebrating the opening of the FORCEnet Execution Center in building V-53 on Naval Station Norfolk July 19, 2005.

The FORCEnet Execution Center is charged with conducting operational experimentation, specifically Trident Warrior, the major annual FORCEnet Sea Trial event designed to provide speed to capability and rapid fielding of improved command and control warfighting capability to the fleet. CHIPS asked Cmdr. Tony Parrillo, the center's director what the stand up of the FORCEnet Execution Center will mean to Trident Warrior experimentation and deploying FORCEnet capabilities to the fleet.

CHIPS: What will the stand up of the center mean to FORCEnet?

Cmdr. Parrillo: This is actually FORCEnet Execution Center No.2. The significance of opening this center is that we are here in Norfolk, Va., and we are close to Fleet Forces Command, which is the lead for Sea Trial and the primary organization and infrastructure that we support. I report to Capt. Chris Abbott, who is the NETWARCOM Innovation and Experimentation Division head or N9, and he runs the Sea Trial process for the FORCEnet pillar. We are also close to U.S. Joint Forces Command, which has a very robust joint experimentation cell. They are doing a lot, and they have gotten a lot bigger and a lot more influential over the last couple of years.

The original FX Center is in San Diego on NAB (Naval Amphibious Base) Coronado. As the Director of the FX Center, I have West and East Coast offices, with a few less people in San Diego. When you talk about reach back and a dispersed staff, I can speak from experience. I deal with it on a daily basis. Sometimes it is a leadership challenge to direct a staff without being face-to-face with them, but this is one of the transformational issues the Navy is facing right now.

In net-centric operations the best way to act is to have a broadly dispersed force so you are a very difficult target to find. So you can focus all your power or energy or weapons on targets from many locations. The enemy won't be able to react because your forces or strength is coming from 'everywhere' and, at the same time, the enemy can't find you because you are everywhere. With reach back, we also reduce our forward footprint, giving the enemy less targets, thus enhancing safety.

For example, the admiral or the strike group commander is used to being able to reach out and touch his intel officer and ask, *Are you sure that this is the best intelligence you have?* The Navy is progressing to the point where we can collaborate across many geographic and time zone boundaries to get the best intelligence from the expert back in the Pentagon or at ONI (Office of Naval Intelligence) or wherever. This will be done without ever meeting the person or possibly even knowing his or her name. Collaborative planning among many people is hard, and the more people you have, it becomes exponentially harder.

CHIPS: You mentioned reaching out to the Program Executive Offices and acquisition community. Do you hope to influence the acquisition process by what you find out in your experimentation?

Cmdr. Parrillo: Yes, we do. The fastest way to bring speed to capability is to interface directly with the acquisition community, working together to field the latest and best equipment for the fleet. That is the nice thing about our Coronado office. It is near the Space and Naval Warfare Systems Command headquarters, and here in Norfolk, we are collocated on the same floor with SPAWAR Systems Center Charleston.

We are closer to what the acquisition community is planning, and we bring a fleet perspective. I have seasoned fleet information professionals, both officer and enlisted working with me. It is a nice synergy for the acquisition community to know what the warfighter needs and for the warfighter to get things faster.

A great addition has been Mr. Mark Honecker, who as the new

Deputy Director of Naval Network Warfare Command, Mr. Mark Honecker, (center), Cmdr. Tony Parrillo, director of the FORCEnet Execution Center (left) and Capt. Chris Abbott, director of the FORCEnet Innovation and Experimentation Division cut the ceremonial ribbon celebrating the opening of the FORCEnet Execution Center in building V-53 on Naval Station Norfolk July 19, 2005. Photo by John Donaldson, NETWARCOM Public Affairs.

deputy director of NETWARCOM, brings years of experience with the acquisition community as well as OPNAV and the Navy budgeting offices. Hopefully, this will bring us full circle to bring cutting-edge command and control, ISR and other FORCEnet capabilities to the fleet faster than ever done before.

CHIPS: Are there any particular PEOs or organizations that you want to work with?

Cmdr. Parrillo: PEO C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), and PEO IWS (Integrated Weapon Systems) to name two. And I would also like to mention our work with both 2nd and 3rd Fleet. Trident Warrior 2005, our major Sea Trial experiment will be with 2nd Fleet. Trident Warrior 2006 will be with 3rd Fleet. Previously, Trident Warrior 2004 was with 3rd Fleet.

We are trying to get the maximum fleet exposure, at the same time working closely with the PEOs. We also try to work with the Marine Corps Combat Development Command, SPAWAR, the other SYSCOMS and Navy Warfare Development Command, which is the Navy's lead for doctrine and CONOPS.

The Naval Postgraduate School is the lead for our analysis efforts. I work with the Naval War College on some of the doctrine and wargaming. OPNAV N71 is our official resource sponsor. We have worked a little with the Joint Staff and hope to expand on that as well as align our efforts with JFCOM. We are collaborating with the Air Force in the Joint Expeditionary Force Experiment, which is the Air Force's big experiment next year.

We look forward to working with U.S. Northern Command for homeland security and homeland defense issues. We are working with a coalition interagency, the AUSCANNZUKUS organization, which includes Australia, Canada, New Zealand, United Kingdom and United States military services. We are also working with some of the elements of the Department of Homeland Security like the U.S. Coast Guard. We hope to collaborate further with our interagency partners in the global war on terrorism.

That's a lot of organizations to try to work with, so it really keeps us hopping. Capt. Rick Simon, the FORCEnet coordinator from NETWARCOM helps us out a great deal trying to bring it all together for the Navy and Department of Defense.

CHIPS: Who decides whether the FX Center will participate in exercises like RIMPAC or Rim of the Pacific? Your resource sponsor?

Cmdr. Parrillo: Yes and no. RIMPAC is an exercise and TW is an experiment. We have found in the past that combining exercises and experiments is not the most ideal way to conduct TW, so often we try to find our own venues. An exercise is training for whoever is going to deploy. They are worried about fighting a war while in our experiments we want to try to repeat the exact same experiment five times in a row under different network conditions.

When the services are preparing to fight a war, they don't want to do the same thing five times in a row. Also experiments take

The FORCEnet Execution Center staff L-R: Information Systems Technician 3rd Class Zachary Jones, Cmdr. Tony Parrillo, Lt. j.g. Kenneth Box, Lt. Cmdr. Jacqueline McElhannon, Information Systems Technician (SW) 2nd Class Craig Smith, Information Systems Technician (SW) 1st Class Donald McEathron, Quartermaster Chief (SW) William Alston and Electronics Technician 1st Class Molly Vivian (not shown). Photo by John Donaldson, NETWARCOM Public Affairs.

second place to the real training, so it would be bad to spend a lot of money setting up an experiment, just to have it canceled for real world training. We occasionally will piggyback with some of the resources that are committed to an exercise, but we usually look for our own venues. Experiments have a different focus than an exercise so sometimes training and experiments don't match up well.

CHIPS: Do you look at the results of other exercises and demonstrations?

Cmdr. Parrillo: Absolutely! For example, 2nd Fleet had its MARCOLE 2 (Maritime Command Limited Experiment) and worked with some cross-domain solutions. We are continuing and refining that work this summer for TW05, which will take place in the November-December timeframe.

Actually for RIMPAC, we are working with 3rd Fleet to help build coalition solutions for the RIMPAC exercise. My experts in cross-domain solutions and networks and the coalition environment are working with 3rd Fleet to help develop networks that will be faster and smoother. It is a greatly dispersed audience. RIMPAC has countries as disparate as Chile, Japan and South Korea.

CHIPS: Are the results from exercises and demonstrations shared to avoid duplicating something that has already been done?

Cmdr. Parrillo: As part of our experimentation campaign, Naval Postgraduate School created FIRE, which is the FORCEnet Innovation Research Enterprise. FIRE is our giant database on FORCEnet experimentation and our collaborative tool for creating those experiments. In FIRE we break everything down to its lowest component level. So if you want to find out

everything that has been done for cross-domain solutions, you can just search the database. This data mining capability will go a long way to preventing duplication, as well as allowing us to plan our campaigns.

CHIPS: Is the FORCEnet Execution Center a lab?

Cmdr. Parrillo: No. We do the coordination. As I said earlier, my staff is dispersed everywhere. We use whatever labs are necessary. We use labs at SPAWARSYSCEN San Diego and SPAWARSYSCEN Charleston's lab at St. Julien's Creek. Occasionally, we even use Air Force or National Security Agency labs. We run the experiments administratively here, and then the bits and bytes are tested in the lab prior to being loaded aboard ships for at sea testing.

CHIPS: Can you talk about some of your objectives?

Cmdr. Parrillo: The number one objective of Trident Warrior is speed to capability. That is getting the FORCEnet capabilities out to the fleet. We try to pick an ESG (expeditionary strike group) or CSG (carrier strike group) that is in their turn-around cycle and help outfit the entire strike group with the latest equipment so that everybody has the same baseline. Then, the strike groups get to try out the new equipment and practice in TW and tell us what they like and don't like. Hopefully we get to tweak the equipment before they go on a cruise. That is the first goal.

Another goal is to find the things with the greatest military utility and promote them to the OPNAV, acquisition or PEO communities. We report the Military Utility Assessments to the Sea Trial Executive Steering Group on what we found were the best things from all our experiments. After all, if it doesn't have a military utility, then there is no reason to test it or continue forward with it.

Hopefully, that will have an effect on the POM (Program Objective Memorandum) and PPBE (Planning, Programming, Budgeting and Execution) process in the Pentagon and then it will trickle down to the acquisition community. The things that we find that have the most military utility are the ones that are fielded to the fleet first.

CHIPS: Did results from TW04 impact the POM?

Cmdr. Parrillo: Yes, there was internal reprogramming to speed the development of some of the things that we found. Mr. Bill Farmer, from the Advanced Digital Network System (ADNS) PEO, likes to quote that Trident Warrior took years off his developmental time line.

CHIPS: Can you talk about any of the improvements to command and control that you hope to achieve?

Cmdr. Parrillo: The key to improving command and control is to help shorten the decision cycle of the commander. As Vice Adm. James McArthur would say, 'FORCEnet is all about the commander.' Bring him the right information in the right format for him to have the best situational awareness to make the best decisions possible.

Just because there is data or information does not mean it is good. Too much information can be as bad as not enough information. You have to be able to display information in a way that the commander can understand to see both secondary and tertiary effects of the things he is doing. We have been looking at different ways to visualize the tactical and strategic situations. We have also been looking at ways to affect people and countries and non-country actors in a non-kinetic way, not by just using effects-based operations and dropping bombs on targets.

If the correct people are involved in the loop, the commander can make the instantaneous decisions that are necessary in today's world. We look at how the people interact with the equipment and interact with one another. The better they can interact with one another and with the equipment, the faster and better they can make decisions. Finally the technology, which most people tend to focus on, is really a smaller portion of the equation than people like to believe.

CHIPS: When you are testing human systems integration are you looking at the ease of using the system?

Cmdr.Parrillo: FORCEnet is made up of three elements. According to the FORCEnet functional concept, the three elements are the warfighter, the process and the technology. Sound HSI practices must be incorporated into all the core processes that define and monitor acquisition and the implementation of FORCEnet.

HSI provides a breakdown of the experimentation process because it looks at the participating capabilities by viewing each of the elements for the work performed by a human in a system, as in a larger system.

HSI is pure in the analytical part because it starts with a process and identifies what work is performed by human beings in the process. Then HSI measures how well the capability or technology supports the performance of human tasks in a live operational context. The reasons for investing in technology are to speed up the process and/or save money. The HSI analysis can show us where machine-to-machine interfaces can replace people. This can speed up the process as well as save the Navy money by reducing personnel.

CHIPS: The CHIPS staff saw a demonstration of a SATCOM capability for the battlefield. The satellite dish had to be lightweight and easily assembled on the fly. Is this the kind of thing you look at?

Cmdr. Parrillo: We look at even the most basic of things. For example, is the chair comfortable? If the chair is not comfortable then the person making the decisions is going to be distracted by a sore back rather than making the best decisions possible. Is the screen or display user-friendly?

The commander may need a three-dimensional display so that he can see the terrain from different angles. Some angles hide things. If you are just looking at a 'God's eye view' you may not be able to see the hills or terrain in the way. Are the controls comfortable and easy to use? There are a myriad of things that go into HSI.

CHIPS: Are there any new technologies that you are testing that you hope will be ready for fleet use?

Cmdr. Parrillo: There are so many good things that I'm reluctant to mention any particular one for fear of leaving something out. After we execute TW05 and get our results, can I give you an update on some of our standout performers?

I will mention that we tend to focus on technology that is ready to be fielded. For example, the S&T (science and technology) community, like the Office of Naval Research and Defense Advanced Research Projects Agency, focuses on things that are further out in development. We would like to be able to get technologies from the S&T community as they become operationally ready.

We are looking at the things that we can get for the fleet in the near-term and that involves mostly working closely with programs of record. Perhaps, a program of record staff are looking at two different paths that they could go down for one of their applications or programs. We can help them try out different courses of action. We also work to refine and develop requirements for the Navy. We start with the Navy's capabilities and gaps that are missing, and we look at that with OPNAV and the fleet and see what we can do to solve near-term gaps.

CHIPS: Can somebody come to you and ask you to test something for them in the TW or Sea Trial environment?

Cmdr. Parrillo: People can come to us; however, it all starts with STIMS, which is Sea Trial Information Management System, run by NWDC. When any one has an idea, I believe that this includes industry, they suggest what they think should be tried. The ideas are vetted by the Sea Power 21 pillar.

For example, if company X proposes a technology widget, it will be vetted by the FORCEnet Fleet Collaborative Team, and if the team thinks that it is something worth pursuing, it will continue down the Sea Trial path. If it is not, it can be rejected by the FCT or the operational agent. Then all the pillars of Sea Trial, Sea Shield, Sea Strike, Sea Basing and FORCEnet, get together and prioritize capabilities according to the Navy capability gaps.

A lot of times things fit nicely with what we are planning on doing and sometimes they do not. Just because we missed number two on the top ten, does not mean that we did not want to do it; it just did not fit with the venue we have for the next year. We do have some technology that comes up at development conferences where people can come to us. For the most part, we go with what big Navy tells us are the near-term goals. The Naval Capability Gaps provide the initiative areas then we work with the acquisition community and others, like S&T to narrow or close those gaps.

CHIPS: I see you have a terrorist-induced disaster scenario planned for TW05. How do you determine what your scenario is going to be and who is going to participate?

Cmdr. Parrillo: The global war on terrorism scenarios for '05 and '06 came out of an OPNAV wargame to explore what more the Navy can do to fight the war on terror. Over the last several years OPNAV has been recalibrating the Navy's commitment to the major theater wars to integration with other things like humanitarian assistance or homeland security for a more holistic approach.

We are trying to address a lot of those issues including maritime domain awareness which came out of a Presidential Directive just before Christmas this past year. We are looking at finding ways to better fight the global war on terrorism. Back to the FORCEnet functional concept, you have your people, your processes and technology. If you are looking at all three, it will make the Navy a better protector of the American people both near the coast and overseas.

This year we are looking at a scenario with tankers exploding in harbors, helo raids on terrorist camps, maritime interdiction and more. We are looking at command and control issues for some of these issues, including disasters, whether man-made or natural. For instance, after the tsunami hit Indonesia, when Navy warships left the area, the USNS Mercy, a hospital ship, hosted the command post.

Even two years ago no one would ever have imagined that a hospital ship would be the command post for the Navy overseas. Every unit needs robust communications and capabilities. You do not need all the decision-makers or intelligence functions on the hospital ship, but they need to be able, in the time of crisis, be able to reach out and touch the experts wherever they are around the world.

CHIPS: Is the Coast Guard in TW05?

Cmdr. Parrillo: The Coast Guard will hopefully be in TW06. We have had discussions on maritime domain awareness with the Coast Guard all summer. As we move into the initial planning conference for TW06 we are planning to have them involved. We know there will be a Coast Guard cutter in the area potentially working with us in TW06.

We would also, if possible, get more of the interagency players involved, possibly the Federal Aviation Administration or other DHS organizations and possibly some of the first-responders and law enforcement. Trying to test some of the connectivity is all a 'crawl, walk, run' theory, but we need to at least test some abilities to exchange information from DoD to other agencies. From there we will hopefully get better, and we will need a seamless transition from homeland defense to homeland security.

CHIPS: Do you get the requirements from Fleet Forces Command?

Cmdr. Parrillo: They are the lead for the Sea Trial process. They help define the final priorities of the things we look at, and then when we are done with our Military Utility Assessment, we feed that back to them and they feed it to OPNAV.

This method will help define the Navy's funding priorities for the next POM cycle. CHIPS

Marine Corps C4I Integration Architectural Strategic Plan

By Mr. J. D. Wilson

Overview

The Marine Corps migration to an "end-to-end" Marine Air Ground Task Force (MAGTF) command and control (C2) strategy requires an equally dynamic strategic plan for C2 and communications, computers and intelligence (C4I) architectural development. This article outlines the proposed methods to analyze the material procurements and technology insertions necessary to transition our current enterprise C4I architecture to support the new MAGTF C2 concept of operations (CONOPS).

Mapping Capability to Architecture

The Marine Corps Combat Development Command (MCCDC) has developed a five-layer MAGTF C2 reference model to represent the necessary "… end-to-end, fully integrated, cross-functional set of MAGTF C2 capabilities." The Deputy Commander, for C4I Integration (C4II) at the Marine Corps Systems Command (MCSC), works with the MCCDC command and control infrastructure (C2I) and Headquarters Marine Corps (HQMC) C4 to identify the connectivity interfaces between these layers and ensures the identified material solutions create a fully integrated environment.

Grouping the reference model layers by function provides "C2 capability categories" that can be used to describe architectural "gaps and overlaps." With these categories, standard language can be employed to describe architectural investment needs. For example, to achieve a certain C2 end state potential by a certain date, more "operational bandwidth – satellite systems" or "enterprise service – network storage" may be specifically addressed.

Many of the 546 programs of record (POR) overseen by C4I are that of users of the C2 capability versus providers. Platforms, such as, tanks or an Assault Amphibian Vehicle Personnel (AAVP) need connectivity to the C4I architecture, but their primary focus is another combat function like fires or maneuver. These users access C2 capabilities by embedding C4II material solutions like communications, network services, applications or end user devices in their platform. By assigning each POR a C4I material solution category every system procured can be traced to one of the C2 capability categories, as illustrated in Figure 1.

Architecture Integration

The connectivity interfaces that link the layers are the glue binding the disparate systems together into a fully integrated C4II architecture. To design the interfaces of the Marine Corps architecture, the technologies used in the configuration of the material solutions must be analyzed. The data for this analysis is taken from the Department of Defense Architectural Framework systems views and technical views. Understanding these views enables the strategic planner to recommend when new technology insertion is required or how it will impact the current architectural structure.

As the Marine Corps moves toward the end-to-end MAGTF C2 strategy there are three mutually supporting frameworks that must be defined. The first, and probably the most difficult, is the provision of command and control systems interoperability.

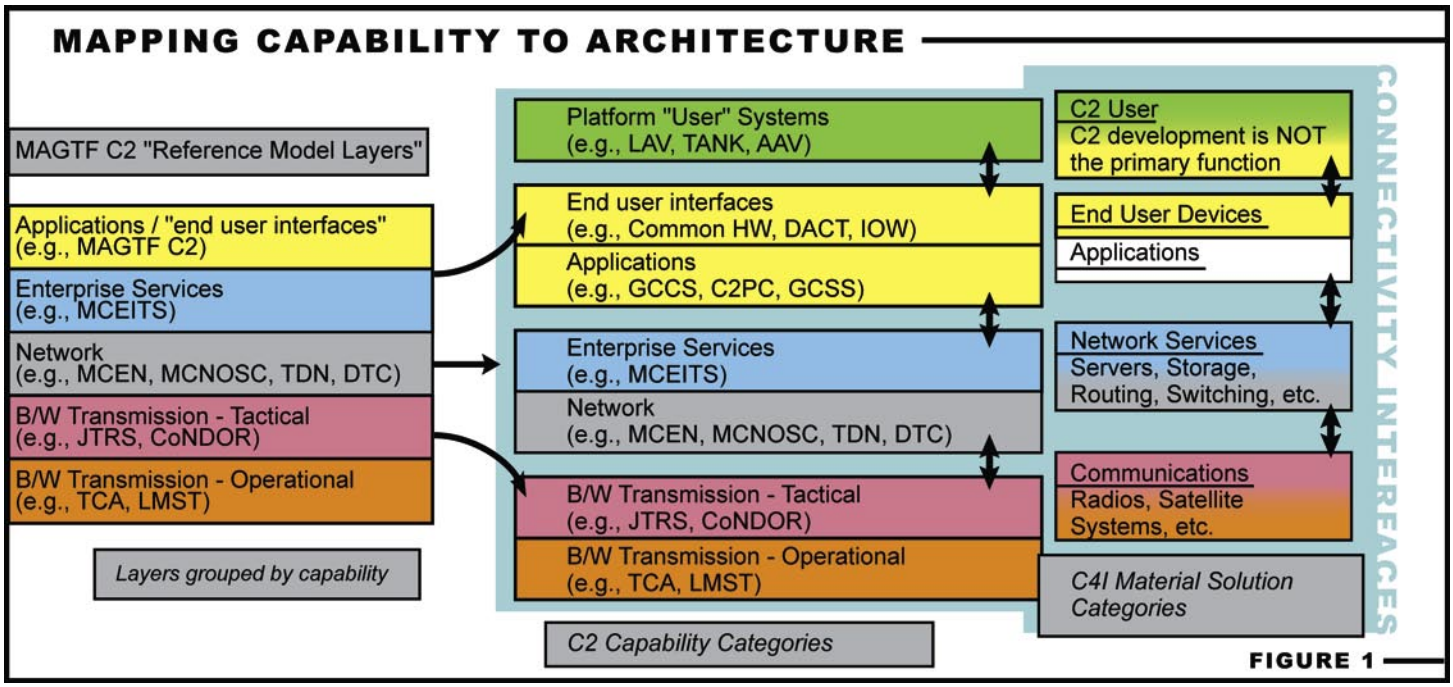
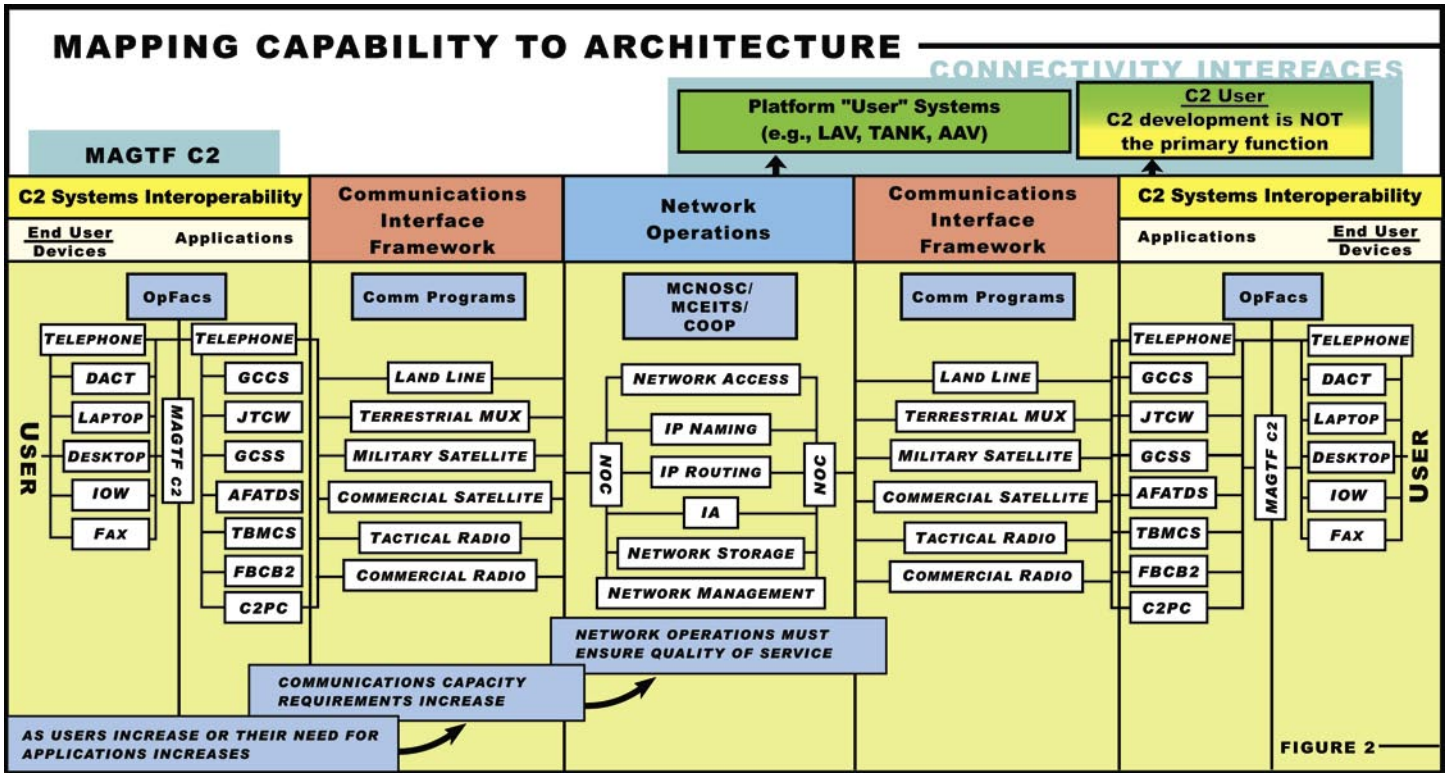


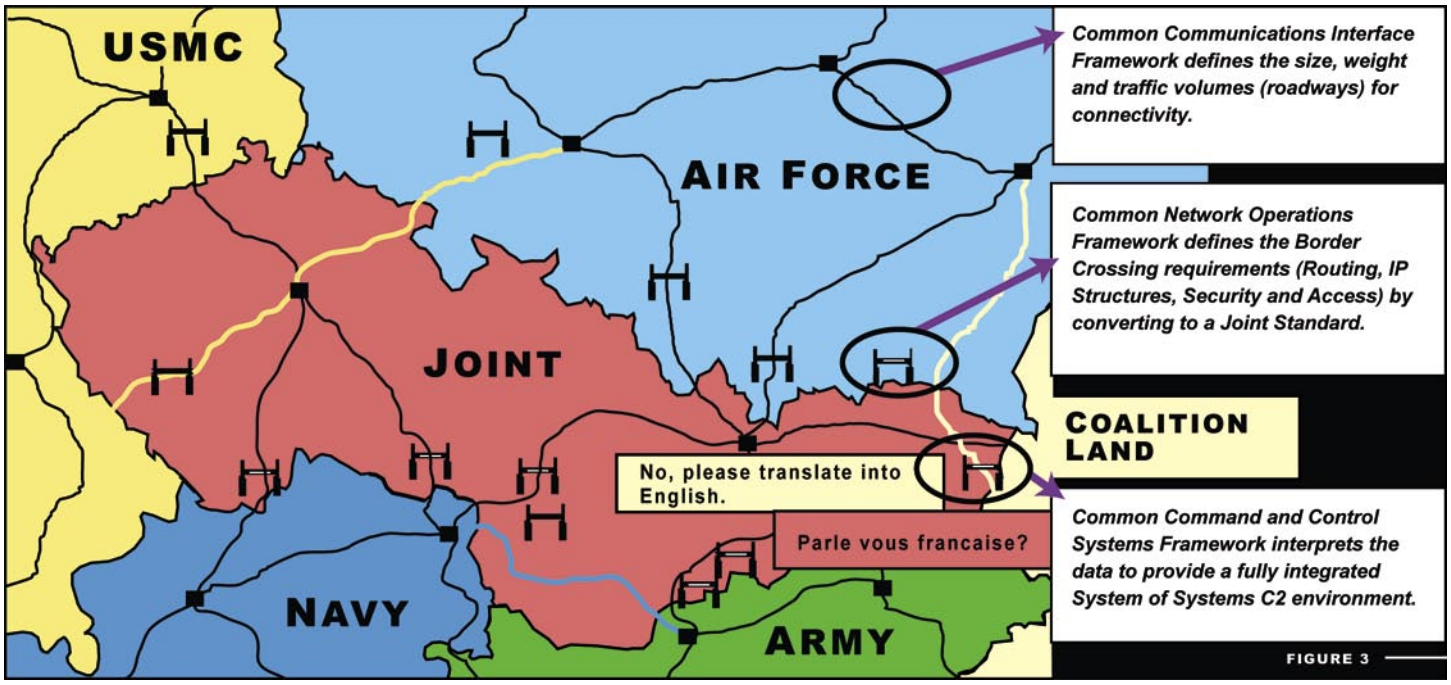
FIGURE 1

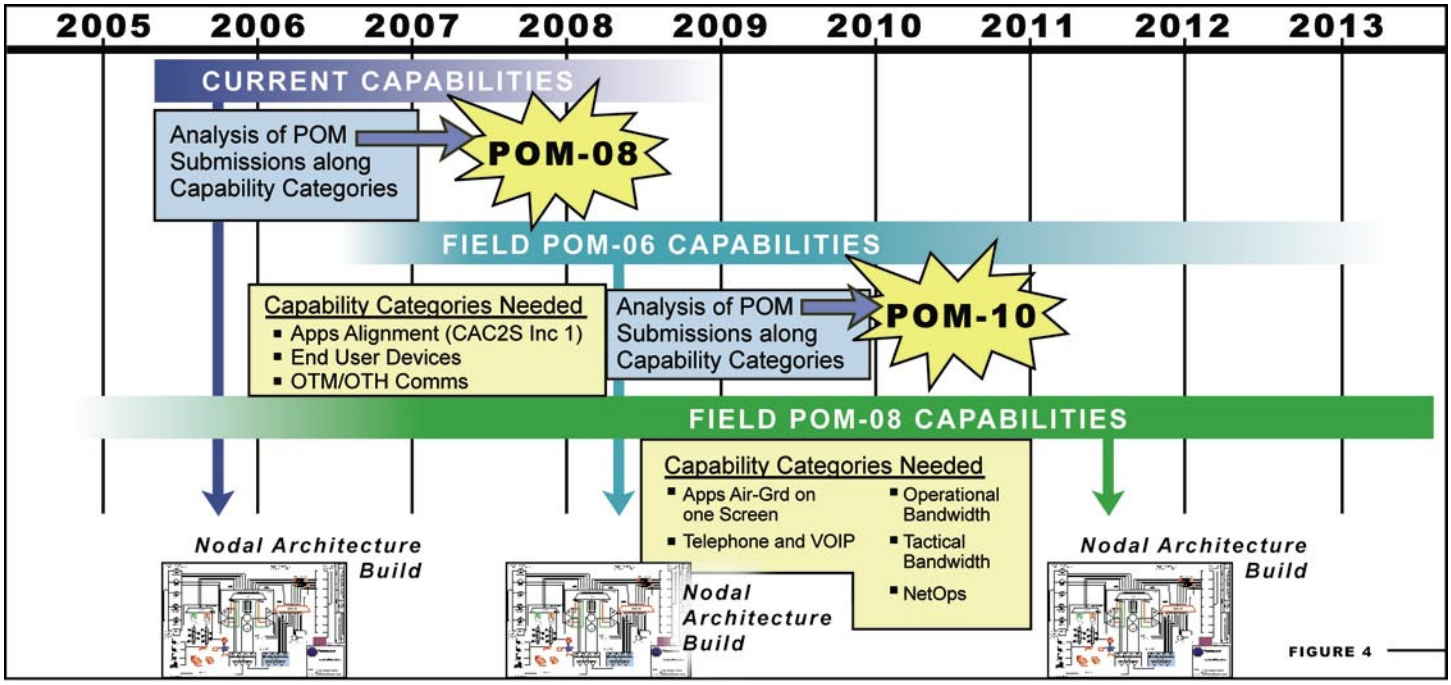


This framework identifies the methods used by the user to access data from a fully integrated system of systems. This framework is the cornerstone of the MAGTF C2 strategy and the joint command and control (JC2) effort. This could be envisioned as a translator at the United Nations, who ensures everyone understands what is said, regardless of the language spoken. This concept is illustrated in Figure 2.

The second framework defines an environment of common communications interfaces that describes the physical connectivity between disparate communication carrier systems. The Navy and Air Force have expressed interest in becoming signatories on an expanded memorandum of agreement (MOA) modeled after the Army/Marine Corps Common Communications Architecture.

Additionally, support to describe and evaluate communications access schema and the technical attributes required of this framework is being provided under the Office of Naval Research (ONR) sponsored Joint Virtual Laboratory-Network (JVL-N) effort.





Aligning each of the legacy systems, core programs and new initiatives with a capability category enables systems engineering and integration planners to analyze the capability they provide against the Marine Corps future architectural needs.

With the MOA between the services agreeing to collaborate on a common communications framework and the ability to test and model the approach through JVL-N, the physical connectivity interfaces can be standardized. This framework could be thought of as the state and interstate road network built to support the size, weight and traffic volume of the trucks moving their payloads between two or more sovereign countries. This concept is shown in Figure 3.

The last is a common network operations framework that defines the interfaces and tactics, techniques and procedures (TTPs) required for a dynamic network: security access and disassociation of users. Each of the services' architectures, FORCEnet, LandWarNet, Constellation Net, have unique network access requirements and, when applied within a combatant commander's region, must be coalesced into a Joint Annex K for theater-wide connection to the Global Information Grid.

MCCDC command and control infrastructure group presented this problem to the Senior Advisory Council of the Joint Test and Evaluation Program Office, and the Marine Corps was assigned as the lead for a new Joint Feasibility Study (JFS) known as the Joint Mobile Network Operations (JMNO) JFS. This Office of the Secretary of Defense funded effort will quantitatively analyze each of the services and coalition partners' network operations methods to determine the best of breed to create a common set of joint TTPs.

This evaluation, once charted as a joint test, is planned to be conducted at the Marine Corps Tactical Systems Support Activity (MCTSSA) using the Defense Research and Engineering Network (DREN) to connect the U.S. Joint Forces Command (USJFCOM) and services test facilities, such as the Central Technical Support Facility (CTSF), Space and Naval Warfare Systems Command (SPAWAR) and Langley Air Force Base to evaluate the proper joint network operations methods. This framework could be envisioned as the border crossing requirements between two or more sovereign countries. Data can be distributed uniquely within the separate countries, but must be converted to a standard network operations and security structure to pass between.

POM Alignment

Aligning each of the legacy systems, core programs and new initiatives with a capability category enables systems engineering and integration planners to analyze the capability they provide against the Marine Corps future architectural needs. This facilitates a proactive analysis of the systems and technical views to demonstrate how the system will integrate into the next generation MAGTF C2 nodal architectural build. It also provides a quantitative method to assist in the gap/overlap analysis necessary to support the Program Objective Memorandum (POM) Evaluation Group and POM Working Group reviews.

Using this process, the Marine Corps will be able to anticipate what capabilities are required to achieve the level of subscribers and service necessary at a given MAGTF C2 node to make informed decisions concerning investment offsets as shown in Figure 4.

Jeffery D. Wilson is the JMNO Feasibility Study Director. He develops joint tactical communications and network architecture at the Marine Corps Systems Command. He holds master's degrees in telecommunications systems and computer science. CHIPS

Birdtrack – COMPACFLT's Requisition and Asset Visibility Tool

By Meredith Omura

Commander U.S. Pacific Fleet (COMPACFLT), strategically located between the U.S. mainland and the western edge of the Pacific theater, supports a large forward-deployed naval force. COMPACFLT's challenge is to optimize material positioning and requisition fulfillment while maintaining fleet readiness for its area of responsibility, which includes Japan, Guam and South Korea. COMPACFLT is also providing assistance to the Marine air and ground components in Iraq and Afghanistan.

COMPACFLT's solution was to develop an inventory positioning analysis and asset visibility tool aimed at speeding the flow of replacement parts to ships and forward-deployed activities throughout the Pacific and Southwest Asia. This automated supply-chain management application named Birdtrack, originally developed to track average customer wait times for replacement parts, now includes a number of decision-making tools.

Before the development of Birdtrack, COMPACFLT used a spreadsheet to manually track its customer wait times. However, this process grew so unwieldy that automation was necessary. The manual version of Birdtrack was developed in 2000 to help determine how COMPACFLT was going to provide logistics support to units that operated in or deployed to the Pacific Fleet. The old spreadsheet version of the tool measured delivery times and yields from inception of the requisition through each pass point in the supply chain, helping to optimize the placement of material for use by forces in the theater.

In analyzing logistics support, the fleet supply team looked at up-front processing time, starting from when the requisition was generated to when it was recognized by the system, issue processing timeframes and transportation time from the issuing point to the end user. Finally they considered the time from when the part was received at the end user's location to when the user reported that it had been received. In this analysis, the team identified concentric circles of activity related to requisitions: shipboard activities in the center, shore-based activities close to the requisition point in the next ring, materials flowing from other Navy locations in the next ring and materials supported through the Defense Logistics Agency and General Services Administration in the outer ring.

A cohesive team headed by Capt. Thomas Traaen, director for Fleet Supply, COMPACFLT, in partnership with Naval Supply Information Systems Activity (NAVSISA) Customer Support Group Pearl Harbor, began work on the automated version of Birdtrack in May 2003. In just six months, the team had a proof-of-concept version in place that enabled users to make confident decisions.

In February 2004, COMPACFLT used the tool to identify logistics support provided by four Fleet Industrial Supply Centers located in Pearl Harbor, Yokosuka, San Diego and Puget Sound, as well as support provided by other sources of supply within the Department of Defense (DoD) and by DoD prime vendors. Additionally, Birdtrack recommended material that could be repositioned to provide improved customer support and responsiveness.

The Oracle-based application runs on commercial-off-the-shelf hardware and software. The hardware and software infrastructure has proven so flexible that the development team has been able to enhance it on an as-required basis. One set of users, for example, wanted to manage selected types of inventory. They provided a file of the inventory they wanted to manage, and the team provided them with the capability to categorize stock numbers of items, giving them a high-level view of item usage. The submarine and surface ship community wanted to track the various items being sent to Iraq and Afghanistan, how often they were sent, and how long it was taking to get the items there. The team categorized these requisitions to provide requisition analysis and material positioning information.

The high-level view of inventory usage, provided by Birdtrack, provides more sophisticated decision-making capabilities. This has enabled COMPACFLT to recommend strategic positioning of replacement parts at a lower cost and at a faster rate than previously done. When a fighting unit in Iraq needed parts in six days, COMPACFLT, using Birdtrack, measured the average customer wait time for the parts at approximately 18 days. Birdtrack then showed how that time could be reduced to less than six days by stocking line items in theater.

Recently, COMPACFLT used Birdtrack to respond to the December 2004 tsunami disaster. It tracked relief materials to better anticipate workload and monitor backlogs. According to Traaen, "Getting the parts to the ultimate user in six days, as opposed to 18 days, has a massive impact on unit readiness and minimizes disruption to the planned operational tempo."

The capabilities of Birdtrack will be the springboard for leveraging the Logistics Distance Support strategy toward greater efficiencies and increased business process improvements in support of the Navy's Human Capital Strategy. Additionally, Birdtrack capabilities are being considered as a means to support the strategic realignment and requirements of the joint services toward achieving their long-range goals.

The continuing use of Birdtrack to track, manage and provide the high-level view of item usage and inventory will result in a fleet that is ready for any challenge, any time, any place.

Meredith Omura is with the Naval Supply Information Systems Activity (NAVSISA) Customer Support Group Pearl Harbor.

CHIPS

A Lean Six Sigma Approach to COTS IT Acquisition

By Allen C. Tidwell

Commercial-off-the-shelf (COTS) information technology (IT) supports the business of the Department of Navy (DON). The approach to acquiring COTS applications is resource intensive and involves a number of rigorous steps. While these steps protect the investment in IT, they can slow the acquisition process and inhibit the DON's need to take advantage of modern technology in a timely manner. The Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RDA)) has established goals that will aid in expediting this process. However, it will require considerable effort on the part of the acquisition community to look at how we do business to find opportunities for improvement in the acquisition process.

Not Just "COTS IT"

This discussion does not address "shrink-wrapped" COTS, those applications that can be purchased through local supply or enterprise-wide licensing, but rather those COTS applications that provide the business capabilities for an enterprise. Such COTS applications are characterized by higher levels of complexity, requiring process engineering and change management for implementation as well as cultural change for end users. Additionally, such COTS applications are more costly and generate considerable oversight interest.

Since they are applicable to the enterprise, they require a higher degree of technical expertise because of the number and types of external interfaces and migration of legacy data to the COTS application. Due to this size and complexity, these COTS applications generally impact organizational missions as well as the capability of a large number of users to do their job.

How does the DON acquire large, complex and costly COTS products? The Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management Framework defines a complex matrix of the activities, processes and products necessary to acquire these products. While this model provides some flexibility to the acquirer, it is oriented toward the documentation, evaluation, justification and decision-making support for weapons systems where specifics are required to determine exactly what is to be acquired.

On the other hand, business IT requires a capability to support a business function that can be adjusted or adapted to a proposed COTS solution. The current acquisition processes do not provide a flexible methodology for the acquisition of COTS software for business use in which tradeoffs in providing the user the necessary capability must be accomplished in an expeditious manner.

Other groups within the Department of Defense (DoD) are looking into ways to modify the current acquisition processes to provide a more flexible methodology to acquire business IT. Figure 1 is a summary of why it is so important to streamline the acquisition process. So what can be accomplished within the context of the current processes to streamline the process and provide a more efficient and effective acquisition process for COTS IT?

Why Streamline COTS Acquisition

- ***No enterprise COTS information technology acquisition model***
- ***Current process is lengthy***
- ***The Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management Framework is more suited to weapons systems***
- ***Acquisition documentation development is cumbersome***
- ***High costs associated with program delays***
- ***Mandated by ASN (RDA)***

Figure 1.

Since no enterprise COTS information technology acquisition model exists, attempting to impose the current acquisition process on business needs often results in delays to program execution. Delays are costly resulting in reductions to the return on investment for as much as $165,000 per day for the Navy Standard Integrated Personnel System (NSIPS) or $3 million per month for the Defense Integrated Military Human Resources System (DIMHRS). In response to the need for an IT acquisition model, ASN (RDA) mandated that all Naval organizations follow the guidance in his Navy Marine Corps Acquisition Source Document – Blueprint for the Future. Several of the guidelines are below.

- Seek to continuously cut government and industry cost;
- Ensure that at least five Six Sigma events are held in each depot or industrial activity – government and industry;
- Seek to apply Six Sigma or theory of constraints in at least one area of business enterprise;
- Identify a set of internal metrics for the year, and plan to turn in a report card on these metrics;
  – One metric will be cost and schedule performance for all programs and activities under your leadership;
- Seek to reduce the volume of acquisition documents by 50 percent, including only essential, relevant information;
- Seek to have final approval of acquisition documents within the Navy Enterprise in no more than 90 days.

PEO-IT's Approach

In order to streamline the acquisition process and follow the guidance of the ASN (RDA), the Program Executive Office - Information Technology (PEO-IT) is applying the Lean Six Sigma methodology to the processes supporting the acquisition of business IT. For the purposes of this analysis, PEO-IT will use the Acquisition Documentation Coordination and Review Process as representative of the process since it touches all of the stakeholders involved and provides cross-functional participation.

Additionally, this process incorporates the ideals of the ASN (RDA) Source Document which defines that each PEO and program manager should have final approval for acquisition documentation within the Navy enterprise in no more than 90 days.

So what is "Lean" and how will it help us understand the process? Lean is a systematic approach to process improvement, which provides rapid benefits at all levels of an organization. It is a philosophy that forever changes the culture of organizations where it is properly implemented. And very importantly, Lean is a systematic method of identifying simple solutions to eliminate waste and produce services at the appropriate speed and quality to meet customer demands. (See Figure 2 for a summary of the principles of Lean Six Sigma.)

The PEO-IT applied this methodology to the set of processes described above, asking what is the value of the activities involved in the process. This generates a mapping of the value stream and an understanding of the sequence of activities and the triggers for that sequence. Figure 3 is an illustration of the approach used by the PEO-IT.

Following the documentation of the current state of the value stream, a team of Green Belts, who were trained on the improvement methodology of Six Sigma, broke the activities into phases for detailed analysis. They determined the inputs and outputs to each set of processes. The next step was to identify the wasteful activity within the processes that disrupts the natural flow, costs money, reduces efficiency, impedes communication and thus frustrates people. The goal was to ensure the value stream is not sub-optimized to serve the desires of people, individual processes or departments.

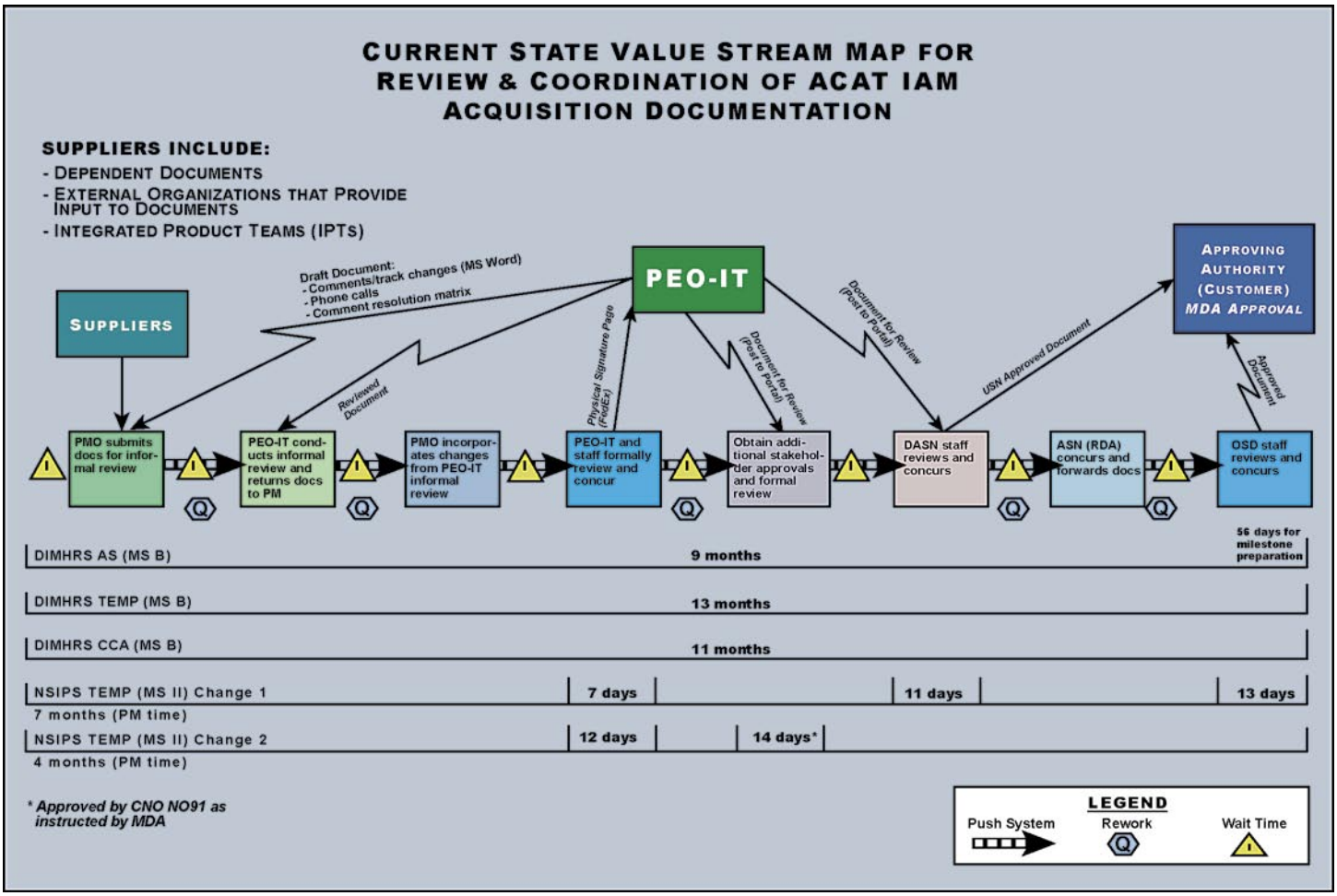
Principles of Lean Six Sigma

•Every job involves a set of processes
•Processes have inputs (from outside) and outputs (to customers, who are often within the agency)
•Efficient processes have flow — a natural, easy rhythm
•Wasteful activity disrupts flow, costs money, reduces efficiency, impedes communication and frustrates people.

Figure 2.

The Phase I Future State Value Stream Map, shown in Figure 4, depicts a reduction in the process from seven value stream steps to four and a 64 percent reduction in the work effort. More importantly it shortens the cycle time from the variable 3 to 11 months to 46 working days, in addition to the document creation time. The document creation time is derived from the work package associated with the work breakdown structure (WBS).

Figure 3.



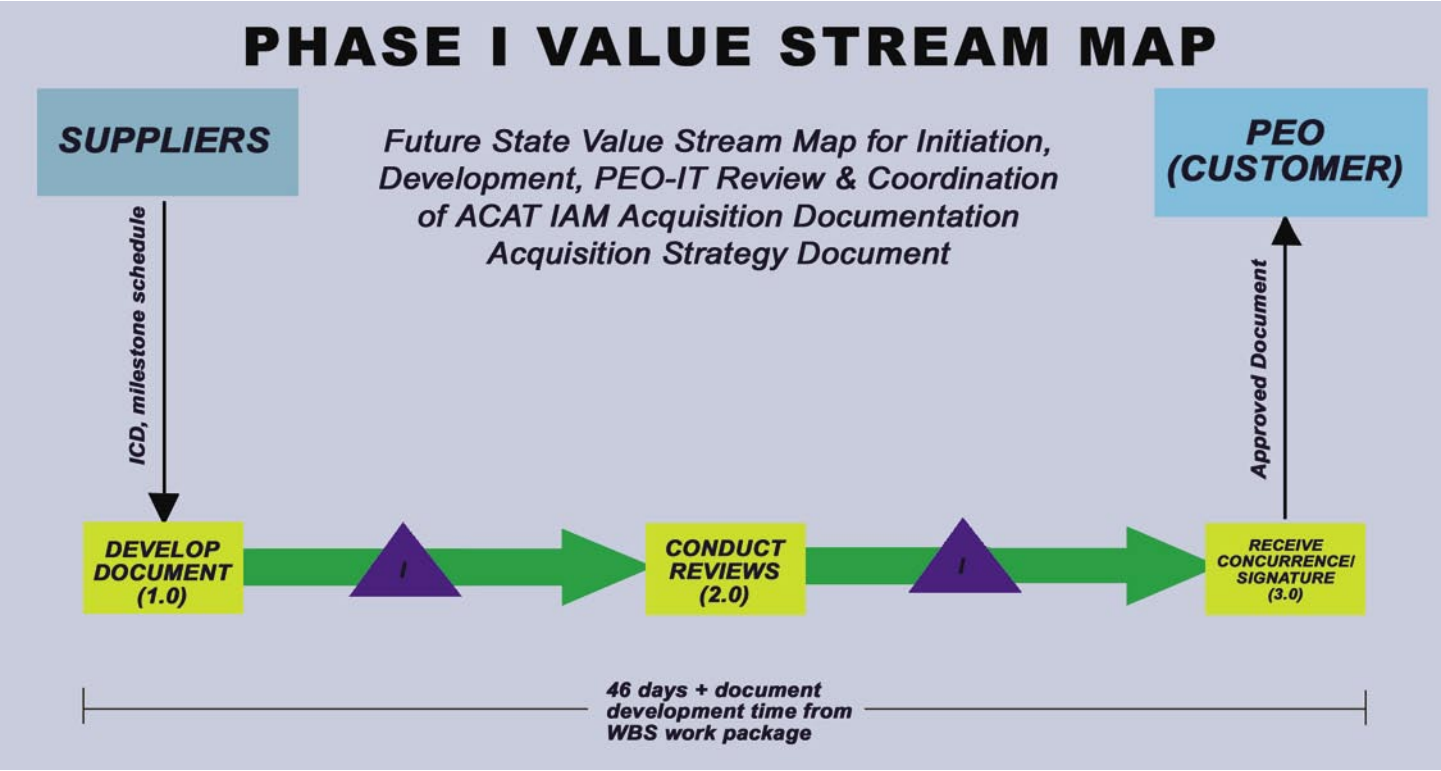


Figure 4.

Commercial-off-the-shelf information technology supports the business of the Department of Navy. The approach to acquiring COTS applications is resource intensive and involves a number of rigorous steps. While these steps protect the investment in IT, they can slow the acquisition process and inhibit the DON's need to take advantage of modern technology in a timely manner.

Other benefits include the development of a common business process within the PEO-IT for the initiation, development, coordination and review of acquisition documents with standardized tools to support the process. These standardized tools will also provide the capability to identify trends and cost and schedule impact through a set of established metrics.

This analysis also supports the PEO-IT effort to implement Software Acquisition Capability Maturity Model (SA-CMM) compliant processes. SA-CMM helps instill discipline into program and acquisition activities by building a set of repeatable processes — the *what* not *how*. Lean Six Sigma helps to identify those processes that are of value and becomes a default improvement model for ongoing process management.

The results of this analysis have application across the DON and DoD. It will form the basis for a new model in the acquisition of business information technology within the PEO-IT and support a paradigm shift in the acquisition process. The acquisition community will become involved earlier in the acquisition process with all stakeholders and customers.

The PEO-IT is participating with the Space and Naval Warfare Systems Command (SPAWAR) Lean Six Sigma Deployment Champions, the Deputy Assistant Secretary of the Navy for Logistics (DASN (L)) Transformation Team Leaders and the Office of the Assistant Secretary of Defense for Network Information Integration (OASD (NII)) to advance these concepts and communicate the results of the analysis across the Navy enterprise.

Lean Six Sigma efforts will accurately depict a microcosm of the model necessary to acquire and implement commercial-off-the-shelf IT as a basis for improvement. Lean Six Sigma efforts will enhance the acquisition process to enable industry and the DON to conduct business in a timely and efficient manner. The results of this effort, as directed by the ASN (RDA) and implemented within PEO-IT, will shorten the time to acquire COTS IT. It will support development of a model that streamlines the acquisition of COTS IT and provides a common process to support the acquisition community.

It is doing business smartly.

Allen C. Tidwell is a project director for Enterprise IT, Program Executive Office - Information Technology. CHIPS

The Defense Biometrics Identification System

By Michele Buisch

Because of the current problem with identity theft, verifying identification cannot be taken too lightly, especially when someone is trying to gain access to a military installation.

Such a security breach can mean life or death consequences. In December 2004, 22 people in an Army dining hall were killed, and many more were wounded when a suicide bomber wearing an Iraqi security forces uniform made his way onto the base in Mosul, Iraq, according to published reports.

A military guard checks the identification of a visitor using the Defense Biometric Identification System (DBIDS) wireless handheld device.

To secure Department of Defense (DoD) locations throughout the world, the Defense Manpower Data Center (DMDC) has developed an identification system that uses barcodes and biometrics to identify cardholders. The Defense Biometric Identification System (DBIDS) is a DoD identity authentication and force protection tool that is fully operational in military locations around the world. Commander, Fleet Activities Yokosuka (CFAY), Japan, is the latest military installation to pilot the DBIDS program and the first U.S. Navy installation to do so.

As DoD's largest physical access control system, DBIDS uses fingerprints and, in some cases, hand geometry to accurately identify personnel entering military installations. This system is more secure and quicker for personnel entering a military installation than flashing an identification (ID) card at a guard who then must compare the picture on the ID card to the cardholder. In addition to validating identity credentials, DBIDS also verifies authorizations and assigns access privileges based on identity, affiliation and the current threat level. Unlike the "flash pass" method, DBIDS reveals phony or expired ID cards and anyone unauthorized to access military installations. DBIDS identifies individuals who are wanted, barred from the installation or have other law enforcement alerts.

Active duty personnel, family members, DoD contractors and retirees are registered in DBIDS using their Common Access Card (CAC) or any DoD-issued identification credential. For people who do not have DoD credentials, but require access to the base, DBIDS provides a way to identify these individuals. Once these individuals, including foreign national employees, guests, frequent visitors (such as taxi or delivery drivers), children of DoD employees and U.S. Embassy personnel, are entered into the system, they are given a DBIDS identification card. DoD identification cardholders use the card they have already been issued, such as the CAC.

Originally called the Biometrics Identification System (BIDS), BIDS was created at the request of U.S. Forces Korea in 1998 as a force protection system in recognition of the tenuous truce between North and South Korea.

Since a peace treaty was never signed, and the peninsula is under an armistice, there are times of heightened concern that require an enhanced security posture. In response, by early 2000, BIDS was deployed to numerous locations in Korea. Then the Sept. 11, 2001, terrorist attacks on the United States resulted in full implementation at all military installations in Korea with scanning at all gates 24 hours a day.

In addition to enhancing force protection in Korea, DBIDS has assisted in the investigation of several crimes. In one case, the DBIDS audit capability helped law enforcement officials identify two suspects in the murder of an active duty Army Soldier based on the times the suspects entered the base. Once identified, one of the suspects admitted to committing the murder.

At another Korean installation, DBIDS identified an individual who had stolen a vehicle and a CAC inside the vehicle. Two days after the vehicle and the CAC were reported stolen the information was entered into the system. When the individual attempted to enter the installation, DBIDS alerted the guard to the stolen CAC and the person was apprehended.

At CFAY, two barred individuals and two wanted individuals were identified trying to enter the installation shortly after the guards began using DBIDS. In addition, the audit capability was used to investigate the beating of a Sailor off base.

Although DBIDS has proved successful in Korea and at other military installations, Patrick J. McGee, manager for Asia Operations, DMDC, said DMDC still faces the challenge of demonstrating the system's benefits and ease of use. "Confidence in the system is paramount, and while DBIDS does prove itself quickly once put into action, overcoming the resistance to change paradigm is sometimes a difficult thing," McGee said. "Once put into use, however, users can't believe they lived without it."

The system works like this: The guard scans the card's barcode and/or the individual's fingerprints *(depending on the Force Protection Condition (FPCON) level and installation policy)* using a wireless, handheld device. Then the guard reviews screen displays to verify that the ID card is an authorized DoD credential

that is not expired, lost or stolen. It also verifies the individual's identity and that he or she is not wanted, barred or suspended from entering the installation, and has access to the installation under the Force Protection Condition.

If a restriction has been placed on the individual, the screen display will tell the guard how to proceed. "DBIDS virtually eliminates the threat of unauthorized persons gaining access; stopping them at the front door so to speak," McGee said. "And these operations not only act as a physical protection measure but also as a deterrent."

The screen displays include color photo, identity information, color-coded message screens, audible sounds to quickly and easily alert the guard of the individual's status and a variety of administrator capabilities. In addition, the text on the screens is multilingual. "All this occurs in a matter of two to three seconds of the scan, less time than it takes the guard to visually validate an ID card," McGee said.

The scalable system can cover a building, installation or entire theater of operations. The majority of DBIDS sites, including CFAY, use fingerprint scans when the FPCON or installation policy dictates that additional checks are required. However, DBIDS Kuwait uses hand geometry because of the difficulty encountered in trying to capture usable fingerprints from laborers.

At CFAY, DBIDS equipment was deployed in 2004 with the opening of a registration center. In April, gate access and the Visitor Control Center were installed. Nearly 32,000 people are registered at CFAY in DBIDS and approximately 22 percent are DBIDS cardholders. The remainder are DoD identification cardholders, according to McGee.

Fully operational DBIDS installations include: U.S. Armed Forces Europe; U.S. Armed Force Korea; Fort Hood, Texas; Fort Polk, La.; Monterey Peninsula, Calif.; and U.S. Joint Task Force, Southwest Asia (Kuwait and Qatar).

DBIDS expansion is an ongoing process throughout many areas of the DoD. This expansion has led to the creation of the new Identity Authentication Office within DMDC, which is dedicated to managing DBIDS. In addition to working on improved versions of the system, the office is investigating linking to other government identity authentication systems to share data and digital fingerprints using CAC chips for authentication.

New DBIDS deployments are underway at Yokota Air Base in Japan and other areas in Southwest Asia, according to McGee.

For more information about DBIDS, please visit the DBIDS Web site at https://www.dmdc.osd.mil/dbids/.

Michele Buisch is a contractor supporting the Department of the Navy Chief Information Officer. CHIPS

Implementation of PKI Authentication for DADMS

The use of the Public Key Infrastructure (PKI) and the Common Access Card (CAC) for accessing the Department of the Navy Applications and Database Management System (DADMS) became mandatory Sept. 6, 2005, according to a coordinated naval message: AL NAVADMIN (UC) R 012042Z SEP 05 issued by the Department of the Navy Chief Information Officer (DON CIO) and the Assistant Chief of Naval Operations for Information Technology (ACNO-IT).

This action is being taken to provide additional assurance that only personnel authorized by the current DADMS access control process have access to the network and application information contained in DADMS.

DADMS users must either have a valid PKI software certification (softcert) installed on their system or use a CAC reader and software to provide the authentication.

DADMS users are advised that PKI softcerts have an expiration date at which time the softcert will become invalid. Softcerts are no longer being issued. Once the softcert expires users will be required to use their CAC for authentication.

Navy Marine Corps Intranet (NMCI) desktop computers or laptops are provided with a CAC reader and ActivCard Gold software required for authentication purposes. In addition to the CAC and ActivCard Gold software, users must enter their individual personal identification number (PIN) code which they created when their CAC was issued.

Users accessing DADMS from non-NMCI computers must have a CAC reader attached to their computer as a peripheral and have the ActivCard Gold PKI Common Access Card software installed to provide the authentication.

PKI authentication is in addition to the user identification (ID) and password currently required to log onto DADMS. PKI authentication does not change the current method of obtaining access to DADMS. Any DADMS user ID and password problems should still be reported to the DADMS help desk. CAC problems are to be reported to command CAC issuing activities since the DADMS help desk cannot assist with CAC problems.

Use of the CAC to access DADMS can be tested immediately and is encouraged to ensure CAC problems have been addressed.

For additional information contact the ACNO-IT at (703) 604-7813. CHIPS

NMCI Announces Second Quarter Customer Satisfaction Survey Results

By Denise Deon

The latest Navy Marine Corps Intranet (NMCI) customer satisfaction survey results continued to show slow but steady improvement in user satisfaction with NMCI and EDS related services. For the second quarter of 2005, overall NMCI customer satisfaction increased two percent to 76 percent. Satisfaction for incentive-related questions, those questions focusing solely on EDS' services, also increased to 78 percent from the previous result of 76 percent in March 2005.

More than 118,000 surveys were distributed to NMCI users, generating 18,562 completed surveys for a response rate of 15.7 percent. The June 2005 survey was the second consecutive survey to include Marine Corps users in its distribution. Overall satisfaction for the Marine Corps rose to 74 percent, up from 69 percent from their first survey participation in March 2005.

This quarter marked the first time a Department of Navy (DON) organization attained the 85 percent satisfaction level, which enables EDS to earn incentive payments for those organizations' full performance seats as of June 30, 2005. The first two organizations to reach this level of satisfaction are Commander Naval Installations (CNI) and the Naval Education and Training Command (NETC).

"The slow but continuing rise in NMCI customer satisfaction ratings is encouraging and reflects the hard work of our integrated Navy, Marine Corps and EDS team. We must remain focused and vigilant as we continue implementing and improving NMCI for our customers," said Rear Adm. James B. Godwin III, Direct Reporting Program Manager (DRPM) for NMCI.

NMCI customers are overall most satisfied with the professionalism of EDS personnel (88 percent); and are least satisfied with their inability to make changes to their information technology environment (61 percent), which largely equates to the move/add/change (MAC) process. This same category was also the area that showed the greatest improvement, with satisfaction rising five percent from 56 percent in March to 61 percent in the latest survey results.

"The improvement in customer satisfaction is a direct reflection of the ongoing effort being made to improve the program. Our clients' responses are very valuable to us," said EDS enterprise client executive, Mike Koehler. "We are building on our experience and feedback [from customers] to better understand our client's needs and address key issues. The Navy, Marine Corps and EDS continue to work together to improve delivery to our customers.

Other key areas targeted for improvement include: NMCI training, network reliability and software availability. Several initiatives are underway to address these issues, including the organization of several user focus groups to address training needs and areas for improvement and a pilot program targeting customer satisfaction improvement.

Focusing on improving current services, anti-SPAM software was recently implemented across the enterprise. In addition, the ability to remotely log-in utilizing high-speed access (known within NMCI as broadband unclassified remote access service (BuRAS)) was recently pushed to one segment of the NMCI population with the entire rollout occurring over the next few months.

Other new services planned for delivery later this year include a technology refresh for older seats and rolling out Windows XP.

For more information contact DRPM NMCI Public Affairs at (703) 685-5527.

NMCI by the Numbers - August 2005

Of 6,021,923 messages processed by Ironport during a seven-day period, there were 1,271,822 known SPAM e-mails; 2,990 suspected SPAM e-mails and 4,747,111 non-SPAM e-mails.

NMCI Implements DON Enterprise Anti-SPAM Solution

The Navy Marine Corps Intranet began an enterprise-wide anti-SPAM solution during summer 2005 to provide NMCI users with SPAM detection and filtering. The SPAM protection filters messages that include words or phrases of known and suspect Internet SPAM and words from defined content filter dictionaries.

The anti-SPAM solution started with a three-month transition period. During this transition, the subject line of all known and suspect SPAM messages was tagged, so it could be easily identified by the user and delivered to the user's Microsoft Outlook inbox.

Following the three-month transition period, e-mail tagged as known SPAM is deleted and suspect SPAM is routed to a quarantine server, instead of the user's Outlook inbox. Users will receive a daily SPAM Quarantine Summary Report with a link to the quarantine server for each suspected SPAM message. By following this link, the user can view the message and, if desired, release it to his or her inbox. If users take no action, SPAM messages left on the quarantine server will be deleted after seven days from the date of receipt.

For more information, see the NMCI Anti-SPAM Solution Quick Reference Guide, available from an NMCI computer at http://homeport/userinfo/downloads/userinfo/Anti_SPAM_User_Guide.pdf, or call the NMCI Help Desk at 1-866-THE-NMCI or 1-866-843-6624. CHIPS

NMCI Spyware and Virus Protection Upgrade Begins

Navy Marine Corps Intranet users are receiving enhanced virus protection and relief from Spyware and Adware. On Sept. 16, NMCI began rolling out an upgrade to Symantec AntiVirus (SAV). The updated software provides proactive virus and vulnerability-based detection of blended threats, Spyware, Adware, unauthorized network access and mass-mailer attacks. The rollout is currently scheduled to be complete by the end of December.

The solution, which runs almost invisibly after installation, contains an update of NMCI's existing SAV 8.1 to SAV 10. Users will be able to conduct a scan for viruses on their own or can allow the application to scan continuously for security risks.

Users will receive notifications if any infections to their workstations have been detected.

This upgrade is part of Symantec Client Security, which also includes Symantec Client Firewall. The software provides real-time protection to dramatically reduce the risk of Spyware reaching the system and provides the automatic removal of most current infections, enabling security risks to be easily disposed.

Applications or files found affected by viruses and Spyware are then cleaned or quarantined. CHIPS

Maritime Integration Center

Increasing the Fleet's Capabilities with Reach Back

By Dean Wence

The Navy's Fleet Information Warfare Center (FIWC) established the Maritime Integration Center (MIC) to provide information operations (IO) expertise and resources to deployed forces. The MIC acts as a central point for global maritime IO awareness. FIWC already deploys unit members to carrier strike group (CSG) and expeditionary strike group (ESG) staffs, numbered fleet commanders, special warfare units and Marine Expeditionary Force (MEF) units to integrate IO into fleet exercises and real-world operations. With the establishment of the MIC, the fleet has reach-back capability to IO expertise and a second set of eyes for IO planning.

The MIC, recently relocated to the Naval Network Warfare Command (NETWARCOM) Network, Information Operations and Space Center (NIOSC) at Naval Amphibious Base Little Creek, Va., is now a 24/7 operation. The MIC watch focuses on the five core competencies of IO: psychological operations (PSYOP), military deception (MILDEC), electronic warfare (EW), computer network operations (CNO – attack/defense) and operations security (OPSEC).

The NIOSC is a brand new, state-of-the-art operations center that will manage worldwide naval operational and technical support across strategic, operational and tactical levels. Ultimately, the NIOSC will promote data sharing and foster an environment of collaboration required to plan and respond to current and future threats.

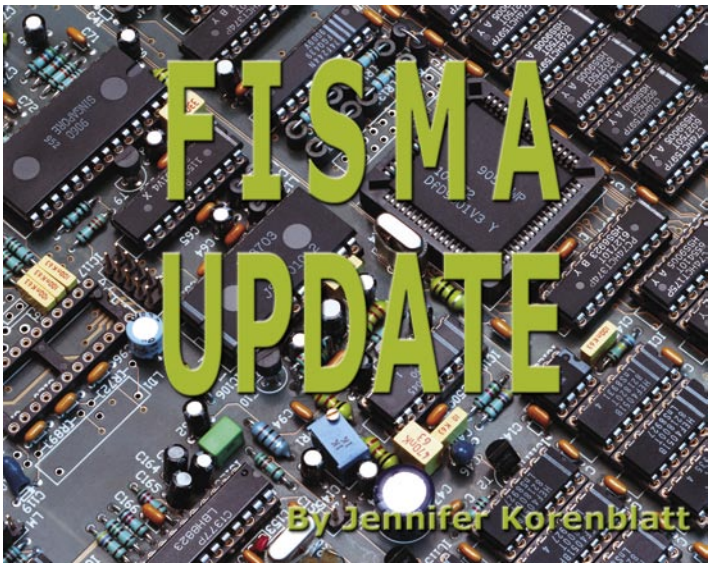
Through the deployed FIWC teams, the MIC acts as an integrated knowledge repository where knowledge and information can be pushed or pulled to the fleet. MIC functions include: modeling, access to historical data and subject matter experts, collaborative IO planning, reach-back capabilities, and monitoring for chat rooms, portals and Web sites.

FIWC retains the expert knowledge in the MIC by ensuring knowledge is passed to deployed watch staffs. MIC watch officers and watchstanders are usually senior unit members who start out as ship deployers on an IO team. When the members return from deployment, they provide a post deployment brief which is incorporated into the training for outgoing deployers and fleet IO courses. This ensures that IO courses and deployers always have the most current information. By the time unit members become MIC watchstanders, they have been on one, two and sometimes three deployments. Passing on this knowledge ensures watchstanders understand what the MIC deployers are doing, and it helps watchstanders anticipate their needs.

By using this approach, the MIC has already reduced the manpower needed for deployed IO teams. Before the MIC was established, FIWC was deploying one officer, one chief petty officer, two petty officers and a computer network defense asset per deployed CSG or ESG. Now, the MIC has eliminated the need to deploy two petty officers. The goal is to eventually deploy one person to provide MIC support. FIWC is also integrating Reservists into the MIC watch, taking advantage of the Reservists' military and civilian experiences, thus reducing the workload for active duty personnel.

The MIC has already supported real-world operations, such as tsunami relief through Operation Unified Assistance and operations in Iraq and Afghanistan. Joint and international exercises supported include Summer Pulse Exercise 2004, Terminal Fury and Joint Task Force Exercise. Whether it is providing collaborative IO planning to the Joint Force Maritime Component Commander, Information Warfare Commander or giving NETWARCOM an overall global IO picture, the MIC is a knowledge asset that is making a difference for the warfighter.

Dean Wence is a knowledge management program analyst with the Department of the Navy Chief Information Officer. CHIPS



FISMA Fact – "Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"

– Federal Information Security Management Act of 2002

FISMA Fundamentals

The Department of the Navy (DON) is required to comply with the Federal Information Security Management Act of 2002 (FISMA) also known as Title III of the E-Government Act of 2002. FISMA requires each federal agency to provide information security for its information technology (IT) assets. The purpose of FISMA is to provide a framework for enhancing the effectiveness of information security in the federal government. FISMA also provides a mechanism for effective oversight of federal agency information security programs.

The director of the Office of Management and Budget (OMB) oversees FISMA compliance. The DON reports FISMA status to the Assistant Secretary of Defense (Networks and Information Integration) (ASD/NII), which consolidates all Department of Defense (DoD) input and reports to OMB. This article explains the importance of accurate and timely reporting of FISMA data.

FISMA Reporting Using the IT Registry

The DoD Information Technology Registry serves as a technical repository to support chief information officers' (CIO) assessments and maintains an IT system inventory to comply with Congressional requirements. The Office of the Secretary of Defense (OSD) uses data from the DoD IT Registry to compile reports regarding FISMA status.

The DON uses its own DON IT Registry to record the certification and accreditation (C&A) status of mission critical (MC), mission essential (ME), and mission support (MS) DON systems and networks. The DON uploads this data quarterly (March 1, June 1, Sept. 1 and Dec.1) into the DoD IT Registry. Data from the DoD IT Registry is used to report FISMA status for the entire DoD to OMB and Congress. The DON must improve the recording and reporting of IT systems data to increase compliance with OSD and OMB FISMA requirements. Punctual and accurate reporting of DON IT systems is key to validating DON compliance with security requirements and justifying funding for IT security tasks.

Key Issues for FISMA Compliance

Three key areas of FISMA compliance that affect the DON are: (1) reporting the certification and accreditation status of DON IT systems; (2) the DON Plan of Action and Milestones (POA&M); and (3) the status of information systems privacy management.

The Secretary of the Navy directed the DON to reach and sustain 90 percent or greater certification and accreditation status for DON systems and networks. This C&A compliance rate is required by the President's Management Agenda for 2005.

OMB requires federal agency CIOs to monitor the status of information security weaknesses, including the lack of full accreditation in POA&Ms for each system and network. OMB reviews POA&Ms for systems for which a Capital Asset Plan and Justifications (known as OMB Exhibit 300) is submitted. The Department of the Navy Chief Information Officer (DON CIO) retains other system POA&Ms and provides a summary report to OSD quarterly.

The DON CIO is responsible for DON compliance with Section 208, Privacy Provisions of the E-Government Act of 2002. OMB Memorandum 03-22, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," issued Sept. 26, 2003, provides OMB requirements for compliance with the E-Government Act and states the conditions in which a Privacy Impact Assessment is required for an IT system. The DON CIO has developed a Privacy Impact Assessment, which is available on the DON CIO Web site. *(See the Reference Links box for information.)*

In fiscal year 2005, OMB introduced a new privacy management section of FISMA reporting, which removes privacy compliance reporting from the annual E-Government Act report to the annual FISMA report.

OMB FISMA Guidance for FY 2005

In 2005, OMB issued M-05-15, "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" to facilitate FISMA reporting. This memorandum provides reporting instructions and FISMA and Privacy Management reporting templates.

FISMA requires system owners to annually review certification and accreditation status of all systems, including those that are accredited (i.e., granted an approval to operate). This annual review must include all items listed in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," issued Feb. 6, 2003.

FISMA requires that certification and accreditation statistics for contractor and government systems be reported separately. Contractor systems are information systems used or operated by a contractor of a federal agency or other organization on behalf of the agency. An example of a contractor system is the Navy Marine Corps Intranet.

DoD FISMA Guidance for FY 2005

In addition to the OMB requirements for 2005, the Office of the Secretary of Defense issued FISMA guidance to assist the DoD in complying with the new requirements. There is a new requirement for system owners to report the status of mission support IT systems in the DoD IT Registry, in addition to the current requirement to report mission critical and mission essential systems. With this new requirement OSD seeks to comply with the President's Management Agenda and the E-Government Act, both of which mandate that all systems be registered in the DoD IT Registry.

DoD FISMA Guidance for FY05 requires submission of quarterly Plan of Action and Milestones to OSD for the number and category of information security POA&Ms and for activities leading up to accreditation for:

√ Exhibit 300 systems that are not fully accredited.
√ Exhibit 300 systems that receive a security score of three or lower on a scale of one to five.
√ Systems in the IT Registry that require certification and accreditation, but do not have an approval to operate.
√ Systems with material weaknesses or significant deficiency in the DON's information security posture. These items might be identified in an audit or by internal review.

OSD is updating this guidance and it should be issued in fall 2005. The new guidance will be posted on the DON CIO Web site when it becomes available.

The Office of the Secretary of Defense develops and reports summary data from all POA&Ms reported to the DoD, to OMB and Congress in the annual DoD FISMA Enterprise Plan of Action & Milestones. DoD and DON POA&M guidance is based on OMB Memorandum M-04-25,"FY 2004 Reporting Instructions for FISMA." OSD mandated that all defense agencies and military departments must register all mission critical, mission essential and mission support systems in their respective IT registries and report the status of these systems to OSD by Sept. 1, 2006.

The "DON FY 2005 Information Technology (IT) Registration Database Guidance" provides details on what must be entered in the database and who is responsible for entering it.

DON FISMA Reporting Responsibilities

FISMA reporting is required at all levels of the DON.

• The DON CIO, Mr. David Wennergren, reports DON FISMA status to OSD, and provides supplemental reporting information to the DON Privacy Act Official in support of the DON privacy management reporting section of FISMA.

• The DON Deputy CIO for Policy and Integration, Mr. Robert Carey, is the DON Senior Information Assurance Official. He is responsible for the DON information security program.

• Program Managers, System Managers, Command Information Officers, and Functional Area Managers are responsible for updating the FISMA data in the DON IT Registry.

Dates to Remember

Oct. 7, 2005 – FY 2005 Annual FISMA Report due to OMB.

March 1, June1, Sept.1 and Dec. 1 – Agency CIOs are required by law to report quarterly to OMB with POA&M status. OSD forwards the data to OMB on the 15th of these months.

Sept 1, 2006 – The OSD requires the DON to upload all of its certification and accreditation data on mission support systems into the DoD IT Registry by this date.

Oct. 15 – DON CIO certifies with DoD CIO that the DON IT Registry data are accurate and complete.

Reference Links

Subchapter III of Chapter 35 of Title 44, U. S. Code, "Federal Information Security Management Act (FISMA) of 2002" (PL 107-347). Web link: http://csrc.nist.gov/policies/FISMA-final.pdf.

Section 208, Privacy Provisions, of the E-Government Act of 2002. Web link: http://www.whitehouse.gov/omb/memoranda/m03-22.html/ and scroll to Attachment B.

OMB Memorandum M-03-22, "Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," of Sept. 26, 2003. Web link: http://www.whitehouse.gov/omb/memoranda/m03-22.html/.

OMB Memorandum M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," of Aug. 23, 2004. Web link: http://www.whitehouse.gov/omb/memoranda/fy04/m04-25.pdf.

OMB Memorandum M-05-15, "FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," of June 13, 2005. Web link: http://www.whitehouse.gov/omb/memoranda/fy2005/m05-15.html/.

DON FY2005 IT Registration Database Guidance, March 2005. Web link: http://www.doncio.navy.mil and search for "IT Registration."

DON Privacy Impact Assessment Summary Version 1.1. Web link: http://www.doncio.navy.mil and search for "Privacy Impact Assessment."

Compliance is Mandatory

DON compliance with FISMA requirements is mandatory and ensures that the Department performs due diligence in gathering and reporting data on the security of its IT systems. The timely and accurate reporting of DON FISMA data to DoD and OMB is essential to demonstrating the DON IA posture. FISMA requirements change, and the DON must remain vigilant of the new requirements each year to ensure compliance.

Jennifer Korenblatt is a contractor supporting the DON CIO Information Assurance Team.

The Naval Surface Warfare Center Dahlgren Division

The U.S. Marine Corps, Army, Coast Guard and National Guard select NSWCDD as their primary CWID 2005 site

By John J. Joyce

The Naval Surface Warfare Center Dahlgren Division (NSWCDD) is uniquely positioned to help navigate the Navy's road to transformation. Its broad spectrum of resources, including its workforce and infrastructure have made it a premier naval scientific and engineering institution dedicated to solving a diverse set of complex technical problems confronting the warfighter.

The NSWC Dahlgren CWID lab site team, back row (l-r) Robert Hill, Dennis Warne (site manager), Mike Cajohn (Marine Corps liaison), Hank St. Laurent (site lead engineer) and Benjamin McCormick. Front row (l-r) Mike Remington, Ralph Thompson (deputy site manager), Sean Cunningham, Steve Horowitz and Timothy Williams.

NSWCDD fills a major role in the annual Coalition Warrior Interoperability Demonstration (CWID). The demonstration tests and evaluates technologies and capabilities focused on selected core objectives defined by combatant commanders.

"This is the seventh year that NSWC Dahlgren has been a JWID/CWID site. We began in 1999 with only the Marine Corps. Since then, we have hosted additional services and continue to build successful working relationships with a multitude of commands and organizations," said Capt. Joseph McGettigan, commander of NSWCDD.

CWID Participants

The demonstration involved 26 countries, including Australia, Canada, New Zealand, United Kingdom and many NATO nations. Participants interacted in a scripted scenario over a global network at 30 sites around the world. For the first time in CWID 2005, decision makers from government agencies, national and international law enforcement organizations and first responders worked alongside our traditional military allies.

"I got the impression that everyone here was trying to help the guys at the front — to save the lives of warfighters, said New Zealand Army Lt. Col. Tony Hill.

More than 40 technology trials were assessed for interagency information sharing and coalition interoperability under the leadership of the host combatant commander, U.S. Northern Command (USNORTHCOM), Peterson Air Force Base, Colo., and the executive agent, the Defense Information Systems Agency (DISA), Arlington, Va. USNORTHCOM works with key interagency partners to identify new ways to improve cooperation, coordination and information sharing.

CWID focused on homeland security (HLS), homeland defense (HLD) and coalition interoperability. U.S. Joint Forces Command (USJFCOM) provided planning and execution oversight for the worldwide event that was conducted in a simulated operational environment June 13–23, 2005.

"Location and cost effectiveness have been crucial to the success and growth of CWID at NSWC Dahlgren. It is good economics for us to host more than one service, the Army, Marine Corps, Coast Guard, National Guard and Navy, because the services share a lot of the same systems: CONOPS (concept of operations), infrastructure and the networks required for CWID," McGettigan said.

Secret Sharing

There were two major network enclaves for CWID: (1) The warfighter enclave – the secret network of coalition and guest nations, and (2) The HLS/HLD enclave – the network for homeland security. The Coalition Secret Network or "purple" enclave stood up for the first time to release secret classified information to the 26 coalition members. Nations were grouped into communities of interest separated by flexible, cost-effective virtual private networks and firewall managers that permitted controlled, protected communications, instead of security enclaves that required the use of Type-1 encryption devices and costly approved guards.

The purple network was a huge success, according to DISA CWID Joint Management Office Director, Air Force Lt. Col. Buddy Dees. "We had a stronger coalition exchange of information since everyone agreed that information put on the purple enclave was releasable to all participants of a coalition force," Dees said. "We were able to show that the technology is trustworthy."

A "black" domain for unclassified sharing was also used throughout the worldwide demonstration. Warfighters from Norway to New Zealand assessed the effectiveness of 52 interoperability trials in a realistic environment for possible operational use in the Global Information Grid within 18 months of the execution period.

CWID organizers required each trial to address at least one of the demonstration's core objectives: mission assurance; situational

awareness; multilevel/multidomain protection; collaborative information environment; intelligence, surveillance and reconnaissance dissemination; wireless security; language translation; and integrated logistics. What's more, the CWID scenario merged aspects of HLS and HLD with coalition operations so the demonstration could be used as a proving ground for emerging technologies through the entire spectrum of first responders.

Meeting the goal to move promising technologies through the CWID process from the demonstration to the field within six to 18 months has been a persistent challenge in the wake of past demonstrations and this CWID is no different.

"According to the Naval Sea Systems-NSWC Enterprise Charter, we want to accelerate technology into affordable capability for the warfighter. At Dahlgren, we apply research and development, science and technology, and test and evaluation to deliver technological solutions to today's warfighters and reshape the future Navy," McGettigan said.

Fielding promising CWID technologies results in a combined effort that includes DISA, the Joint Staff, Joint Systems Integration Command and USJFCOM's Command, Control, Communications, and Computer (C4) Systems Directorate (J6) and Joint Requirements and Integration Directorate (J8).

Defining Roles and Responsibilities

According to Dennis Warne, CWID site manager for the NSWCDD lab, there were some challenges in the HLD/HLS scenarios in dealing with county and state first responders, who do not have DoD clearances or equivalent security clearances.

"What is considered sensitive, classified or unclassified in a multifunctional environment? Another challenge in CWID is how do you define warfighters? This is not a real term when you are dealing with fire, police, rescue or emergency personnel. They are not warfighters, at least not in the traditional sense," Warne said. "A lot of these questions still need to be determined by policy, laws, concept of operations, and tactics, techniques and procedures."

Warfighter Collaboration

At Dahlgren, active duty and Reserve warfighters collaborated with industry representatives to discover innovative ways to apply the solutions they were testing on the Combined Forces Battle Laboratories Network, which merged HLD and coalition task force (CTF) operations into one integrated scenario.

The scenario consisted of two parts: one for HLS and HLD and the other for the CTF. In the HLS/HLD scenario, USNORTHCOM with local, state and federal agencies responded to terrorist attacks within the United States. These fictitious attacks were tied to conventional U.S.-led CTF operations on another continent.

For the CTF portion of the demonstration, CWID provided a framework to facilitate interoperability trials through a full range of military operations conducted by U.S. and coalition forces. CTF operations were set in a hypothetical context that involved imaginary countries. Contrasting the theoretical backdrop was a very real focus on valid capabilities that can be delivered to the warfighter quickly.

L-R: Marine Corps Lt. Gen. Robert Shea, Joint Staff Director, Command, Control, Communications and Computer (C4) Systems (J6); Army Maj. Gen. Dennis Moran, Joint Staff Vice Director for C4; and Army Maj. Corey Brumsey are briefed by Information Systems Technician 3rd Class Ricky Payne at NSWCDD during CWID trials.

"This CWID approach fits in with the way that we harness the intellectual capital of our workforce to put technology into the hands of the warfighter to solve their problems today. CWID also fits in with the work that we do designing the Navy *Next* and the Navy after that. Many joint efforts in both the RDT&E (research, development, test and evaluation) realm and operational tasks are performed at NSWC Dahlgren. Our customers reach beyond the Navy to the Office of the Secretary of Defense, the other services and other government agencies," McGettigan said.

DISA managed the event's day-to-day operations and engineered the demonstration network. The agency set up a demonstration architecture that enabled controlled and protected communications as prescribed by operational requirements and national security policies.

According to Warne, there were no disappointments with any of the technologies tested.

"We don't look at them that way. They either executed to their requirements or they didn't. We do not want to drop a trial just because it did not come up number one or number two. Some are just more mature than others, and some need to be reassessed," Warne said.

The next CWID is planned for May 30–June 23, 2006. For more information, go to the CWID home page at http://www.cwid.js.mil/.

For more information about NSWCDD go to http://www.nswc.navy.mil.

John Joyce is part of the NSWCDD Corporate Communications Office and a Navy Reservist serving with the USJFCOM Joint Public Affairs Support Element.

CHIPS

Can You Hear Me Now?

The Foundation of Future Spectrum

By the DON CIO Spectrum Team

The radio frequency electromagnetic spectrum is more important to the Department of the Navy (DON) today than it has ever been in the more than 100-year history of radio. As the diversity of spectrum applications grows, the complexity of obtaining spectrum support grows accordingly. Along with engineering, coordinating and managing the tens of thousands of frequencies used in today's complex radio systems, Navy spectrum managers also use and maintain a wide array of databases. Without them it would be impossible to reliably operate radar, telemetry networks, microwave data links, mobile radios or anything dependent on a frequency in the electromagnetic spectrum.

Automated net-centric spectrum management tools of the future will rely on these databases, as cognitive radios of the future autonomously adapt to meet the needs of a dynamic battlefield. Highly accurate and up-to-date databases are the foundation of future spectrum management.

Two Fundamental Types of Databases

There are many sources for information used in spectrum management including national and international radio regulations, maps and geodetic information, propagation studies, sunspot numbers and more. At the core of spectrum management are two fundamental types of databases. The first contains documents detailing what equipment characteristics are certified and authorized for use within the United States, its possessions and host nations in which the DON operates.

The second database contains detailed licensing information of how individual radio frequencies are assigned for use within the United States, its possessions and host nations around the world. When these two databases are combined, they form the picture of not only how the DON uses the electromagnetic spectrum today, but also what portions of the electromagnetic spectrum are available to meet requirements in the future.

Equipment certification defines how a spectrum-dependent device may operate within the electromagnetic environment. Detailed data are registered, defining all the characteristics of the transmitter, antenna and receiver. Usually a transmitter is capable of more power, features or greater bandwidth than the spectrum can support everywhere the DON operates. This is why the database also includes information about how the system is authorized to operate.

Limitations may vary from location to location and country to country. Certification of spectrum-dependent devices can begin as early as the conceptual stage of development. As a device is developed, the spectrum community is able to provide the guidance necessary to successfully operate the system in the congested, highly regulated radio frequency spectrum environment. Restrictions are also defined in the certification database to assure that operations abide by local, national and international radio regulations.

Frequency Assignment

Frequency assignment is the licensing of an individual radio frequency in a particular geographic area. The assignment database lists detailed parameters that define the electromagnetic radiation from an antenna. These parameters include the maximum power authorized from the transmitter, the maximum antenna height, the amount of spectrum occupied by the transmitted signal and the type of modulation used.

In addition to the technical characteristics of the signal, the assignment databases also contain administrative information about who is authorized to use the frequency, under what conditions it may be used and what equipment is authorized to transmit. When combined, the equipment and frequency databases contain nearly all the information needed to determine the characteristics of the electromagnetic spectrum-dependent devices that the DON operates, at any time and in any place.

Years ago, radio frequency spectrum management was done with mechanical slide rules, formulas, best guesses, rules of thumb and hours or sometimes days of labor to predict characteristics of the electromagnetic environment. Cognitive radios that continually reprogram themselves to maximize the local spectrum must do all this and much more in less than the blink of an eye. Success depends not only on the advanced technology of future radio systems, but also on today's spectrum manager updating and maintaining an accurate database.

Net-centric spectrum management uses the information in the equipment and frequency databases to dynamically model the spectral environment while software-defined cognitive radios will determine the best frequencies and transmission parameters to complete communication. With accurate information, the next generation of spectrum management automation tools will model and predict the electromagnetic environment. The accuracy of these predictions depends entirely on the accuracy of the databases. Therefore database accuracy is essential.

Many of today's spectrum records are decades old and not detailed enough to support the electromagnetic demands of future radio systems. The engineering tools may not have been available, or the level of detail was not required for equipment certification and frequency assignment when the system first entered the inventory. Some transmitters have been in operation for nearly as long as there has been spectrum management.

In 1952, the U.S. Navy built a very low frequency transmitting station located at Jim Creek, in Oso, Wash., and it is still in operation. On the other hand, many modern systems are so complex they do not conform to the current certification and assignment processes. Nevertheless, the DON spectrum management community is actively engaged in aggressively updating and validating all spectrum-related databases.

Frequency Reviews

Radio frequency assignments are generally reviewed at least once every five years. During the review process a spectrum manager evaluates all electromagnetic parameters of the system and compares it to the data in the record to verify it is accurate. The five-year review process is also an opportunity to add data omitted from the original application or update data which may have changed. Even small data errors such as incorrect latitude or longitude for transmitters or receivers, erroneous antenna heights or terrain elevation can all result in frequency assignments that cause interference with another system. The frequency assignment is the license that authorizes the DON to transmit, and it must be accurate at all times.

There are no periodic reviews of equipment certification. However, whenever there are modifications or upgrades, they are added to the certification. Also, when the associated frequency assignment is reviewed, spectrum managers review the equipment certification. New capabilities or modifications to the equipment are recorded along with any administrative changes. Sometimes, new restrictions or rules regulating operation are also added. Occasionally equipment replacement or upgrades require the spectrum manager to submit new documentation requesting certification of new equipment recently added to the inventory.

The DON is one of the federal government's largest users of the electromagnetic spectrum. The Department's interest in the electromagnetic spectrum is straightforward — ensuring spectrum access for the U.S. Navy and Marine Corps. Access to frequencies for required training, day-to-day support and operations is a paramount concern and a priority endeavor of the DON. Given the fact that spectrum reallocations, policy determinations and new allocations all have serious consequences for the DON, it is in the Department's best interest to be as good a steward as possible in our use and management of spectrum.

Thanks to a dedicated group of professional spectrum managers working in the fleet, ashore and throughout the chain of command, the Department of the Navy will be ready with a strong foundation to build the future of spectrum management.

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

What has the DON CIO Spectrum Team Done Lately?

√ Participating in National Telecommunications and Information Administration (NTIA) working groups and coordinating with DoD to formulate a consolidated DoD position for development of the Presidential Strategic Plan for Electromagnetic Spectrum Management.

√ Developing a Land Mobile Radio policy in conjunction with ASN (RDA), HQMC C4 and OPNAV N46 for effective emergency communications. It will establish standards for encryption and interoperability within the DON.

√ Worked with the DoD and the Federal Communications Commission to resolve a consumer garage door radio frequency interference issue by locating new frequency assignments for garage door openers away from the frequency used by first responders near Camp Pendleton, Marine Corps Base Quantico and Navy Region Northwest.

√ Sponsored and led the introduction of DON XML Naming and Design Rules (NDR) into the Afloat Electromagnetic Spectrum Program (AESOP) software upgrade. The NDR-compliant version of AESOP proved so successful during Trident Warrior 2004 exercises that the Chief of Naval Operations recently mandated its use in all communications and radar planning.

√ Led a Department of State delegation at the Inter-American Telecommunication Commission meeting in Argentina – a coalition of 35 countries from the Americas that collaborate on spectrum policy and use issues. As a result, the DON will be included in U.N. treaty negotiations, which will ensure that the Navy's equities are protected and that warships can operate with impunity.

√ As an international chair of the International Telecommunication Union (ITU), identified the need for and initiated a global study to recommend technical standards to protect maritime communication systems.

√ As the DoD representative, worked on developing the U.S. position on the technical, operational and regulatory provisions regarding the use of spectrum by space services to reduce the risk of encroachment and reallocation into DoD-designated frequency bands.

√ Rallied Australia, Russia and the Arab States at the U.N. proceedings in Geneva to oppose a European proposal to reserve certain frequency spectrum bands, thereby preserving the maritime mobile allocation for the DON's continued use.

√ Coordinated more than 570 radio frequency assignments for the DoD in support of Hurricane Katrina relief operations. This included coordination between the DON CIO, OPNAV, HQMC and the Navy Marine Corps Spectrum Center. CHIPS

The Lazy Person's Guide to Controlling Technologies Part II: Electronic Tethers

By Retired Air Force Major Dale J. Long

I have resigned myself to a simple fact of modern life: Thanks to the marvels of modern communications technology, I will never again be "out of touch." Thanks to the cell phone, someone from work will still be able to find me once I leave the office. My wife will be able to call me (usually just after I have passed the supermarket) and ask me to pick up some thing she needs for dinner.

It's not all bad, though. Having a cell phone means I can reach out and touch my staff no matter where they are in the country. It means I can call up vendor representatives no matter where they are and check on an order or project status. It also means never having to miss saying goodnight to my children no matter where I am, though I would prefer being there in person.

Cell phones, pagers, e-mail devices and related hybrids have created a shared expectation that we will all be available 24 hours a day, 7 days a week. These wireless convenience devices have significantly changed how people relate to each other over the past 20 years.

This edition of the Lazy Person's Guide will examine some of these changes and look at convenience technologies past, present, and possibly future in our personal communications environment.

Reach Out and Touch Someone

I have written before in *CHIPS* on the development of both wired and wireless communications, primarily from the standpoint of technology development, so we will skip a lengthy discussion of how the telegraph, telephone and radio were invented. What I would like to note, however, is that these three technologies were disruptive to long-established patterns of behavior.

After centuries of working relationships based solely on personal contact and paper correspondence, the ability to transmit text or voice instantaneously over great distances had a profound effect on the conduct of both public and private business.

Advances in telephone networks and the evolution from the telegraph to e-mail, however, did not change the essential fact that people have to be in particular physical locations to use wired electronic communications. Even cordless phones don't let you stray too far from the base unit. Our new wireless communications networks, though, enable communications without the inconvenience of staying within range of a wired tether. We are in the process of extending some type of wireless service to every corner of the country.

However, we are not doing it as quickly as some might like. The United States and Europe developed extensive wired networks that form the backbone of our traditional telephone systems and the Internet, making us the world leaders in telecommunications in the 20th century.

At the risk of sounding whiny, these same legacy networks are now the boat anchors holding us back from being the world leaders in telecommunications in the 21st century. Countries in Europe and Africa that never developed comprehensive wired telephone networks have leapfrogged the United States with cellular phone systems years ahead of what we have.

Japan has taken wireless access to great heights, building both cellular phone and wireless networking systems that reach to every corner of the country, including deep into its mass transit subway systems. Just try getting a reliable cell phone or wireless network connection in the New York or Washington D.C., subway. Finland and Ghana reportedly have more comprehensive cellular phone networks than we do in the United States.

Countries who realize that their future economic success depends on sophisticated telecommunications networks providing seamless universal access to wireless voice and data as a public utility are deploying these systems at a rapid pace. In the United States, wireless deployments have been slowed by fights over standards and efforts by established vendors to delay or prevent deployment of wireless network access by municipal governments.

While there is some evidence that corporate interests allegedly run business operations better than governments, my opinion is that allowing market competition to determine technical standards does not always result in the fastest path to the best technology. Cases in point: Beta versus VHS (video home system) high-definition television (HDTV) broadcast standards; Blu-Ray versus HD-DVD (High Density Digital Versatile Disc); Global System for Mobile Communications (GSM) versus Code Division Multiple Access (CDMA); CDMA versus Wideband Code Division Multiple Access (W-CDMA) on cell phones; and any Microsoft product versus pretty much any of its crushed or marginalized competitors.

None of these were decided on their technical merits. Beta had better picture and sound than VHS but lost. The new DVD standard battle might come down to deciding whether backward compatibility with existing DVDs is more important than disc capacity, though what really will matter is who signs up the most movie studios for its format. Much of the rest of the world settled on GSM or W-CDMA

for cell phones. The United States and parts of Europe, however, use CDMA2000, which is based on older, less compatible standards and has prompted some speculation that CDMA exists to provide a domestic market and patent protections for some U.S. and European mobile phone providers.

Therefore, it is my opinion that technical superiority rarely decides the outcome in the market. What usually decides the outcome is convenience. Monopolies also pretty much guarantee victory, though convenience plays a role there too. It is generally more convenient to buy from a monopoly than to go off the beaten track for an alternative. How many of us are so annoyed with our cable television providers that we are willing to ditch them (and their broadband Internet access) to get satellite TV service with most of the same channels and slower Internet access?

Convenience drives our desire for wireless connectivity, which in turn is driving research and development, service offerings, infrastructure development, and marketing and sales in our modern telecommunications environment. It is because of convenience that my generation is willing to pay $40 a month for a cell phone so our spouses can call us while we are on the way home to ask us to pick up a bag of ice to make iced tea for dinner. It did come in handy when my car would not start, but that only happens once every six or seven years and there is usually a landline nearby.

Form and Function

For me, cool miniature technology all started with comic strip hero Dick Tracy and his wrist TV communicator. In 1964, when I was at the very impressionable age of seven-years-old, Dick Tracy traded in his two-way wrist radio for a two-way wrist TV. An entire generation of American youth saw this vision of the future in their newspaper "funnies" section every day. Who knows? It may have been what started today's now adult engineers on the path to miniaturizing every electronic device they can get their hands on, perhaps in the hope that some day they would get to wear a videophone on their wrists, too.

However, it's been more than 40 years since Diet Smith gave Tracy that watch, and I still don't have one like it on my wrist. Cell phones with cameras come close, but not quite. But we do have quite a few gadgets about the same size that are amazing. I think what impresses me the most about cell phones, pagers, Blackberrys, etc., is that no matter where you are, the system can find you and deliver your call or message. Of course, that's also the scary part: They can find you wherever you are hiding. For every technophile who wants 24/7 connectivity there is probably a technophobe that fears being tracked down or identified by secret chips implanted in some electronic device he or she is carrying.

Let's concentrate on the big three of wireless convenience devices: pagers, cell phones and e-mail. Yes, personal digital assistants (PDAs) are very popular, but even though some have the ability to network their main purpose is to organize information.

Page Me

Pagers are lightweight, portable receivers that let someone call a phone number and send you a short message. Usually the display shows you a callback number or some text. The pagers I enjoyed the most were the radio pagers we had 20 years ago when I worked in a Strategic Air Command munitions maintenance squadron. It wasn't Dick Tracy quality, but it was as close as I had ever been to it. Unlike alpha-numeric text pagers, callers could leave voice messages. When the pager went off, you pushed the button and the caller's recorded message came out of the speaker.

They were for official use only, but as with every technology ever given to military people, we did make some non-official personal use of them that did not interfere with government business and incurred no cost to the government. Since we were in the bomb business no one blinked when one of our pagers went off announcing the impending start of a kinetic energy seminar (meeting at the bowling alley) or trajectory analysis study (meeting at the driving range).

The pagers' primary function, however, was as a broadcast system that instantly notified everyone who had one that the alert "Klaxon" had gone off, signifying that we had to get six fully loaded strategic bombers lined up at the end of the runway to take off within a launch time prescribed by the proximity of the closest potentially hostile ballistic missile submarine off the New England coast and how fast its missiles could reach us. For this purpose, these pagers did their job very well and at a fairly reasonable cost.

The main limitation of pagers is that they are primarily one-way. They are rapidly losing ground in the market to cell phones as the latter comes down in price and as additional features are added. I often wonder why people would want both a pager and a cell phone. Zippy is no help; he just wants one of everything clipped to his belt whether he needs it or not.

However, I did get a plausible explanation from some U.S. Border Patrol agents: battery life. Cell phone batteries apparently only last as long as the manufacturer advertises if you keep them in sleep mode. Using a cell phone drains them much faster. So agents turn their cell phones off and leave their pagers, which run on replaceable AA batteries, on. Maybe as the rechargeable battery technology in cell phones improves we will see the end of pagers entirely; they are still a relatively cheap alternative if all you need is a quick notification.

Call Me

I dealt with cellular phones at some length in a previous article (http://www.chips.navy.mil/archives/04_summer/Web_pages/Telephony.htm) so this time we'll just touch on two things: video capability and hybrid phones.

When I last wrote about cellular phones 15 months ago, picture resolution was measured in hundreds of pixels and most would only transfer images between phones on the same service. What a difference a year makes. Now camera phones are offering multi-megapixel resolution, and you can either transmit your photos over the service or download them to your computer.

But what practical use does a camera phone have? Yes, it can be cool to send vacation pictures while you are on vacation or a snapshot of that attractive nightclub singer to your buddy. But where's the beef? If you're in the military reconnaissance or intelligence

business, you already know the value of real-time information. If you're a customs inspector at a port of entry you can send photos of cargos and manifests back to the office where someone can check them against computer records. If you're an emergency medical technician you can send a photo of a wound back to a trauma surgeon for advice on how to patch it up and keep the victim alive long enough to make it to a hospital.

Hybrid phones that combine information organizers and e-mail capabilities are also improving. I finally got the Kyocera 7135 I mentioned in the cell phone article last summer, and it has become my second brain. I can discuss it without risk of appearing to endorse it because, predictably, it's being phased out and replaced by even newer technology. This phone/PDA hybrid keeps my schedule, holds information for all my contacts, can tell me what time it is anywhere in the world, holds various word processing, spreadsheet and PDF documents and has an e-mail client. It also has fairly large screen, 160x160 pixels (2 by 2 inches) with a 65,000-color display. I have not traveled with a laptop since I got it.

Cell phones share one particular characteristic with pagers: The caller has to know your number. This can limit who can reach you. You can also turn the phone off while in a meeting, at a restaurant or in a movie theater, so you do have some control over when people can reach you. I have suggested to my wife that we should just cancel our traditional wired phone service and just use a cell phone, but she is not willing to give up wired service yet. However, an increasing number of people are apparently opting out of wired service in favor of wireless.

In a way, it's a bit like the "why carry a pager and a cell phone" discussion. If your phone number can follow you anywhere, why do you need more than one phone number?

Mail Me

Unlike cell phones, where people tend to discuss their business without leaving tracks or leave short voice mail messages, wireless e-mail devices can be like clipping an electronic avalanche to your belt. Messages accumulate… and accumulate… and accumulate. In the last issue I outlined a 12-step program for regaining control of your life in the face of 24/7 e-mail. This goes double for a Blackberry. Here's a story about why.

Before I retired, the headquarters where I was assigned had 22 directors and some other key staff using Blackberry wireless e-mail devices. A sizable sum of money was spent buying a Blackberry server, attendant networking equipment and the Blackberry devices themselves. After several weeks of deployment and testing, all the senior O-6s and flag officers had little e-mail readers clipped to their belts.

The user community fell into two basic groups. Group one wore Blackberry devices as a decoration, using them only when absolutely necessary. They might check them periodically to see if their boss had sent them something, but clearing the unit often fell to their executive officer.

Group two embraced Blackberry devices and played with them constantly, often exhibiting all the finest symptoms of e-mail addiction. In this group, a very senior flag officer was very comfortable with technology and really enjoyed his Blackberry. However, this proved disruptive on a couple of levels.

Flag officer staffs are generally (no pun intended) well-oiled machines that maximize every minute of their boss's day. They work to three particular rhythms: boss in the office, boss in a meeting, boss out of town. For example, when the boss is in a meeting it gives the staff a chance to clear the outbox and refill the inbox, the wooden ones filled with the paper and the electronic ones. In the hour the boss is in the meeting, any good staff can shuffle stuff in and out and have time left over to plan the weekend golf outing.

However, if the boss takes a Blackberry into a meeting, the staff may get messages every few minutes with questions about various things that come up in the meeting. Instant answers are expected. They may no longer have "quiet time" to organize things. From the perspective of some people I knew on the staff, the disruptions from the e-mail made it somewhat harder to review and shuffle the dozens of staff packages in and out of the office every day.

Also, it has been my experience that if lower-ranking officers tune out of a meeting to send e-mail or take a cell phone call they normally get their heads handed to them by the person at the head of the table for the breach of etiquette. But who's going to tell a flag officer in a meeting that he might be sending, along with his e-mail, the wrong message about the value of everyone's time in the meeting?

Last Words

Portable wireless technology has become the zebra mussel of the modern work environment. For those of you unfamiliar with this particular mollusk, the zebra mussel is a non-native invasive species that has pretty much taken over parts of Lake Champlain between Vermont and New York. First they were a novelty. Then they became a pest and a nuisance. Despite many attempts to control them, they have become a permanent part of the ecosystem that has resisted all attempts at control.

Then a strange thing happened. Some of the scientists who had been objecting to the zebra mussel's impact noticed that they were cleaning up a somewhat more serious problem in the lake: algae blooms. Invasive, disruptive species are not supposed to have an upside, but somehow this one managed to become useful.

That's kind of how I see camera phones and wireless e-mail. We are constantly being bombarded by advertisements about new technology, but much of it is still a solution in search of a problem. Like the zebra mussel, I am sure it all has at least one useful purpose. I will start figuring it out right after I play another game or two of Bejeweled on my cell phone.

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.esi.mil/.

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

Business Intelligence

Business Objects

Business Objects - Provides software licenses and support for Business Objects, Crystal Reports, Crystal Enterprise and training and professional services. Volume discounts range from 5 to 20 percent for purchases of software licenses under a single delivery order.
Contractor: ***EC America, Inc.*** (SP4700-05-A-0003)
Ordering Expires: 04 May 10
Web Link: http://www.gsaweblink.com/esi-dod/boa/

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: 17 Dec 06
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 06
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Microsoft Products

Microsoft Database Products - See information provided under Office Systems.

Oracle (DEAL-O)

Oracle Products - Provides Oracle database and application software licenses, support, training and consulting services. The Navy Enterprise License Agreement is for database licenses for Navy customers. Contact Navy project managers on the next page 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 05
Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

www.it-umbrella.navy.mil

Special Note to Navy Users: On Oct. 1, 2004, and May 6, 2005, the Navy established the Oracle Database Enterprise License, effective through Sept. 30, 2013. The enterprise license provides Navy shore-based and afloat users to include active duty, Reserve and civilian billets, as well as contractors who access Navy systems, the right to use Oracle databases for the purpose of supporting Navy internal operations. Navy users in joint commands or supporting joint functions should contact Bill Huber, NAVICP Mechanicsburg contracting officer at (717) 605-3210 or e-mail William.Huber@navy.mil, for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWAR-SYSCEN) San Diego DON Information Technology (IT) Umbrella Program Office.

The Navy Oracle Database Enterprise License provides significant benefits including substantial cost avoidance for the Department. It facilitates the goal of net-centric operations by allowing authorized users to access Oracle databases for Navy internal operations and permits sharing of authoritative data across the Navy enterprise.

Programs and activities covered by this license agreement shall not enter into separate Oracle database licenses outside this central agreement whenever Oracle is selected as the database. This prohibition includes software and software maintenance that is acquired:

a. as part of a system or system upgrade, including Application Specific Full Use (ASFU) licenses;
b. under a service contract;
c. under a contract or agreement administered by another agency, such as an interagency agreement;
d. under a Federal Supply Service (FSS) Schedule contract or blanket purchase agreement established in accordance with FAR 8.404(b)(4); or
e. by a contractor that is authorized to order from a Government supply source pursuant to FAR 51.101.

This policy has been coordinated with the Office of the Assistant Secretary of the Navy (Financial Management and Comptroller), Office of Budget.

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: 26 Mar 09
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: 12 Jun 06
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Enterprise Management

CA Enterprise Management Software (C-EMS2)

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 to 5 percent off GSA Schedule pricing plus spot discounts for volume purchases.
Contractor: ***Citrix Systems, Inc.*** (W91QUZ-04-A-0001); (772) 221-8606
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.serena.com

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 06
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 and video products, and Vigilant Security and Management products. Discounts are 10 to 8 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

ProSight

ProSight - Provides software licenses, maintenance, training and installation services for enterprise portfolio management software. The BPA award has been determined to be the best value to the government and; therefore, competition is not required for software purchases. Discount range for software is from 8 to 39 percent off GSA, which is inclusive of software accumulation discounts. For maintenance, training and installation services, discount range is 3 to 10 percent off GSA. Credit card orders are accepted.

Contractor: ***ProSight, Inc.*** (W91QUZ-05-A-0014)
Ordering Expires: 19 Sep 06
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

Quest Products

Quest Products - Provides a full range of Quest Software Enterprise Management products and services including training. Product groups include Application Management and Database Management *(code quality and optimization, performance and ability, and change and configuration)* and Windows Management (Active Directory, Exchange and Windows).

Contractor: ***Quest Software, Inc.*** (W91QUZ-05-A-0023); (301) 820-4200,
Ordering Expires: 28 Jul 10
Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-05-A-0023

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 page 65.*

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) 312-3656
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,dataconversion,training,testing,objectdevelopment, 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 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 competively 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) 947-2059
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); (202) 220-2960
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.esi.mil
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/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.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.esi.mil
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/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.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-4045)
Ordering Expires: Nonexpiring. Download provided at no cost; go to the Antivirus Web links below for antivirus software downloads.
Web Link: http://www.esi.mil
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/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Xacta

Xacta - Provides Web Certification and Accreditation (C&A) software products, consulting support and enterprise messaging management solutions through its Automated Message Handling System (AMHS) product. 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. Xacta's AMHS provides automated, Web-based distribution and management of messaging across your enterprise.

Contractor: ***Telos Corp.*** (F01620-03-A-8003); (703) 724-4555
Ordering Expires: 31 Jul 08
Web Link: http://esi.telos.com/contract/overview/

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); Small Business; (800) 942-4874, ext. 2224

Ordering Expires: 30 Nov 05
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/adobe/adobe-ela.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
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) 885-4554
Hewlett-Packard (N00104-02-A-ZE80); (800) 535-2563 pin 6246
Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638 or (312) 655-9167
Softmart (N00104-02-A-ZE84); (610) 518-4000, ext. 6492 or (800) 628-9091 ext. 6928
Software House International (N00104-02-A-ZE86); (732) 868-5926
Software Spectrum, Inc. (N00104-02-A-ZE82); (800) 862-8758 or (509) 742-2208

Ordering Expires: 30 Mar 07
Web Link: http://www.it-umbrella.navy.mil/contract/enterprise/microsoft/ms-ela.shtml

Red Hat

Red Hat *(Netscape software formerly owned by AOL, not Linux)* - In December 2004, America Online (AOL) sold Netscape Security Solutions Software to Red Hat. This sale included the three major software products previously provided by DISA (Defense Information Systems Agency) to the DoD and Intelligence Communities through AOL. *Note: The Netscape trademark is still owned by AOL, as are versions of Netscape Communicator above version 7.2. Netscape Communicator version 8.0 is not part of this contract.*

August Schell Enterprises is providing ongoing support and maintenance for the Red Hat Security Solutions (products formerly known as Netscape Security Solutions) which are at the core of the DoD's Public Key Infrastructure (PKI). This contract provides products and services in support of the ongoing DoD-wide enterprise site license for Red Hat products. This encompasses all components of the U.S. Department of Defense and supported organizations that use the Joint Worldwide Intelligence Communications System (JWICS), including contractors.

Licensed software products available from DISA are the commercial versions of the software, not the segmented versions that are compliant with Global Information Grid (GIG) standards. The segmented versions of the software are required for development and operation of applications associated with the GIG, 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 GIG, GCCS or GCSS, you must contact one of the Web sites listed below to obtain the GIG 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.

GIG or GCCS users: Common Operating Environment Home Page
https://coe.mont.disa.mil
GCSS users: Global Combat Support System
http://www.disa.mil/main/prodsol/gcss.html

Contractor: *Red Hat*
Ordering Expires: 06 Mar 07 (includes one one-year option)
Download provided at no cost.
Web Link: http://dii-sw.ncr.disa.mil/Del/netlic.html

WinZip

WinZip - This is an IDIQ contract with Eyak Technology, LLC, an "8(a)" Small Disadvantaged Business (SDB)/Alaska Native Corp. for the purchase of WinZip 9.0, a compression utility for Windows. Minimum quantity order via delivery order and via Government Purchase Card to Eyak Technology, LLC is 1,250 WinZip licenses. All customers are entitled to free upgrades and maintenance for a period of two years from original purchase. Discount is 98.4 percent off retail. Price per license is 45 cents.

Contractor: *Eyak Technology, LLC* (W91QUZ-04-D-0010)
Authorized Users: This has been designated as a DoD ESI and GSA SmartBUY Contract and is open for ordering by all U.S. federal agencies, DoD components and authorized contractors.
Ordering Expires: 27 Sep 09
Web Link: https://ascp.monmouth.army.mil/scp/contracts/compactview.jsp

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

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: 27 Nov 06
Authorized Users: Gartner Group: 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.
Web Link: http://www.it-umbrella.navy.mil/contract/r&a/gartner/gartner.shtml

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 Expires:
Contract ordering for all new equipment purchases has expired.
All Labor CLINS, Support Services and Spare Parts can still be ordered through 28 Jul 07.

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
SSC Charleston Order Processing: (757) 445-1493 (DSN 565) or (como@mailbuoy.norfolk.navy.mil)

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, ext. 103

Dell (N68939-97-A-0011); (800) 727-1100, ext. 7261973

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

Hewlett-Packard (N68939-96-A-0005); (800) 727-5472, ext. 15614

Ordering Expires:
Control Concepts: 03 May 07 (includes two one-year options)
Dell: 31 Mar 06 (includes one one-year option)
GTSI: 31 Mar 06 (includes one one-year option)
Hewlett-Packard: 07 May 06 (includes one one-year option)

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
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) 725-5012; Awarded 1 Jul 97

Ordering Expires: 30 Jun 06, with one one-year option

Northrop Grumman Information Technology (N68939-97-A-0018); (703) 413-1084; Awarded 1 Jul 97

Ordering Expires: 11 Feb 06, with one one-year option

SAIC (N68939-97-A-0020); (703) 676-2388; Awarded 1 Jul 97

Ordering Expires: 30 Jun 06, with one one-year option

TDS Inc., a Centurum Company (Small Business) (N00039-98-A-3008); (619) 224-1100; Awarded 15 Jul 98

Ordering Expires: 14 Jul 06, with one one-year option.

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

For DON IT Umbrella Program contract assistance, phone (757) 445-2568, (DSN 565), e-mail como@mailbuoy.norfolk.navy.mil or go to our Web site at http://www.it-umbrella.navy.mil/.

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, WIMAX Secure	Cisco, 3COM, HP, Enterasys, Foundry

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 WiMAX Secure Wireless Networking and DolphinSearch Datamining Software.

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: 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, Aug-Sep) No separate acquisition, contracting and technical fees.

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

CHIPS Article Submission Guidelines

CHIPS welcomes articles from our readers. Please submit articles via e-mail as Microsoft Word or text file attachments to chips@navy.mil or by mail to Editor, CHIPS, SSC Charleston, 9456 Fourth Ave, Norfolk, VA 23511-2130. If submitting your article by mail, please send the article on disc with a printed copy. To discuss your article with a CHIPS editor, call (757) 444-8704 or DSN 564-8704.

Relate the subject matter of your article to information technology (IT) and how IT is helping to accomplish your command mission, improve services, perform a task or automate or enhance a process. Provide lessons learned from your experience. Our motto states: *"CHIPS: Dedicated to Sharing Information, Technology, Experience."* The theme of your article should meet the intent of our motto.

An article is more interesting when you can convey a personal experience; it is also easier to read. When writing use active rather than passive voice. Avoid technical terms that only a few readers would understand. Write out the full name or title before using an acronym the first time; thereafter, use only the acronym. Avoid using a myriad of acronyms throughout your article since they can be confusing to the reader.

Articles may contain illustrations. Do not embed photos or images in your MS Word document, please send them as separate file attachments. Make sure photos and illustrations add value to your article and are mentioned in the text. Please do not use Web-based or MS PowerPoint graphics because they do not have a high enough resolution to reproduce clear, quality illustrations in publication. Please save graphic files with a resolution of 300 dpi.

Please submit your article to your public affairs officer and chain of command for release authority before you submit your article to CHIPS.

While we do not require a standard length for articles, we prefer articles one to two pages in length. Typically, one magazine page equals two and a half pages of typed text using a standard 12-point font or approximately 700-1,000 words.

We reserve the right to edit articles, which is a necessary step in the production process. Our goal is to enhance your style — not change it. We use the Associated Press Stylebook, the U.S. Navy Style Guide and guidance from the Chief of Navy Information (CHINFO) for editorial management.

Subject matter experts review each article for technical accuracy and to ensure conformance to CHINFO guidelines. We may make changes to your article to conform to magazine production guidelines and the CHIPS style manual and format. If an article requires extensive changes, we will contact you.

CHIPS is published quarterly. Our deadline dates are: Feb. 1, April 1, Aug. 1 and Oct. 1.

Thank you for your interest in CHIPS magazine. CHIPS

Thanks to our customers for 17 great years!

The DON IT Umbrella Program's business strategies meet the requirements of the FORCEnet Functional Concept for an agile and robust ashore business IT infrastructure. The Umbrella Program offers standards compliant tools, software, business and modeling tools, ERP Systems Integration Services, Section 508 tools, Enterprise Architecture Tools and much more.

Navy Oracle Enterprise License Agreement provides significant benefits including substantial cost avoidance for the Department of the Navy.

AHOY!! The Navy Oracle Database Enterprise License Agreement now encompasses Navy afloat users (and contractors) as well as the shore-based organizations included in the original agreement. This modification provides even greater cost avoidance for the Department of the Navy. The agreement facilitates the goal of net-centric operations by permitting the sharing of authoritative data across the Navy Enterprise. See the Special Note to Navy Users in the Oracle (DEAL-O) on page 65 for complete information.

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 NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC CHARLESTON
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988