CHIPS

Magazine

October-December 2008

SSC Atlantic - SSC Pacific
Realigned, Reloaded, Reenergized

Sharing - Information - Technology - Experience

CHIPS October – December 2008

Volume XXVI Issue IV

Department of the Navy Chief Information Officer
Mr. Robert J. Carey

Space & Naval Warfare Systems Command
Commander Rear Admiral Michael C. Bachmann

Space & Naval Warfare Systems Center Atlantic
Commanding Officer Captain Bruce Urbon

Senior Editor
Sharon Anderson

Assistant Editor
Nancy Reasor

Layout and Design – Sharon Anderson

Web Support – Deborah Midyette
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 and Naval Warfare Systems Center Pacific.

CHIPS is published quarterly by the Space and Naval Warfare Systems Center Atlantic. USPS 757-910 Periodical postage paid at Norfolk, VA and at an additional mailing office. POSTMASTER: Send changes to CHIPS, SSC Atlantic, 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 Atlantic, 9456 Fourth Ave., Norfolk, VA 23511-2130, or call (757) 444-8704; DSN 564. E-mail address: chips@navy.mil; fax (757) 445-2103; DSN 565. Web address: www.chips.navy.mil/.

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.

Features

Navigation Guide

Cover - Collage of images that tell the story of the Space and Naval Warfare Systems Centers Atlantic and Pacific. This page, nearly 3,000 flags flown in remembrance of those who died from the terrorist attacks on the World Trade Center, Pentagon and in a field in Shanksville, Pa., marking the opening of the Pentagon Memorial on Sept. 11, 2008. Fluttering from 184 of the flags are blue ribbons with the names of those killed when American Airlines Flight 77 slammed into the west side of the Pentagon. Fifty-nine of the victims were aboard the aircraft, the other 125 were Pentagon personnel. Photo by Christy Crimmins.

Editor's Notebook

This issue we feature the Space and Naval Warfare Systems Centers which were realigned under SSC Atlantic and SSC Pacific due to the 2005 Base Realignment and Closure legislation. SSC Charleston was aligned under SSC Atlantic along with site locations in Pensacola and Tampa, Fla., Washington D.C., Little Creek and Norfolk, Va., Europe, the Middle East and Antarctica. SSC Atlantic also includes the former SSC Norfolk and SSC New Orleans. SSC San Diego was aligned under SSC Pacific.

The stand up of an East and West Coast systems center signifies the alignment of core competencies in the professional skills that the SPAWAR Systems Centers are noted for: C4I engineering; shipboard systems; marine navigation; robotics; technology transfer; environmental science; ocean engineering; software engineering; help desk and customer support center; and much more.

Jennifer Watson, who is now head of the Business Systems/Enterprise Information Services department and the national competency lead for Business Systems/EIS in the newly commissioned SSC Atlantic organization, talked about the realignment.

"The merging of these three commands, along with the implementation of our new Competency Aligned Organization/Integrated Product Teams framework, will promote more organizational clarity and awareness," Watson continued.

"Internally, this will enable in the sharing of common priorities, objectives and processes. Externally, our naval and joint warfighting customers will benefit through a more agile and efficient capability to deliver end-to-end C4ISR and business/enterprise information solutions. This is a great Navy day!"

In July, the CHIPS staff visited two experiments sponsored by U.S. Joint Forces Command — Noble Resolve and Bold Quest — and interviewed Rear Adm. Gregory A. Timberlake for this issue.

In August, the CHIPS assistant editor, Nancy Reasor, attended the Air Force IT Conference in Montgomery, Ala., with our colleagues from the Defense Department acquisition community.

September brought a somber reminder that we must never take our freedom for granted or let our vigilance down. The Pentagon Memorial opened Sept. 11, the seventh anniversary of the 9/11 terrorist attacks. The memorial serves as a tribute to the victims from the World Trade Center, Pentagon and Shanksville, Pa., attacks.

We remember our colleagues in the Pentagon, the deep grief of the nation on that infamous day — and the coming together of the whole nation in a spirit of renewal and strength — we have not forgotten.

Welcome new subscribers!

Sharon Anderson

A U.S. Sailor rings the bell as the name of each person lost at the Pentagon is read during the Pentagon Memorial dedication ceremony, Sept. 11, 2008. The national memorial consists of 184 inscribed memorial units honoring the 59 people aboard American Airlines Flight 77 and the 125 in the building who lost their lives Sept. 11, 2001. Defense Department photo by Cherie Cullen.

SSC Pacific Commanding Officer Capt. Mark Kohlheim with SSC Pacific technical director Carmela Keeney at the commissioning ceremony for SSC Pacific, headquartered in San Diego, Calif. Below, SSC Atlantic Commanding Officer Capt. Bruce Urbon departs the newly commissioned SSC Atlantic organization, which is headquartered in Charleston, S.C. Ceremonies for the stand up of SSC Atlantic and Pacific were held Sept. 29 at multiple locations and linked via VTC.

Work Continues on Next Generation Enterprise Network

I receive several requests each month for interviews with magazines that report on government policy, management and trends. A popular question among reporters pertains to what projects I am working on, my top five projects, or some variation of that. Lately, my response has been to tell them about our critical work on cyber security, the consolidation of information technology services due to joint basing in Guam, consolidating our enterprise architecture work, and the important work we're doing to bring the Next Generation Enterprise Network (NGEN) to fruition.

In pondering what to write for this column, I recalled the reporters' questions and my responses, and thought that an update on one of our most important projects, NGEN, would be in order, since it will affect the majority of our people. When the Navy Marine Corps Intranet (NMCI) contract expires on Sept. 30, 2010, NGEN, as the follow-on to NMCI, will be in place to continue to supply a secure IT infrastructure for naval networking in the continental United States, ashore and at some overseas locations. The NMCI to NGEN transition will affect all of our approximately 700,000 users who are currently on NMCI.

While NGEN will continue the work of NMCI, there will be some changes as well. The services provided by NMCI are almost completely outsourced and do not afford the Department the desired level of control over network design and operations. Because our IT networks and information are recognized as absolutely critical to our mission, the Department has determined that we must exert greater oversight and direct control of the design and operations of NGEN.

Critical management control and oversight roles will not be outsourced. That being said, we expect the role of industry in the future of supporting Naval networks to be broad and necessary. Support roles related to basic network services will continue to be provided by industry under the direction of the government. The shift in roles and functions identified for NGEN will require that military and civilian billets be included in the NGEN operating structure and that these people will possess the skills to successfully perform their functions. I foresee the composition of the NGEN workforce changing over time depending on workforce constraints, policy, technology innovations, and acquisition and operational strategies.

The Department revealed information about the roles and functions for NGEN during a DON-sponsored "industry day" held in Washington, D.C., on Sept. 8. About 500 industry and government representatives from 207 large and small companies attended the event. The DON shared its vision for the Naval Networking Environment 2016 … a bit about how we intend to achieve that and notional plans for potentially separating the work related to NGEN into segmented pieces, e.g., enterprise services, end user computing devices, desktops and peripheral support, local area networks, application servers, and more.

The intent of the segmented approach to NGEN is to increase competition and reduce costs throughout the program's life cycle. We also shared the Department's plans for an increased role and expanded control over the network.

The acquisition and contracting strategies have not been set, but it is likely that many companies could end up providing portions of the services associated with NGEN. We are also in the middle of conducting the Analysis of Alternatives as directed by the Office of the Secretary of Defense — examining the risk/reward related to cost, technology, schedule and performance and courses of action associated with how we deliver network services to the NGEN population.

With the notional segmented approach to NGEN, small businesses will be able to compete, as well as larger companies. This is actually not so different from the way NMCI works now; although EDS is the integrator, it does subcontract a significant portion of its work to smaller companies.

Planning efforts for NGEN have proceeded in five primary areas: requirements definition (complete), Network Operations Concept of Operations (complete), acquisition planning, a security concept of operations, and transition planning. We have gathered NMCI lessons learned and will focus on user identified needs, improved reliability and security, and network performance.

This is an exciting time that affords opportunities to improve upon an already successful network infrastructure. In returning operational control of the infrastructure to the Department, we will institute common DON governance across all areas of the network and improve flexibility and agility to support changes in DON business rules and operational warfighting missions.

Robert J. Carey

Talking with Rear Admiral Wendi B. Carpenter

Commander, Navy Warfare Development Command, Norfolk

Rear Adm. Wendi B. Carpenter

Rear Adm. Carpenter received her commission through Aviation Officer Candidate School, Naval Air Station Pensacola, Fla., in 1977 and was designated a naval aviator in July 1979. When the admiral went into the woman's pilot program, it was only a few years old; she was the 31st woman designated. Graduating at the top of her class, she was assigned as the Navy's first Selectively Retained Graduate Instructor Pilot (SERGRAD) in the T-44 aircraft at VT-31, Naval Air Station Corpus Christi, Texas. Throughout her career, Carpenter accumulated 3,500 military flight hours.

Rear Adm. Carpenter left active duty and accepted a Reserve commission in February 1985. Remaining highly active in the operational Reserve force, she has accepted numerous recalls to active duty and led four Navy Reserve commands at the commander and captain level.

Rear Adm. Carpenter's flag assignments include: Deputy Commander, Navy Region Southeast, Jacksonville, Fla. from October 2004-September 2005; acting director, OPNAV N31 (Information, Plans, Security Division) from April 2005-May 2005; vice director, Standing Joint Force HQ (SJFHQ), U.S. Joint Forces Command from December 2004-September 2006; and Deputy Commander, 2nd Fleet, from October 2006-June 2008.

Carpenter was nominated for appointment to Rear Admiral (upper half) on Feb. 13; her promotion ceremony was Aug. 8, the day after her interview with CHIPS. CHIPS met with the admiral in NWDC's temporary spaces in building N-30 on Naval Station Norfolk.

CHIPS: Can you talk about how NWDC has contributed to the change from conventional large force-on-force warfare to the irregular warfare now ongoing in Iraq and Afghanistan?

Rear Adm. Carpenter: The Navy has conducted irregular warfare for centuries. One of the beauties of how the Navy operates is that we are highly flexible and adaptable in our force packaging, and we have continued to be so in the global war on terror.

For instance, the Navy has recently developed a concept called Global Fleet Station which has provided tremendous benefits in the area of humanitarian operations and direct engagement with populations facing challenged societies, both politically and economically.

We have had Navy personnel conduct the full range of direct support efforts, including dental and medical support. We have had the Civil Engineer Corps go in and develop potable water systems and schools. Nation building helps to thwart areas and conditions where instability might arise or unstable forces may attempt to gain control.

We have conducted anti-piracy operations for years, most recently including a number of operations off the coast of the Horn of Africa and Somalia to help with the anti-piracy efforts there. We do quite a lot of anti-piracy operations with coalition forces.

U.S. Central Command has some standing organizations that the Navy has worked with for a long time, building maritime partnerships that help in the global war on terror and in thwarting irregular warfare by our enemies.

Navy Warfare Development Command is always working to develop concepts that we can release to the fleet to repackage our forces or change the organizational construct or the doctrines under which we operate. Our lessons learned programs contribute to that. We need to operate inside the decision loop of our enemy, as well as working within our own constructs of how we want to apply forces, given our rules of engagement and the kinds of things we want to do with respect to shaping the environment.

We want to be about building partnerships, capacity, preventing wars, and not having to go in and work in a situation [conflict] where some instability has already started.

CHIPS: Can you talk about some of the recent innovative products that NWDC has delivered to the fleet?

Rear Adm. Carpenter: Certainly; the Navy Continuous Training Environment is an excellent example, and within it are an entire set of smaller innovative products. But, it is not so much the innovative products that NWDC delivers that would say this has the Navy Warfare Development Command stamp on it. We partner with many other organizations and centers of excellence in the Navy to develop capability.

For instance, we work with the Office of Naval Research to develop technology solutions in areas where there are warfighting gaps or when a new technology emerges that will give us an advantage. We work closely developing solutions for anti-submarine warfare with the ASW (Naval Mine and Anti-Submarine Warfare Command) center of excellence on the West Coast.

We also work with organizations, such as the Chief of Naval Operations' Strategic Studies Group, the Naval War College, and the Naval Undersea Warfare Center, to generate and develop concepts for future Navy force packaging, strategic concepts and war gaming.

CHIPS: What is the Joint Innovation and Experimentation Enterprise? What experiments is the command working on right now?

Rear Adm. Carpenter: That's a joint initiative that works to promote innovation and experimentation across all the services.

United States Joint Forces Command (USJFCOM) is the predominant lead in that area, but each of the services has representatives.

I have people on my staff who work in this building, but there are also some people who are engaged and work at USJFCOM J9. They help to coordinate the exercise and experimentation requirements that go into the kinds of transformational things we want to look at from a joint perspective.

I met recently with Dan Davenport [Rear Adm. Dan W. Davenport, Director, Joint Concept Development and Experimentation (J9)] at USJFCOM, who is a two-star Navy officer. Navy Warfare Development Command is the Navy's enterprise lead for that coordination. It dovetails with my experimentation hat.

I will soon have a two-day session where we will look at the kinds of things that we want to experiment across the joint arena so that each service can identify what we want to test and evaluate or look into further as a spiral experiment in a joint context, partnered with other services.

In order to reach joint solutions, we try to build solutions as much as possible from the bedrock of naval service capabilities and develop joint interoperability and capability, with not only our communications systems, but with the manner in which we operate and the way we generate doctrine.

Our goal is to ensure alignment among our force, methods and important missions, such as command and control and communications, for operations across the full spectrum. The result will be greater efficiency and effectiveness.

Much of this will feed into the training that will go through [JFCOM's] J7 when they are working to train forces going into Iraq or Afghanistan or the Joint Task Force Horn of Africa, which is predominately manned by Navy personnel at this point.

JFCOM's J9 and J7 go hand-in-hand, and much of what NWDC does with respect to experimentation feeds into there, and it feeds into the Navy Continuous Training Environment.

CHIPS: Can you discuss the NWDC's modeling and simulation program and operations analysis?

Rear Adm. Carpenter: Very smart people are involved in both modeling and simulation and operations analysis. Operations analysis supports most of the other things we do. A lot of what NWDC does supports concepts and doctrine. The other programs help us in meeting the requirements to deliver to the fleet concepts and doctrine.

Modeling and simulation support us in the experimentation role because we take lessons learned or a concept we are developing and conduct war games or experimentation to further examine the areas that we need to test.

For instance, doctrine may change as technology changes, so we need to experiment with that. Sometimes, we want to do an organizational change. Right now, the Navy is doing some organizational changes with respect to a concept called MHQ with MOC, Maritime Headquarters with Maritime Operations Center. That is a major command and control initiative.

The modeling and simulation helps us to not only duplicate capabilities that enemies may have and experiment against those, but we can also simulate friendly forces. Through our modeling and simulation capabilities, we can replicate all of this in a virtual environment.

Rear Adm. Wendi B. Carpenter's promotion ceremony Aug. 8. Joining the admiral are her former aide Lt. Nolan King, her daughter Rachel Carpenter, and friend June Gurr.

We can now model realistic forces, including U.S. and foreign ships, submarines and aircraft. We link all these things together to conduct experimentation but also employ the simulation for fleet training. These efforts serve dual purposes as we evolve modeling and simulation continuously by completing experiments, while still meeting requirements for fleet training.

Occasionally, we combine experimentation with fleet exercises or training and support [that] with simulation. We deploy an analysis team to conduct evaluations of what's happening. They are not evaluating the performance of the fleet but the way that doctrine is applied and whether or not techniques and procedures are accurate. Or, they look at what may need to be changed in response to evolving scenarios, conditions or technologies.

The team brings that information back and completes an in-depth analysis. Last week, I took a report back from an exercise called Terminal Fury, which places the Pacific Fleet in a high-end scenario with a lot of moving parts. My folks came back with all the data that we captured with the modeling and simulation pieces.

We know what happened, what kinds of forces were presented to the training audience, and what their responses were. We know what kind of actions and decisions the commander made. Having all of that is a powerful force to promote change and maturity in our operations and concepts.

Now, we can analyze all of those and figure out if there were pieces where we were inadequate in our training, if we need to modify our doctrine or tactics, techniques and procedures, or if in the scenarios presented, we can identify where we can change our concepts a little bit to give ourselves an operational or strategic advantage.

Operations analysis enables us to get the maximum benefit out of these kinds of scenarios, benefiting not only the training audience, but allowing us to take away pieces that can inform our whole Navy so we make the whole organization better.

It all melds very closely together, and every single one of these areas within NWDC has to be running on all cylinders in order to feed the rest of them. There is no one area that's supreme, and they all complement each other.

As we work with other organizations, we consider ourselves

in less of a production role and more as enabling the Navy to get better in specific areas by collaborating with other organizations.

CHIPS: I noticed in the command brief that NWDC is developing the Navy's next generation digital doctrine system. Can you explain what it is?

Rear Adm. Carpenter: If you had been with me yesterday, I could have given you a quick demo. I was at an organization yesterday, which is not an inherently joint organization but a forum whereby the Army, Navy, Air Force, and Marine counterparts and I sit and discuss ways that we can help each other at the tactical level, to produce some things that are not necessarily joint across all the services but are useful to several.

For instance, convoy operations with the Army, the Marine Corps, and the Air Force, which they are all doing in Afghanistan and Iraq. We each have a similar system, and yesterday, we were comparing and contrasting the capabilities of those and how to get common procedures and techniques.

With the advent of computers, databases, and search engine possibilities, we have said that it would be very useful to the people in the field or to someone stationed at one of these Global Fleet Stations or conducting convoy operations.

It is particularly useful for commanders or senior level leaders as they are preparing operational requirements to go forward. We do a lot of this training anyway, but when they are out on the pointy end, they can just program in a phrase in a search engine and find specific information to help their circumstance.

If they would program in a phrase like 'Global Fleet Station,' it would give them not only the current doctrine and the TTPs and the links to go to those places, but it would also give them the specific paragraph that might be the most informative for them if they refined their search. If they put in a specific area of what the Global Fleet Station was going to do for humanitarian assistance and successes and lessons learned, they could pull that information out.

They can cut and paste because it is in an HTML format; they can make their own 'little black book' of procedures, tailored specifically to their needs.

I am an aviator, so we talk about pocket checklists and quick checklist cards where I have something there at my disposal to answer my questions or to give me information almost instantly. The Navy term is 'gouge.'

This new system, NDLS, gives total gouge to the folks out there deployed and doing the nation's business. It gives them capability to access what is already out there in the doctrine and find where someone learned a valuable lesson. It helps them know: How can I input that into doctrine, or can I see if it has already been done as a lesson learned? We will eventually get to a capability where a blog of dialogue is accessible from the desktop, and people will get in and out very rapidly.

Users can configure it exactly the way they want. If they repeatedly go to certain books and they want to look at joint doctrine, they can 'bookmark it.' If they want to find information for a certain geographic area, that maybe the Army has done, we are trying to link those to the other kinds of programs so they can talk and share information. We think this will be valuable in today's environment operating in ways that we have not before.

New NWDC headquarters building goes green

Rendering of the future headquarters of Navy Warfare Development Command aboard Naval Station Norfolk, Va. Groundbreaking for the new building was June 12; building completion is planned for November 2009 with occupancy expected by March 2010.

The 84,849 square-foot facility will accommodate 264 people. Three new parking areas with 498 parking spaces will ease traffic congestion on the busy Norfolk base. The approximate cost of the building project, which includes furnishings, is $28 million.

The NWDC headquarters will be the home of the state-of-the-art modeling and simulation lab which will support the Navy Continuous Training Environment, Navy experimentation and concepts of operations development.

The building will meet current Leadership in Energy and Environmental Design (LEED) Green Building Rating System™ standards, a third party certification program and the nationally accepted benchmark for the design, construction and operation of high performance green buildings.

Not only is there a Navy Lessons Learned Program, but there is a Joint Lessons Learned Program. We have set up the joint parameters in the Navy lessons learned, and we will eventually nest underneath the joint piece.

The conversation we had yesterday was that, perhaps, we can get to a point where all of these functions can also be aligned under a joint system so we allow greater integration and greater capability for all the forces.

We were thinking about ways we could make the systems complementary so that we could get the maximum use out of all of them and ensure that the information was out there the right way, with immediate availability to deployed forces.

CHIPS: How is NWDC preparing for the headquarters move from Newport, Rhode Island, to Norfolk, Virginia?

Rear Adm. Carpenter: It is a daily evolution. I have a lot of people on staff working that. We broke ground on the new building outside of Gate 3 [of Naval Station Norfolk] June 12.

We have some staff already here in Norfolk, and we still have staff in Newport, Rhode Island. We have a specific plan for moving people down in phased approaches. It partly has to do with the kinds of jobs they are doing and, partly, the things that need

Rear Adm. Wendi Carpenter with Cap'n Moby, the mascot for the Navy Lessons Learned Program. Moby serves as a vivid reminder that not learning from the mistakes of the past can have deadly consequences. The NWDC Web site (www.nwdc.navy.mil) hosts the Navy Lessons Learned Program.

to be down here sooner rather than later for our engagement purposes, such as our interaction with Joint Forces Command.

I have space in this building and in an adjacent building where we have about 60 seats. We have almost all of those filled now. We have some work going on in another building about a mile away, E-26, which will be somewhat refurbished in order to make room for an additional 60 seats. They are going to start refurbishing in the fall, and we should be able to move those people down here in January or February.

As we are transitioning people down, many people who are close to retirement have elected to retire, or there are other opportunities for them because there are new facilities moving into Newport. As jobs open up in Newport due to retirements or moves, we move that position down here and hire in Norfolk.

We have already done that with some contractors and government services. In many cases, contractors have more flexibility. With respect to the military, anyone who is in Newport will remain in Newport until the end of their projected rotation date. When that rotation date comes up, the personnel system is looking to fill the billet here, so the military will gradually transition down over the next two years.

We do quite a lot of video teleconferencing, and I make a couple of trips to Newport a month. We have worked closely with the human resources folks in the Newport area to make it as smooth a transition as possible for anyone who elects to move down here or for anyone [civilian personnel] who does not want to move and wants another [job] opportunity up in that area.

CHIPS: You were the deputy at 2nd Fleet when the plans for the move were made. Has it been difficult to take command in the middle of the move?

Rear Adm. Carpenter: I reviewed the plan that they established before I arrived and made a couple of tweaks here and there, largely with respect to contractor support. We have some additional missions assigned; it is called ADDU, or additional duties, that are now assigned to the CNO's staff. Because of that, there are a couple of billets that will potentially move down sooner rather than later.

Part of the transition plan is contingent on the building being on schedule. The modeling and simulation that we do at Newport now can be done anywhere. We designed the new building specifically to support future fleet requirements for modeling and simulation. We have designed our facility to provide an expanding capability that can meet the future needs of the fleet.

Modeling and simulation will be one of the final groups to move down even though we already have some technological support in Norfolk and a number of contractors who work at Dam Neck, Virginia, at the Distributed Training Center, Atlantic.

We do the modeling, simulation and experimentation from Newport in our M&S lab, but we also have pieces of that training network in various locations around the country, so we have distributed staff in those areas as well.

CHIPS: Can you talk about NWDC's role in NATO Standardization?

Rear Adm. Carpenter: We have a pubs section that produces a lot of the NATO pubs that have to do with the maritime environment, and I have people on my staff from other nations as well.

I have an ongoing relationship with Allied Command Transformation and with the Combined Joint Operations from the Sea Center of Excellence (CJOS COE), which resides at 2nd Fleet. My previous association with 2nd Fleet makes it easy to continue dialogue.

I have, attached to my staff, an 0-6 who resides in Brussels. Technically, he serves the military committee, and he has direct interface on a daily basis with respect to the Navy's interchange on any NATO publications or doctrine that needs to be developed.

I have a Brit on the staff, and he will comment on publications that have to do with NATO. We work with them closely with representation at the right areas, and we do a lot of coalition development with the other nations as we move forward on maritime strategy and our Navy Continuous Training Environment.

We are doing our modeling and simulation work to produce the kinds of training we need for our own fleets, and now we have the integration of many of the NATO nations involved usually on a bilateral agreement basis.

CHIPS: I was amused by Cap'n Moby on the NWDC Web site (www.nwdc.navy.mil), the Navy Lessons Learned Program mascot.

Rear Adm. Carpenter: It seems to have gotten a lot of attention. Do you know how Cap'n Moby got his name? Of course, from Moby Dick, but the real genesis behind Cap'n Moby is that if you don't learn lessons, it can cost you.

CHIPS: I read that subscribers to the program increased. Do you have information about lessons learned that saved lives, money, or lessons that were incorporated into doctrine changes?

Rear Adm. Carpenter: Not off the top of my head, but there probably are things if I reach way back in my memory.

I can think back in my own career, and this isn't related to the Navy Warfare Development Command, but there happened to be an incident when I was flying VIP aircraft where another squadron had an issue with how they were deicing their airplanes, or more importantly, how they weren't, in bad weather.

They made certain assumptions that the military's fluid

"The Navy has conducted irregular warfare for centuries. One of the beauties of how the Navy operates is that we are highly flexible and adaptable in our force packaging, and we have continued to be so in the global war on terror."

Rear Adm. Wendi B. Carpenter
Commander NWDC

was the same as the civilian fluid, and it wasn't. The commanding officer of my base called me and told me, 'This is what we found in the investigation, and I am concerned that maybe we don't know all the facts or don't understand things that we should, so tag, you're it. Figure it out, and come up with some better training and insight for me.'

I became, for lack of a better word, the Navy's guru on deicing. It was eye-opening for me, and I had flown fixed-wing large aircraft for years and used deicing fluid. The Navy's publications were not as correct as they should have been. It could be catastrophic or misleading in some instances where you had no margin of error.

We took the lessons that we learned and instead of eating somebody up for making a mistake, we looked at how we could learn from the lesson. How do we apply it to our doctrine, procedures and manuals, change what we are doing, and then produce a training program to change the behavior of everybody and make sure the education reaches down to the levels it needs to?

That is the exciting thing about being at this command. There is great opportunity to learn from the lessons and make it better so that we can help our shipmates and help other people, whether it is military or civilian, to have better impact, be safer on their jobs, and just have a better life.

CHIPS: I understand that the Navy Lessons Learned Program would like to reach not only U.S. military and civilian employees, but also contractors, joint and combined operations and allies.

Rear Adm. Carpenter: We routinely operate with each other, and sometimes, our doctrine is different. But under NATO TTPs, when we work together, we develop similar tactics, techniques and procedures, and we train together so that obviously helps us.

We share a lot of information in many international forums, not just my command but also many in the Navy, and they bring those back to us. NATO is in many of our exercises and experiments.

For instance, I was involved in an experiment in the spring, and my counterpart at the staff CJOS COE, [Royal Navy], Commodore Bob Mansergh, was working with me on the experiment. We told everybody up-front that we were interchangeable because of our schedules. I couldn't be there every single minute like I wanted to be, and he couldn't either, but the two of us would probably equal one person being there most of the time.

We also thought we could bring the added benefit of the different perspectives of how we operate. Each nation has its own particular set of rules of engagement. We have to make sure, particularly at the command level, and for command and control, that the rules of engagement are worked out ahead of time.

We know that because we have operated in coalitions for such a long time. Our senior commanders are active in making sure that they figure out ahead of time what a country can and cannot do. They might help plan an operation but not execute an operation, or they might not be willing to help plan an operation because of their rules of engagement or the direction they are heading politically.

We have good ongoing relationships. I just gave a brief at the Army War College three weeks ago, and we had a number of coalition allies in there that were not predominately NATO, but they were predominately Army officers.

Of course, we have those kinds of battlefield lessons learned going on all the time at the joint level and by people who are in the field capturing lessons learned.

Joint Forces Command sends teams out to do those kinds of things as well. They incorporate the lessons learned into joint and coalition doctrine, and get it out to us.

The Navy Warfare Development Command plays in that some, but probably the vast majority of it is going on in theater. We will take in post-deployment briefs from Navy groups that come in.

CHIPS: Is there anything else you would like to talk about?

Rear Adm. Carpenter: I am a bit unusual [in command] because I am a Reserve officer. The Navy doesn't normally ask us to do something for three years, but I had previous association with the CNO, since I worked for him when he was 2nd Fleet Commander. They asked if I was willing to come on full-time active duty for two to three years to take this command.

I have been pretty much full time since about 2000 but never imagined such an amazing opportunity would be put into my lap. I am thrilled.

I genuinely can't think of another place that I would rather be because there is such tremendous opportunity for this command. It's a tough process to go through the BRAC (Base Realignment and Closure) with the people in Newport and to make the transition — while not missing a beat — and still take on such an important mission on behalf of our Navy and nation.

The whole command has done tremendous work in the past, but I think that this is the pivotal time because of the move, because of the CNO missions, because of the kinds of integrations that there are, and because of the people that are in the senior positions in the Navy. We are poised at NWDC to have an even bigger impact than we have in years past.

I am excited to get up and come to work every day. It is more than an honor; it is humbling to think about the capability and the capacity of the people that belong to this organization. To have been chosen to help guide them to the next level is a tremendous honor and opportunity.

Thirty-one years after I came into the Navy, I am excited to still be a part and doing what I do. It's fun, I love the people, I love the challenge, and I leave at the end of the day feeling that I made an impact on our security and on the lives of my shipmates. CHIPS

Interview with Rear Admiral Gregory A. Timberlake
Command Surgeon, U.S. Joint Forces Command
Medical Advisor, Allied Command Transformation
Deputy Command Surgeon, U.S. Fleet Forces Command


Rear Adm. Gregory A. Timberlake

Rear Adm. Timberlake is currently on leave of absence from the University of Mississippi Medical Center, Jackson, Miss., where he is a Professor of Surgery, Physiology and Biophysics and was the Director of Trauma Services and Head of the Section of Trauma and Surgical Critical Care.

Very active in developing and providing trauma care both in this country and internationally, Dr. Timberlake served 10 years on the American College of Surgeons Committee on Trauma and its Subcommittee on Advanced Trauma Life Support. He is one of the coauthors of the last three revisions of the course and textbook *Advanced Trauma Life Support for Physicians*.

Rear Adm. Timberlake is a Fellow of the American College of Surgeons, the American Association for the Surgery of Trauma and numerous other prestigious medical organizations. Additionally, he authored or coauthored more than 40 peer-reviewed manuscripts and several books and monographs on the care of the sick and injured.

CHIPS talked with Rear Adm. Timberlake in July about the changing dynamics of military medicine and technology advances in caring for combat injuries.

Rear Adm. Timberlake: The 'Long War' has changed the way military medicine operates. Over the last several years, we have all come to the realization that the current medical model is not appropriate for the realities military medicine faces. For example, U.S. Central Command may not have a need for 1,000-bed fleet hospitals or 500-bed combat support hospitals (CSHs) as it might have in previous campaign plans. It needs something modular that can adapt to current warfighter needs.

Currently, a modular approach to theater hospitalization capability (Role 3 capability–NATO), such as we have in Bagram [Afghanistan], Balad or Baghdad in Iraq has proven effective. This modularization brings the required flexibility needed by our surgeons (and the associated surgical equipment) forward to the battle area where it is needed. The Army calls this capability forward surgical teams (FSTs). The Navy and Marine Corps call it the forward resuscitative surgical system (FRSS).

Additionally, military medicine is becoming more joint. If one service is out of a required capability, then we work with the other services to fill the gap. Last year, we had over 170 requests for forces, and we were able to fill all of them through the use of this joint integration. The request for medical capabilities helped to sustain our efforts in Iraq and Afghanistan, as well as the significant footprint we currently maintain in Kuwait.

Additionally, we met requirements in the Horn of Africa, and more recently, humanitarian assistance (HA) missions that are ongoing in SOUTHCOM (U.S. Southern Command) and PACOM (U.S. Pacific Command). To accomplish our HA missions we have utilized not only the traditional hospital ships, USNS Comfort and Mercy, but also traditional Navy gray hulls, like USS Kearsarge.

We worked with Special Operations Command because their organic medical support teams needed augmentation. We put together packages, working with the services, that included the people, training and equipment, so SOCOM requirements were met.

One of the capabilities that has helped meet these enduring and 'new' mission requirements has been ongoing feedback and the joint operational lessons learned process conducted through the Joint Center for Operational Analysis, here at USJFCOM. The JCOA identified many of these medical issues and sparked new ways of doing business to improve support to the joint force.

A half a year or so before I came here, the Deputy Secretary of Defense (DEPSECDEF) tasked us to improve joint warfighting through Joint Force Health Protection (JFHP) transformation. We were to come up with a way to identify the gaps and seams that the joint force needed to fix in the medical community looking out to 2015-2025.

It has been an exciting journey. First, we started with the premise that we were doing pretty good today. The joint medical community right now is providing our warfighters with the lowest died-of-wounds and disease non-battle injury rate we have ever seen. We are doing very well, but you can always strive to do better.

We put together a number of teams from my office that included membership from the Office of the Assistant Secretary of Defense for Health Affairs, the Joint Staff Surgeon's Office, the services and the combatant commands (COCOM). We focused on the operational-expeditionary side of delivering health service support to the joint force.

We looked at the medical support people need, from the time they deploy, to the time they return, whether they are injured or not. This initiative includes preventive medicine. You deploy a healthy, fit force. *How do you keep them healthy?* If they get sick or wounded, you need to make sure you can treat them. *How do you make sure that you have the appropriate medical command and control?*

I am proud to say that the JFHP concept of operations, mandated by DEPSECDEF, and developed in partnership with Health Affairs and the Joint Staff, was approved in August 2007 by the Joint Requirements Oversight Council, whose members include the vice chiefs of each military service.

The CONOPS provides a unifying vision that directs joint capabilities-based analysis and six joint capabilities documents. The six functional areas are: Joint Casualty Management; Joint Medical Logistics and Infrastructure Support; Joint Medical Command and Control (which will be added to the Joint Command and Control Joint Capabilities Document as an annex); Joint Patient Movement; Joint Health Surveillance, Intelligence

and Preventive Medicine; and Joint Human Performance Enhancement.

The top gaps in the six JCDs will be prioritized to provide an enterprise-wide approach and integrated investment strategy across the Military Health System for solution analysis. I am also proud of the fact that medical was the first functional area within the Logistics Portfolio to have a CONOPS.

Within the six functional areas, over 200 gaps and seams have been identified. Although the plan is to develop solutions for the 2015-2025 timeframe, many findings are being used to prioritize resources for research and development in the near term, as noted in DoD Guidance for Development of the Force.

CHIPS: How has treatment in field medical facilities changed, and how has technology helped in treating wounded service members?

Rear Adm. Timberlake: We have seen a huge evolution in our facilities. The first thing is that we are bringing surgeons closer to the wounded. There is no question that having the FRSSs and the FSTs in the forward areas of the battle have allowed us to save patients that would have died of injuries before. That's number one. We have brought in more specialists. For example, we have neurosurgeons in both joint areas of operation now, and they can intervene as soon as wounded come in.

We have improved technology for vascular injuries. We have been able to use angiography and take pictures of the arteries and the veins, so we can tell which ones need surgery or how well the surgery has done. We have new ventilators, and we have new types of tourniquets that work better.

We are teaching corpsmen, medics and ground troops in combat life-saver training how to stop bleeding. We have new hemostatic dressings and bandages that help the blood to clot and the three services are looking at two next generation products that seem to work even better.

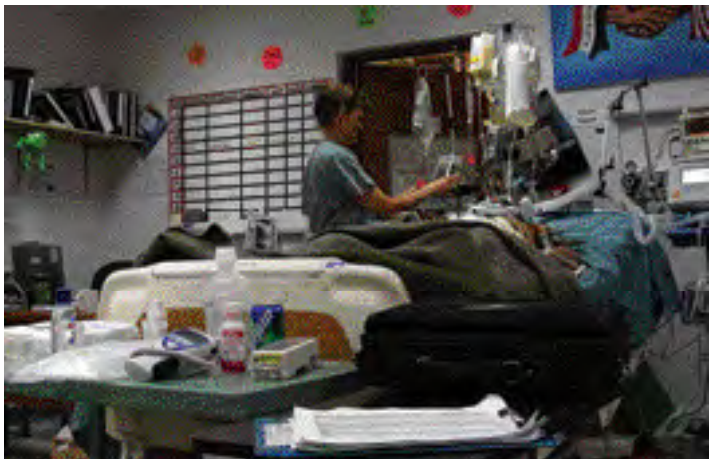
Another huge advance is 'damage-control' surgery, or the concept that you don't have to do everything in one operation. By that I mean, those injured in a battle may get care from a corpsman or medic who stops the bleeding and starts intravenous fluids, takes them back to one of these forward areas where a surgeon does just enough to prevent death and limb loss but does not do the definitive repairs. You do enough to save their life and get them to the next level of care.

We used to talk about the 'golden hour' — the critical first 60 minutes of treating a severe injury — but we now talk about the 'platinum 10 minutes.' Corpsmen treat the injured on the battlefield in the platinum 10 minutes, and move them up the combat care chain.

Looking at the platinum 10 minutes, the golden hour, and then back to a theater hospital where we may do more resuscitation, stabilization, and maybe more surgery, we are talking about two, four or six hours. It is a shorter timeline than we have ever seen.

Following battlefield care we move them to theater level then to Landstuhl Regional Medical Center where a tri-service team evaluates them. The tri-service team is made of organic Army personnel, supplemented by Air Force personnel, and for the last three years, a Navy contingent — around 300 people.

There are neurosurgeons and vascular surgeons, critical care specialists, psychiatrists to critical care and OR (operating room) nurses, psychologists, chaplains and specialty corpsmen, from general duty that work on the wards, to X-ray technologists and laboratory technicians.



Army Capt. Virginia Griffin monitors instruments used to treat a patient in the intensive care unit at Ibn Sina Hospital, where the 10th Combat Support Hospital (CSH) is based, in Baghdad's International Zone. Photo by Jim Garamone, American Forces Press Service.

Patients are reevaluated and, in as little as 24 to 48 hours, they are back in a place, like Walter Reed Army Medical Center or National Naval Medical Center, Bethesda, Maryland, Brooke Army Medical Center in San Antonio, Texas, or San Diego Naval Medical Center, for completion of their definitive care.

There was one famous case over a year ago where an Army Soldier was doing a platoon sweep and an insurgent stabbed him in the face. The knife was next to one of the major arteries in his brain. He was taken to one of the theater hospitals where they determined that it was unsafe to remove the knife. He needed definitive care at Bethesda by the combined Army-Navy neurosurgical team. The Air Force diverted a plane, picked him up in theater and took him directly to Bethesda where he had his life-saving surgery.

Compared to my civilian practice, they are moving people that I wouldn't have sent out of the intensive care unit to get a CT scan. They are moving them back to CONUS in a short time. We have come to accept it as normal, but it is truly extraordinary.

These represent major changes to military medicine. We no longer have a 30-day theater hospitalization policy. We used to set up these big hospitals, and if injured service members couldn't be returned back to their unit in 30 days, then we would start thinking about evacuating them.

CHIPS: The successes must have a lot to do with training.

Rear Adm. Timberlake: It does, and the TCCC, or Tactical Combat Casualty Care is the basis. The driver was Capt. Frank Butler, who is now retired. He was the command surgeon for SOCOM for a number of years. He was forced to get his Special Operations Command medics and corpsmen trained at a higher level, and now a lot of that training is being taught to all corpsmen and medics, advanced first aid, if you will. It became obvious that we needed to accelerate this approach as a community.

CHIPS: When Joint Task Force-Horn of Africa deployed, did your office do a pre-deployment assessment for what they would need?

Rear Adm. Timberlake: No. It is up to the COCOM, the combatant commanders, and their planning staff to determine what the missions are going to be and what forces they are going to require. However our staff is involved in the training that supports these missions.

The Joint Medical Planner's Course is sponsored by the Joint Staff and is targeted for personnel going to a job as a medical planner. The Joint Operational Medical Managers Course, sponsored by the Defense Medical Readiness Training Institute, and the annual Joint Task Force Senior Medical Leader Seminar (JTF SMLS), sponsored by USJFCOM, are geared towards medical department officers in the ranks of 06s and senior 05s.

The services nominate their attendees with the expectation that the attendees will be in leadership roles, preferably as a joint task force surgeon or a COCOM surgeon.

Currently, there are no medical personnel in the billet structure of USJFCOM's Standing Joint Force Headquarters element. So they contacted us and I assigned one of my medical planners to them for this mission. Cmdr. Michele Hancock went over to CJTF HOA for five months, serving as the medical subject matter expert in the J5 shop helping with planning future medical missions.

We are now working with U.S. Africa Command (AFRICOM) to help their surgeon set up his cell and identify what his tasks and roles should be. We are also helping in some of USJFCOM's J9 experiments. For example, USJFCOM has an experiment called Healthy Africa Scenario Exercise where we are working with West African nations (both military and civilian components), AFRICOM and U.S. European Command, U.S. government agencies, NGOs (nongovernmental organizations) and IOs (interagency organizations) to decide how we can leverage medical capability as a tool to reduce future conflict in African nations.

CHIPS: What does medical experimentation entail?

Rear Adm. Timberlake: We take many concepts, ideas and get people together, like we are doing in West Africa, under the lead of J9, to identify problems and potential answers. We have some play in the Noble Resolve and Urban Resolve experiments, as well as Multinational Experiment 4 and 5.

Our office works with [JFCOM's] Joint Warfighting Center (JWFC), who is responsible for the Unified Endeavor mission rehearsal exercises that train personnel to assume missions in JTF headquarters in the USCENTCOM area of responsibility.

Additionally, they conduct COCOM Priority 1 and 2 Exercises. One of our staff is assigned to the JWFC full time to be my medical representative. We were involved with Second Fleet's certification as a JTF and some of our reservists came in and played the roles of members of the medical cell as if they were part of the JTF.

CHIPS: Is that part of their certification to be a JTF?

Rear Adm. Timberlake: Yes, they have to prove that they can work in that joint environment. They have to coordinate all the service elements assigned to them.

We have also been involved with USJFCOM's Standing Joint Force Headquarters' response for assistance at CDAC-PAK (Combined Disaster Assistance Center Pakistan), our military response to the Pakistan earthquake. Also, when they set up JTF-Lebanon, they asked again for medical planning expertise.

Rear Adm. Gregory Timberlake (seated) with staff members, Air Force Lt. Col. Debra Timm, Army Maj. Patrick Lukes, Navy Capt. Tammy Nathan and Army Col. Sandra Evans in the admiral's office at USJFCOM headquarters in Norfolk, Va.

CHIPS: How do you determine the kinds of medical support needed for a relief effort?

Rear Adm. Timberlake: If the COCOM does not have organic service elements that can respond, then through the request for forces process, a request would come to USJFCOM, and we would work with the services to identify who has got the capability, for example, a CSH, an air transportable hospital, to meet the mission requirement.

With the COCOM, a set of parameters would be determined for the specific mission. This requires discussion with my planning staff. Maybe we need obstetricians, pediatricians or family practitioners because there are going to be a lot of pregnant women in need of medical attention, and surgeons would have a reduced footprint.

The timeline in a relief effort is also important. Medical needs will change as the situation on the ground changes. We have been proactive in influencing the commanders to take a senior medical planner because the planner will have an idea of this dynamic timeline. The medical planner will also be able to interface with the locals, the IOs and the NGOs to be sure that duplication is minimized.

CHIPS: Is the civilian medical community looking at what's been done in military medicine for wider application?

Rear Adm. Timberlake: As with all conflicts, lessons learned in military medicine find their way into civilian practice. In Vietnam a lung problem was described initially out of Da Nang. It was called 'Da Nang lung,' and now it is called post-traumatic pulmonary insufficiency or adult respiratory distress syndrome.

The current conflict has allowed us to begin to explore the platinum 10 minutes and work on training and education that will transfer into the civilian community as it matures.

We are also working on patient tracking systems that will aid our civilian counterparts in disaster relief. The use of warm blood and blood components was sort of known, but the average trauma center has only one or two people a day at most that might need it. We, in the military, need it routinely. In fact, this has become a standard practice — not experimentation.

CHIPS: Do you confer with your NATO counterparts?

Rear Adm. Timberlake: I am also the medical advisor to the Supreme Allied Commander for Transformation. We are the theoretical folks at ACT and Allied Command for Operations, the old SHAPE, Supreme Headquarters Allied Powers Europe. We consult with our NATO counterparts and continually work on doctrine and training to ensure that, with our NATO colleagues, we continue to deliver quality medical care to our warfighters.

This is not to say there are not shortfalls between what NATO calls Role 2 and Role 3 deployable medical units. Outside the United States, most countries have a hard time fielding a theater hospital and maintaining it out of their own organic personnel, materiel and supplies.

CHIPS: Is it because of the cost?

Rear Adm. Timberlake: Partly the cost, and partly because under the NATO emerging construct, which was self-defense, civil defense against the Russian 'bear,' we were all focused on the Fulda Gap. Each country had its own area of responsibility. In that situation, it made sense that you would have minimal medical up-front. You would provide minimal care and send the injured back by ambulances or trains to your countries' hospitals.

Then those trains would go back to theater with bandages and medical supplies. The nations did not have a reason, in most cases, to plan for large expeditionary units. They did not have to develop the same expeditionary capacity that the United States did because we are always forward deployed.

To provide adequate patient care experience for their medical personnel, NATO countries started to include military medicine in their national health services. Now if they have to pull out a significant portion of their medical personnel, it has a potentially negative impact on that country's ability to provide care to its civilian population.

We realized early on that it was going to be an issue, and we developed a concept and wrote a paper on multinational medical units and unit certification. ACO has implemented that. For example, if the Canadians have the lead for a Role 3 theater hospital in Kandahar, but the Canadians by themselves cannot staff an entire theater hospital, they will ask other nations for assistance.

This has been very successful. The hospital in Kandahar is a Canadian hospital that has one-third British personnel and one-third Dutch, along with a few Americans.

The Spanish Role 2 hospital has a couple of Bulgarian surgical teams because the Spanish couldn't provide all the surgical teams that they needed for that size installation.

At Role 2, the staff size is 25 to 50 people. With Role 3, you are talking about hundreds. Our hospitals at Baghdad and Balad have a significant footprint with a lot of specialties. Staff size can be a challenge to the 26 NATO nations to provide forces through the concurrence of the Committee of the Chiefs of Military Medical Services, a committee of chiefs of medical departments of NATO.

This is a clear example of how NATO's member nations can work together to support a military mission using integrated NATO medical assets.

CHIPS: Is there anything else you would like to talk about?

Rear Adm. Timberlake: You mentioned experimentation; we serve as the operational manager for an advanced concept technology demonstration, Epidemiology Outbreak Surveillance (EOS), which is transitioning from a concept into two programs of record (POR) this year.

EOS is an environmental surveillance and clinical diagnostics system of systems that will improve our environmental surveillance capabilities of biological threat agents as well as the clinical response to influenza-like pathogens.

EOS contains pathogen agent detectors and peripheral data collection, distribution and analysis data systems, that can, for example, potentially identify a sudden increase in flu cases in a specific area and whether or not the flu has characteristics of a specific strain like Avian.

The pathogen agent detector piece of EOS is transitioning into a system called JBAIDS, Joint Biological Agent Identification and Diagnostic System, the POR for environmental surveillance for deployed forces to identify biological warfare agents. EOS

"We used to talk about the 'golden hour' — the critical first 60 minutes of treating a severe injury — but we now talk about the 'platinum 10 minutes.' Corpsmen treat the injured on the battlefield in the platinum 10 minutes and move them up the combat care chain."

– Rear Admiral Gregory A. Timberlake
Command Surgeon, U.S. Joint Forces Command
Medical Advisor, Allied Command Transformation
Deputy Command Surgeon, U.S. Fleet Forces Command

will expand JBAIDS' traditional role of environmental surveillance to include clinical diagnostics of upper respiratory influenza pathogens.

The data collection, distribution and analysis data systems of EOS are becoming part of the Theater Medical Information Program – Joint (TMIP-J), now within Defense Health Information Management Systems (DHIMS). Our technical manager is from the Air Force Surgeon General's office.

Future generations of EOS will contain a much smaller footprint, will be more utilitarian, and able to recognize a threat using advanced diagnostics which will push the envelope for future capabilities. We are pleased with the progress and believe EOS is going to be a big advance.

We are also working on a proposal for a new joint capability technology demonstration. We can provide excellent care, as long as the medics are on-site, and those injured can get to the doctor and on to the hospital rapidly; however, operations in remote areas do not have easy access to FSTs or theater hospitals.

We are constantly asking questions like: What if a U.S. Navy frigate operating in the Indian Ocean stops a suspicious vessel and a bunch of Sailors get injured? We seek to answer these questions, in part, by employing advanced technologies to bring supplies forward and return the sick and injured.

Our proposed JCTD is titled Joint Medical Distance Support and Evacuation, and it has support from USSOCOM, USPACOM, U.S. Northern Command and a number of the services.

The proposal seeks to adapt the following: (1) current telemaintenance technology for battlefield telemedicine to provide virtual triage and automated patient monitoring/care at a distance; (2) aerial precision delivery capabilities to provide small medical bundles or equipment to dispersed ground and maritime forces from a variety of rotary and fixed-wing aircraft; and (3) current unmanned aerial and ground vehicle systems (UAS/UGV) to provide rapid precision delivery of medical capabilities and casualty evacuation from 'denied' or remote areas.

CHIPS: How do you choose what to investigate?

Rear Adm. Timberlake: At the COCOM level, it has to have joint theater-wide applicability. For example, there is a new tool that is supposed to determine if someone who is unconscious has a concussion or a blood clot in the brain. That would not rise to the COCOM level.

Generally, when a service or a COCOM has something that they think has wider joint applicability they look for an operational sponsor or an operational manager. For example; USPACOM is the operational manager for Medical Situational Awareness in Theater. MSAT is a situational awareness tool that fuses medically relevant information from a joint medical workstation to joint medical surveillance/intelligence.

They are putting this information together so that the JTF surgeon, COCOM surgeon, or commander of the combatant command has robust situation awareness of medical information.

Some questions this tool will aid in answering are: Are there disease outbreaks? Is there an increase in people taking up beds in an institution so they need to shift resources? Where should I put down my medical footprint if I am going into country 'X' to do a medical mission? It puts that all together for the commander. It is a common operating picture.

I have two Air Force international health specialists dealing with security, stability, transition and reconstruction operations (SSTRO) — commonly referred to as 'soft power.' There are huge issues concerning what the military should do, and how they should interface with the rest of government, NGOs and IOs. We have the lead for medical operational expeditionary.

Sometimes, I wonder how much we can do, especially adding on these soft power missions. In the medical community, we have always answered the bell. Sometimes, I think we could do things differently or better.

We are starting to build the DOTMLPF (doctrine, organization, training, materiel, leadership and education, personnel and facilities) because all the soft power SSTRO initiatives were not a primary mission for the military prior to the publication of DoD Directive 3000.05 in November 2005 which said we had to give equal priority to SSTRO as we have to major combat operations.

SSTRO has never been a primary mission — we've done it — and we've done it well. The challenge is to embed these mission sets into our manning, training, equipping and doctrine postures, so we don't continue to start from scratch when these efforts are called for by our warfighters.

Rear Adm. Michael H. Mittelman will replace Rear Adm. Timberlake as U.S. Joint Forces Command's (USJFCOM) top medical advisor in October when Timberlake assumes duties as the Assistant Deputy Surgeon General for Active-Reserve Integration. CHIPS

Military medicine transformation includes modular field medical facilities in forward battle areas and changes in the treatment of injured warriors in the combat care chain which dramatically reduce the timeline for treatment of the wounded.

Technology has assisted in the transformation with new ventilators, angiography, hemostatic dressings, bandages, tourniquets and much more.

Corpsmen, medics and ground troops now have combat life-saver training on how to stop bleeding and advanced first aid so that those injured can successfully advance to the next level of care.

Mark Arnold points out features of the ventilatory assist device for forward surgical teams (FST). Photo by Karen Fleming-Michael, American Forces Press Service.

Empowering the Information Systems Technician and Information Professional Workforce with an ITIL Framework

By Lt. Cmdr. David T. Purkiss

"Network-centric warfare," "NetOps" and "managing the Global Information Grid as a weapon system" — for many these are still little more than buzzwords or catchphrases. For Navy communicators, they are beginning to become actual concepts. Yet, like the six blind men in the famous Indian legend each describing an elephant very differently, defining such concepts depends largely on one's perspective, and few, if any, are positioned to see and understand the entire picture clearly.

The challenges and solutions of network-centric warfare, as viewed by various commands, engineers, numbered fleet staffs, operational commanders, deckplate operators and technicians; or watchstanders on ship or shore, are as varied as the people and their roles.

However, most can agree on at least three points. First, delivery and support of secure and reliable end-to-end information services across the Navy Enterprise Network is extraordinarily complex and fraught with a myriad of interdependencies and daunting challenges.

Second, we in the Information Professional and Information Systems Technician communities are among the core communities entrusted to transform these concepts into reality.

Finally, and most importantly, we can — and must — do better.

Technology or Process

Situational awareness, or a network common operational picture (NetCOP), to share the health and status of the Navy network is part of the solution set receiving a lot of focus today. Unfortunately, too many within our community are searching for some whiz-bang tool or magical technology to achieve this "solution."

But delivering a new tool or technology and more information to the warfighter does not necessarily provide additional capability, and could actually compound an already complex problem.

As history has shown, delivering actionable information to the warfighter at the right time and place in a meaningful way is a problem littered with lessons from modern warfare.

For example, on Dec. 7, 1941, the latest technology of the day worked perfectly, yet failed to produce a meaningful capability. The SCR-270B Ground Mobile Radar Station on Opana Peak on the North Shore of Oahu detected the in-bound Japanese attack force a full 36 minutes before the first bombs hit.

Radar operators detected and dutifully reported the information to the Communications Center at Fort Shafter Honolulu, Hawaii. That the technology performed flawlessly is an almost forgotten detail, except to the engineering community. From its perspective, the SCR-270B radar was a marvel achievement, and the Opana site was later recognized by the IEEE-USA, an organizational unit of the Institute of Electrical and Electronics Engineers, and memorialized with a National Historic Site plaque just off Kamehameha Highway near Turtle Bay.

Yet, not a single commander, watch officer, Sailor, Soldier, Airman, or anyone who could have come to the island's defense, was armed with the information that could have prevented the death of at least some of the thousands of lives that were lost that day.

The lesson for us modern-day net-centric warriors is that simply delivering technology that performs to "specs" does not empower the warfighter without executing a capable and disciplined "process" that reliably delivers meaningful information to the right place — at the right time — to the right people. In short, *it's the process, stupid — not the technology.*

As the communications officer for Naval Computer and Telecommunications Area Master Station Pacific (NCTAMS PAC), my particular piece of the elephant was IT service support to the fleet: managing shore-to-ship connectivity to include satellite activations, the transport layer, networking and IP services.

Over my 22 years in the Navy, technology has changed drastically and constantly, and the pace is quickening exponentially, yet our operational processes and management methods in the communications world are largely stuck in the 1950s in which our primary mode of operation is to wait until an operations watchstander attempts to use a circuit or information service that is unavailable, or worse yet, a distant end unit detects an outage and reports the problem using the slowest and most inefficient method available.

Not only is this a purely reactive process, it is a very slow one that relies on an antiquated one-way communication flow model using naval message traffic as the "enabling technology."

It is only through the extreme dedication and sheer determination of our Sailors that the Navy successfully communicates using technology that spans 50 years and business processes that are even older. Fortunately, for all of us, and for the sake of our hardworking Sailors, there is a better way.

ITIL is Tried and True

The Information Technology Infrastructure Library (ITIL) is a set of guides and techniques for managing an organization's IT infrastructure, development, operations and maintenance in concert with the business objectives of the organization.

Developed in 1992, and maintained by the United Kingdom's Office of Government Commerce, ITIL was intended to serve as a set of standards that service providers had to follow to deliver IT services to the British government. After its inception, public companies worldwide quickly realized its benefits and implemented parts of ITIL in their internal IT departments.

Since then, ITIL has become an increasingly accepted method of managing IT

Technology has changed dramatically in naval communications, yet improvements to operational processes and business transformation lag behind technology improvements.

Pearl Harbor, Hawaii (Aug. 22, 2006) - Secretary of the Navy, the Honorable Dr. Donald C. Winter, greets IT3 Brent Jackson during a visit to NCTAMS PAC. NCTAMS PAC manages, operates and maintains defense communication system and naval telecommunication system assets by offering a full range of automated data processing and information resource services. U.S. Navy photo by Mass Communication Specialist 1st Class James E. Foehl.

services because it provides a detailed description of a number of important IT practices with comprehensive checklists, tasks and procedures that can be tailored to fit any IT organization.

Each interrelated process follows a disciplined Plan-Do-Check-Act model that facilitates monitoring, reporting, metrics and continuous process improvement. ITIL easily takes advantage of enabling automation and technology when implemented as an integral component of specific process steps, procedures or functions.

ITIL is tried and true; it is the process model for thousands of organizations including: Microsoft, IBM, EDS, Hewlett-Packard, Capital One and the U.S Army, to name a few.

The primary advantage of ITIL is that it consists of open source information, simply a collection, or library, of industry best practices, easily adaptable to any environment, and developed to meet specific IT service needs and goals.

At its core, the ITIL process-oriented approach requires an understanding of the business requirements, then designing a solution to meet those requirements.

The solution designed uses ITIL descriptions adapted to specific environments. The approach is not to select a technology or tool and build a process, but rather to:

- Understand business needs and requirements;
- Design the organization and process workflow;
- Define and specify required tools and procedures; and
- Select and implement tools.

The potential for a disciplined approach to IT service management is capturing attention in Navy IP officer circles as a possible solution to long-standing IT service challenges in delivering products to the fleet. Significant grassroots efforts are being pursued at NCTAMS Atlantic and Pacific in the West and East Regional Network Operations and Security Centers (RNOSC) and other pockets within the Navy.

Defining the Problem

There are several compelling reasons to use the ITIL approach. The Navy's IT and IP workforce are stressed by four divergent drivers:

- Reduced supply – Five years of cost-cutting measures have downsized the shore command, control, communications, computers and intelligence (C4I) infrastructure; consolidated and closed facilities; and cut shore IT manning in half.
- Increased demand – Steady growth in demand and reliance on C4I capacity and greater complexity in providing C4I products.
- Greater risk and cost of failure – Growing capabilities by our adversaries to exploit C4I infrastructure vulnerabilities and attack our networks create potential risks of compromising our most valuable weapon and principal competitive advantage: information superiority.
- No appreciable maturation of processes – Focus on technology and systems has failed to improve IT service delivery and support.

Technology has changed dramatically in naval communications, yet improvements to operational processes and business transformation lag behind technology improvements. As a result of these factors, the IT and IP workforce are now working harder instead of smarter, and leveraging technology as a force-multiplying solution is falling short of expectations. Further, C4I services to the fleet often fail to meet loosely defined requirements or fleet expectations.

New technology and systems are being installed at a breakneck pace. However, not all reach initial operational capability on schedule, and because shore installations are not aligned with ship installation schedules, few legacy systems are being removed or replaced from shore. This creates an ever-broadening range of complexity in technologies and the sheer number of systems for NCTAMS to support. For example, there are four Automated Digital Network System (ADNS) variants and nine different messaging systems supported by NCTAMS today.

Business practices and operational processes are primarily reactive following the traditional communicator model of waiting for the user to report a problem.

The fleet continues to rely on trouble reports, Communications Spot (COMSPOT) naval messages, as the only "official" method of reporting, tracking and collaborating on communications and network outages. This slow reactive method largely precludes the use of automation, data mining and metrics analysis for problem management and process improvement.

In 2005, Naval Network Warfare Command (NETWARCOM) sponsored a study of afloat and shore IT service management processes, conducted by a well-known consulting group. Results showed:

- Few documented or repeatable processes exist on shore or ships.
- Multiple groups work independently

"The good thing about the ENMS system is that it incorporates industry best practices for IT Service Management. We can capture information in real time, search that information on demand, and build a dynamic knowledge base that inherently focuses on those areas where we can improve most."

– IT1 Jason Krahmer
RNOSC West

on the same issues; problem correlation is manual.

• No common operational trouble reports or logs exist.

• Joint Fleet Telecommunications Operations Centers (JFTOC) rely on printed COMSPOT reports using a paper-stacking, color-highlighting priority scheme.

• Problem management, including: detection; investigation; escalation; coordination; root cause analysis; and prevention of recurrences, minimally exists.

• Traditional hierarchical organizational structure and ineffective prioritization create inefficient reliance on senior-level personnel for routine tasks.

An internal site survey at NCTAMS concurs with this assessment, acknowledging inconsistent processes that rely on manual procedures and disparate tools, including 27 different autonomous "databases" and 46 paper-based logs, each independently and redundantly tracking/reporting operational processes.

Ideally, a performance baseline would have been established to assess the impact of such drastic changes in manning, tools and processes. However, few metrics exist to measure performance against service level expectations or to identify trends. The few metrics that are available indicate that performance falls consistently far below expectations or requirements.

IT Service Management

Working together from a disciplined, governed ITSM process framework that aligns and integrates plans and policies, acquisition, technology, operations and fleet service requirements will empower us to succeed as a team and overcome these obstacles to provide first-class IT products to the fleet.

Training our workforce to this standard set of practices and repeatable processes is vital and achievable, and initial training and plans for process changes have already been implemented.

The key to progress is coevolution of the technology, tools and systems, people and processes. The RNOSC IT Service Management working group is currently attacking five simultaneous priorities to achieve this coevolution.

Training. We are aggressively pursuing the RNOSC/ITSM training plan for watchstanders and leaders. More than 200 Sailors, civilians and contractors have completed the initial half-day RNOSC/ITIL awareness training so far at NCTAMS PAC and LANT.

Our goals for this initial awareness training are to: (1) provide a common ITIL-based NetOps vision and the road ahead for RNOSC; (2) introduce ITSM processes based on the ITIL framework; and (3) integrate an RNOSC/NetOps vision with ITIL processes and the Enterprise Network Management System/Trouble Management System (ENMS/TMS), an automated system that allows network administrators to identify and resolve problems.

Comments from our student course critiques are overwhelmingly positive and enthusiastic. We continue to use ITSM/ITIL courses available on Navy Knowledge Online (https://www.nko.navy.mil) and other low-cost options for ITIL training and certification.

The ITIL awareness curriculum was included as part of the operations department indoctrination training for newly reporting personnel at both NCTAMS PAC and LANT, and ITIL certification will become part of our qualifications standards.

A dozen personnel in the department have completed ITIL foundations certification, some preferring to pay out of their own pocket for certification rather than waiting for approved funding.

We have mapped ITIL certifications to specific watch stations and supervisory positions and are working to fund the next phase of our training plan that will include foundations, practitioner and manager certifications for critical service center personnel and managers.

"Adopting ITIL is allowing the Navy to change how we do IT business. We are building a knowledge base within ENMS which allows operators to instantly see possible solutions to trouble tickets greatly reducing the time spent troubleshooting," said IT1 Gene Morsen, who works in the operations department of NCTAMS PAC.

Service Desk Function. We are reorganizing the NCTAMS watch team into tiers of technical support, implementing a formalized service desk function that ties the shipboard communications watch team with NCTAMS into tier one of the watch organization.

This discourages the traditional linear and ad-hoc approach to handling incidents and problems on the watch floors, providing a dedicated service desk for customer interface, effectively capturing data, and accessing a knowledge base for easy configuration verification, service requests and requests for information, and escalation to the next tier of technical support for further diagnosis and restoration.

Additionally, a formalized service desk function will facilitate effective reporting and integration with regional maintenance and in-service engineering resources via the Global Distance Support Center.

A comprehensive Service Desk Function Guide was completed in May to implement a standardized service desk function for each watch team at NCTAMS PAC and LANT, and will be delivered to the Naval Computer and Telecommunications Centers in conjunction with the ENMS/TMS roll out later this year.

This vital first layer of the watch team will provide a dedicated and consistent customer-service interface and record all incidents into the TMS, and enable proactive monitoring of system alerts and alarms using ENMS.

Incident Management. A disciplined incident management process will ensure consistently executed detection, recording, classifying, prioritizing, diagnosing and resolution of all incidents and outages enabled by ENMS/TMS. The RNOSC Incident Management Process Guide was written to integrate the ENMS/TMS tool for information sharing and the defined processes and procedures to generate an understanding of the situation, thus achieving far beyond the limited goal of sharing status, or situational awareness, attaining situational UNDERSTANDING.

The Navy's FORCEnet experiment series, Trident Warrior 2008, which executed in June, was our first opportunity to integrate fleet IT into the shore incident management process using the ENMS/TMS tool.

Using coevolved technology, processes and people, with a coordinated incident management process, the ENMS/TMS tool set and ITIL-trained personnel, critical segments of the incident cycle were drastically reduced from hours to seconds.

Problem Management. A formalized process for performance trend analysis of fleet tactical services will prevent future incidents. The first significant body of performance metrics has been collected over the last four months, culminating in our Satellite Communications (SATCOM) Activation Metrics message, distributed monthly since October.

Problem management will formalize a capable process in a structured and governed way. The first draft of our Problem Management Process Guide has not been started because it depends entirely on a solid service desk foundation and a disciplined incident management process as a precursor for its success.

The ADNS program office and Program Management Warfare (PMW) 160, Networks, Information Assurance and Enterprise Services, under Program Executive Office for C4I, and in collaboration with the Space and Naval Warfare Systems Command, has offered to help using the Fleet Systems Engineering Team (FSET) as the primary and enabling technical resource — which dovetails perfectly with our future plans. Eventually, ENMS/TMS will be an integral and enabling tool for this process.

ENMS/TMS. This is the centerpiece tool. Existing tools such as Route Explorer, WhatsUp Gold and even some homegrown Web-based tools still remain part of the RNOSC toolbox. However, the RNOSC watch team is using ENMS/TMS as our primary means for recording and tracking all incidents and outages. Further development will allow ENMS/TMS to become a primary detection tool as well.

The RNOSC East/West team participates in weekly Change Engineering Board telephone conferences with the tactical switching ENMS/TMS development team from PEO C4I's PMW 790, Ship Integration, to continually improve ENMS/TMS effectiveness. The programmers continue to work with us on improving the system and integrating its function as an integral component of our developing processes, thus continuing the coevolution of process, people and tools.

We are just getting started, but already see improved results in service delivery and support to our fleet customers. We recognize that a better way of doing business exists for delivering and supporting IT services, and we have adopted ITIL as the model framework for Navy ITSM.

RNOSC West leading chief petty officer IT1 Jason Krahmer, the primary developer and trainer for ITIL at RNOSC West, with ITC(SW/AW) Terry Scydick.

An early champion for ITIL, RNOSC West leading chief petty officer for ITIL development, IT1 Jason Krahmer said, "The good thing about the ENMS system is that it incorporates industry best practices for IT service management. We can capture information in real time, search that information on demand, and build a dynamic knowledge base that inherently focuses on those areas where we can improve most.

"We're also able to visualize data from a myriad of perspectives, providing performance trends of not only the technology that we manage, but the processes that guide our operations as well. The traditional COMSPOT method of reporting service interruptions simply cannot do this.

"Moreover, the system promises to move NCTAMS out of its backroom IT role to play a larger role in supporting command and control by providing a real-time NetCOP to operational commanders based on primary source data vice secondhand message traffic. This shift is perhaps the most exciting thing I've been involved with to date."

Based on our positive experience, we recommend the initiation of an ITSM community of practice on NKO to encourage participation and information sharing about ITIL techniques and successes. We think that the potential for improvements in IT support and delivery to the fleet is enormous.

ITIL has transformed IT service management throughout industry and was adopted by the Defense Information Systems Agency as the NetOps process framework. It is becoming the standard to which we will hold the acquisition and engineering communities, as well as network service providers, for effective network management including the Navy Marine Corps Intranet (NMCI), ONE-NET and the Next Generation Network (NGEN).

ITIL is a comprehensive framework of disciplined and continuously improved processes. Should we empower our own Navy IT and IP workforce with anything less?

Lt. Cmdr. Dave Purkiss was the NCTAMS PAC communications officer until July 2008. He just reported to NETWARCOM's readiness directorate.

CHIPS

"We Will Never Forget"

Pentagon Memorial opens on 7th anniversary of 9/11 attacks

By Christy Crimmins

On Sept. 11, 2008, an estimated 16,000 people gathered to dedicate the Pentagon Memorial. Those in attendance included family, friends and colleagues of the victims of the attack on the Pentagon, as well as military and civilian dignitaries.

"From this time forward, the Pentagon will be more than a symbol of government, more than the seat of military power. It is also a place of remembrance," said Secretary of Defense Robert Gates in his remarks. Remembrance and solace were themes for the ceremony.

Attendees were greeted by a "Healing Field" of nearly 3,000 flags as they entered the ceremony grounds, representing the victims from the World Trade Center, Pentagon and Shanksville, Pa., attacks. One hundred and eighty-four of the flags bore blue ribbons and the names of the victims from the Pentagon and American Airlines Flight 77.

The event began with a prelude concert featuring the U.S. Air Force Band and Singing Sergeants, U.S. Army Chorus, U.S. Naval Academy Chorus and the J.W. Alvey Elementary School Singing Sunrays.

Deputy Secretary of Defense Gordon England opened the dedication ceremony with remarks, followed by a reading of the names of those who died at the Pentagon and on Flight 77. The reading paused at 8:47 a.m., the time that the first plane hit the World Trade Center's North Tower, to observe a nationwide moment of silence.

A wreath was laid at the entrance of the memorial as a bugler played taps from the roof of the Pentagon above a flag hung in the same place rescue workers hung one seven years ago. Another moment of silence was observed in honor of the victims of the Pentagon attack.

Remarks were offered by James J. Laychak, chairman of the board for the Pentagon Memorial Fund, who lost his younger brother David W. Laychak in the deadly attack on the Pentagon.

President Bush officially dedicated the memorial, saying, "The day will come when most Americans have no living memory of the events of September the 11th. When they visit this memorial, they will learn that the 21st century began with a great struggle between the forces of freedom and the forces of terror. They will learn that this generation of Americans met its duty. We did not tire, we did not falter, and we did not fail."

The memorial, located on the southwest corner of the Pentagon, covers almost two acres, and is comprised of 184 cantilevered benches of steel and granite. The benches are laid out in a timeline from the youngest victim, three-year-old Dana Falkenberg to the oldest, John D. Yamnicky, 71. The 59 benches representing the passengers on Flight 77 are placed so that visitors reading the names will face the sky. Visitors reading the names of the 125 victims from the Pentagon will face the building.

The Sept. 11, 2008 dawn breaks over the new Pentagon Memorial to be dedicated in a ceremony attended by President George W. Bush, Vice President Dick Cheney, Secretary of Defense Robert M. Gates and Former Secretary of Defense Donald H. Rumsfeld, as well as the senior leadership of the armed forces. The memorial, the first of three national memorials to the 9/11 victims to be completed, contains 184 benches in honor of those who died. DoD photo by R. D. Ward.

The families of the victims had a hand in the memorial's design. Rectangular reflecting pools of water softly glow from beneath each bench inscribed with a victim's name. Forty-two of the benches represent U.S. Navy victims from the Pentagon attack. Approximately 80 paperback maple trees are scattered between the benches, helping to create a serene, park-like atmosphere.

"A memorial can never replace what those of you mourning a loved one have lost," Bush said, "We pray that you will find some comfort amid the peace of these grounds. We pray that you will find strength in knowing that our nation will always grieve with you."

The memorial will be open 24 hours a day, seven days a week.

Christy Crimmins provides communications support to the Department of the Navy Chief Information Officer.

CHIPS

SPAWAR SYSTEMS CENTERS ATLANTIC AND PACIFIC

It's a great Navy day!

SSC Atlantic Commissioned in Charleston, Norfolk, New Orleans

A new command, Space and Naval Warfare (SPAWAR) Systems Center Atlantic, was commissioned during ceremonies Sept. 29 in Charleston, S.C., Norfolk, Va., and New Orleans, La. The event marks a red-letter date in the history of the Space and Naval Warfare Systems Command, as its echelon III organizations were consolidated into two commands: SPAWAR Systems Centers Atlantic and Pacific.

Under the command of Capt. Bruce Urbon, SSC Atlantic includes the former SSC Charleston, SSC Norfolk and SSC New Orleans, along with SPAWAR sites in Washington, D.C., Pensacola and Tampa, Fla., and strategic satellite offices in Europe, the Middle East and Antarctica.

SSC Atlantic also incorporates approximately 48 civilian employees of the disestablished SSC San Diego who work in the Tidewater, Va., area to support the Atlantic Fleet. The newly formed SSC Atlantic has more than 3,000 government employees, 129 military personnel and significant industry partnerships.

SPAWAR Systems Center Atlantic develops, acquires, and provides life cycle support for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems, information technology (IT), and space capabilities. The total obligation authority for SSC Atlantic is more than $4 billion.

The commander of SPAWAR, Rear Adm. Michael Bachmann, addressed the consolidating Atlantic sites via video teleconference during the Monday ceremony.

"We are executing the BRAC law, as mandated by Congress back in 2005. The result will be an organizational structure that's more capable and more efficient, an organizational structure better able to serve the needs of our customers, and an organizational structure that helps us in our quest to move to a Competency Aligned Organization (CAO).

"But the second, and even more important reason, is that it's the right thing to do. Streamlining brings the organization together … a new name for a stronger organization. Providing more continuity enables us to deliver superior products and superior services — on time and on budget. It's good for our people… good for our organization… and good for our nation," Bachmann said.

SPAWAR Systems Center Atlantic Technical Director Phillip Charles, SSC Atlantic Commanding Officer Capt. Bruce Urbon and Capt. James C. Fox, former commanding officer of the disestablished SSC Norfolk, and now executive officer for SSC Atlantic.

SSC Atlantic, headquartered in Charleston, S.C., has a combined workforce of 129 military members, more than 3,000 civilian employees and significant industry partnerships.

"... We are in the 'freedom business.'"

SSC Atlantic Commanding Officer Capt. Bruce Urbon

Urbon, who served as commanding officer of SSC Charleston, said that the competencies and process capabilities of the individual sites are united as never before under SPAWAR Systems Center Atlantic.

"Our collective sights are set on the critical mission of delivering secure, integrated, and innovative solutions that are ready-for-tasking by naval and joint warfighters," Urbon said.

"Today is a pivot point in the history of SPAWAR Systems Command," he continued. "Today, we are recognizing the proven strength of the past as we create this command anew. In so doing, we are moving a key step forward. We are harnessing our individual strengths into a united, coherent Atlantic force. Indeed, today we're mapping out a new mission for this new command — a mission to realize our full potential together."

The consolidation across Team SPAWAR establishes one organization with competencies located in various geographic areas under one command. This allows the team to work more closely and efficiently toward the common goal of warfighter and customer support.

For more than a year, Team SPAWAR has been migrating to a CAO model which redirects it from a traditional vertical organization to a network of teams located across the enterprise. These teams draw together expertise from various areas (competencies) to deliver products and services to customers. The CAO model allows SSC Atlantic to apply resources in a more targeted, evidence-based and cost-effective manner, creating an improved operational culture for employees and customers.

"The bottom line is this: We are in the 'freedom business,'" Urbon told the crowd. "Our business line demands our uninterrupted vigilance, adaptive response and engineering excellence.

"SSC Atlantic has brought all hands on deck, 24/7/365, serving around the world to connect our team competencies and the power of our partnerships to support the warfighter."

SSC Atlantic is a leading-edge Navy engineering center that designs, builds, tests, fields and supports many of the finest frontline C4ISR systems in use today, and those being planned for the future. SSC Atlantic headquarters is located in Charleston, S.C. Visit http://enterprise.spawar.navy.mil for more information about SSC Atlantic and SPAWAR. CHIPS

SPAWAR marks integration of 10,000th MRAP armored vehicle

By Susan Piedfort

In a ceremony in August, Space and Naval Warfare Systems Center (SSC) Charleston, now realigned under SSC Atlantic, celebrated the integration of the 10,000th Mine Resistant Ambush Protected vehicle at its location on Naval Weapons Station, Charleston, S.C.

MRAP vehicles are outfitted with a full complement of command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) systems installed by Charleston employees.

MRAP armored vehicles have been the Defense Department's top acquisition priority for months because they are proven lifesavers for warfighters on the ground in Iraq and Afghanistan.

MRAPs boast a V-shaped hull that deflects bomb blasts and protects troops inside better than other military combat vehicles, especially from the deadly effects of improvised explosive devices.

Four Soldiers, who have used MRAP vehicles in Iraq, spoke to more than 400 Charleston employees, industry partners and leaders from related commands involved in the integration effort. Private First Class Rusty Davis, Specialists Raymond Rodriguez and Richard Montano, and Sgt. Johnny Simmons spoke to the assembled crowd.

"It is an honor for us to be here and to meet you," Davis said. Because of you, the four of us are able to stand here. Six months ago in Iraq, we had just left to return to the [base.] We were six MRAPs heavy and I was driving one. We started taking indirect fire … small arms fire, mortars and IEDs. No one was injured; not one of us got as much as a scratch or a bruise.

"So many people I have spoken to here this morning have called us 'heroes,'" Davis continued. "I am just glad to have a chance to stand here and tell you that you are our heroes."

"Thank you for being here, and thank you for saving Soldiers' lives," added Rodriguez.

Capt. Bruce Urbon, who inherited the program when he relieved Capt. Red Hoover as SSC Charleston commanding officer in June, noted that Hoover would have been especially happy to see the 10,000th integrated MRAP vehicle roll off the line on Aug. 1.

Army Private First Class Rusty Davis talks about his experience of riding in an MRAP vehicle with his comrades while on dangerous convoy duty in Iraq at the ceremony to celebrate the integration of the C4ISR communications suite for the 10,000th Mine Resistant Ambush Protected (MRAP) vehicle. While Davis and the other Soldiers came under fire none were injured due to the protection of the armored vehicle and its communications suite. Specialists Richard Montano and Raymond Rodriguez with Sgt. Johnny Simmons look on. All photos by Tom Egbert of SSC Atlantic public affairs office.

"In the last year, Secretary of Defense Robert Gates, Secretary of the Navy Donald Winter, Chief of Naval Operations Adm. Gary Roughead and various congressmen, generals and admirals have visited the integration facility to view operations and to thank the integrators for their hard work," Urbon told the assembled team.

"As the Secretary of the Navy said, the patriotism and dedication to task he witnessed here is reminiscent of the effort undertaken just a few miles up the road at the Naval Shipyard more than 65 years ago when we fought a different enemy."

The keynote speaker was Paul Mann of the Marine Corps Systems Command in Quantico, Va. As joint program manager for the MRAP vehicles program, Mann leads the team responsible for procurement, fielding and sustainment of the MRAPs. Noting that he just returned Monday from a trip to Iraq and Afghanistan, Mann stressed the difference these vehicles are making in theater.

"With 7,000 MRAPs in two theaters, I saw your handiwork all over Iraq. Soldiers are leaving their bases in confidence in their MRAPs. It is really making a difference in the battle rhythm," he said.

"These MRAPs are a great tool for commanders and operational planners to get warfighters where they need to be to fight and win."

SSC Atlantic's MRAP integration program is a team effort with the Marine Corps Systems Command; the Defense Contract Management Agency; the U.S. Transportation Command, including the Army Military Surface Deployment and Distribution Command, 841st Transportation Battalion, Charleston Air Force Base, 437th and 315th Airlift Wings' aerial port; Charleston Naval Weapons Station; other systems center sites in San Diego and Norfolk; industry partners; and other DoD partners.

The MRAP family of vehicles provides operational forces with multiple mission-role platforms capable of mitigating IED, underbody mines and small arms fire threats.

The MRAP platforms include a suite of government-furnished equipment

SPAWAR Systems Center Atlantic Commanding Officer Capt. Bruce Urbon speaks to the assembled crowd at the MRAP ceremony. Urbon was also the commanding officer of SSC Charleston before its disestablishment.

to help warfighters be successful on the battlefield. SSC Atlantic oversees the integration and installation work after the vehicles are accepted from the manufacturers.

The MRAP team also performs interoperability testing and hands the vehicles over to USTRANSCOM, which orchestrates transportation of the vehicles from South Carolina to the Middle East.

The MRAP integration program went from inception to full rate production in a little over a year. What started out as just a few vehicle deliveries from manufacturers to SSC Atlantic's integration facility grew to more than 1,200 in subsequent months.

Initially integrating about five vehicles a day, the team ramped up to full rate production of 50 vehicles per day by early December 2007.

Since then the team has sustained that rate, and completed as many as 69 MRAPs in a single day.

By early May this year, they had integrated more than 7,000 MRAP vehicles. The 10,000th MRAP was integrated at the facility Aug. 1, 2008.

For more information, visit http://enterprise.spawar.navy.mil.

CHIPS

SSC Pacific's Josh Caplan Receives "Rising Star" Award

Young computer specialist stands out among his peers

Josh Caplan, an employee in the Space and Naval Warfare Systems Center Pacific's information technology engineering branch is a recipient of Government Computer News 2008 Rising Star Award.

The award recognizes young people in the government information technology community who have made a difference in their fields within the past 18 months. The award's goal is to highlight individuals with potential to contribute to the government for years to come, making them true rising stars.

Caplan is a Navy civilian computer scientist with strong technical skills in the fields of information assurance and IT. He was hired in August 2007 through SSC Pacific's New Professional program, a two-year career development program designed to provide continuing leadership and technical training to new employees, while offering an advanced promotion opportunity.

Although he has only been at SSC Pacific for one year, Caplan has already completed all required training and fulfilled all elements of the program. He is currently project manager for a Defense Advanced Research Projects Agency program focused on technology transition.

Caplan assumed multiple leadership roles and participated in center-wide initiatives, which have made him stand out among his peers. He was elected to the New Professional steering committee, the primary liaison between new professionals and senior management, after only two months on the job. He has been actively involved in center-wide process improvement endeavors, and is a member of a Lean Six Sigma team focused on improving SSC Pacific's hiring process.

Caplan is also engaged in community outreach efforts designed to inform the public about work conducted by SSC Pacific, and he participates in recruiting efforts.

Caplan has positively contributed to the federal IT community by attending cross-sector collaborative events to develop new business with government and industry partners. He helped organize the inaugural Defense Systems IA Seminar in San Diego, and he supports the American Council for Technology's Industry Advisory Council, which seeks to develop public-private cooperation in IT endeavors with the goal of improving the government's ability to serve the nation.

Caplan also serves as the SSC Pacific agency official for the Federal Cyber Service: Scholarship for Service program which is designed to increase and strengthen the cadre of federal IA professionals that protect the government's critical information infrastructure. Caplan was a SFS recipient himself.

"I am honored to have been selected for this award, and I am excited to represent SSC Pacific," Caplan said.

CHIPS

SPAWAR Systems Center New Orleans Joins SSC Atlantic

SPAWAR celebrates merger of the systems centers

By Maria L. Tolleson

The realignment of the Space and Naval Warfare Systems Center New Orleans involves more than just a name change. It means increased economic development, high-tech jobs, and a more stable future for the Navy's information technology hub on the south shore of New Orleans' Lake Ponchartrain.

SSC New Orleans, the anchor tenant at the University of New Orleans Research and Technology Park, merged with SSC Charleston and SSC Norfolk to become SPAWAR Systems Center Atlantic.

In a ceremony held at the facility Sept. 29, the outgoing commanding officer Capt. Mark Krause disestablished the New Orleans organization before an audience of employees, media and invited guests.

Krause addressed the New Orleans workforce during his portion of the SSC Atlantic commissioning ceremony video teleconference. He spoke about the opportunities that the merger with SSC Charleston and Norfolk will have for the New Orleans-based organization and about the skills and talents that the workforce brings to the table. Krause will serve as the SSC Atlantic Chief of Staff until his retirement in the spring of 2009.

The commanding officer of SSC Atlantic, Capt. Bruce Urbon, will reside at the headquarters based in Charleston, S.C. The New Orleans office will be led by Jackie Goff, the SSC Atlantic deputy technical director serving as the liaison between the New Orleans office and the SSC Atlantic headquarters.

With the merger, the New Orleans office will collaborate with SSC Atlantic to work on technology-based projects for the U.S. Navy, Marine Corps, Army, Air Force, Department of Homeland Security and the Department of Veterans Affairs.

With the continued success of SSC Atlantic guaranteed, the number of jobs is expected to increase in the New Orleans office, currently at 435 employees.

The New Orleans staff will collaborate with personnel from Norfolk and Charleston on the VA's high profile Chapter 33 project to accommodate increased educational benefits under the newly signed GI Bill.

The VA work performed in New Orleans "will be a great improvement to our veterans' education benefits and medical services. We are joining forces with our local universities and industry partners to identify the talent levels we will need to support our high-tech expansion," said Lt. Chris Galliano, the New Orleans director of corporate operations.

The main pillar of New Orleans' success is in the cutting edge shared services virtual computer hosting environment which has seen major growth since its post-Katrina rebuild.

The New Orleans office is also a government lead in data integration and service oriented architecture and boasts the largest quality of life customer support center help desk in the Navy serving more than 538,000 active and Reserve members on pay and personnel issues, and other quality of life programs. CHIPS

The Navy Band plays at the SSC Atlantic commissioning ceremony in New Orleans.

Capt. Mark Krause addresses the New Orleans workforce during his portion of the SSC Atlantic commissioning ceremony. Krause will serve as the SSC Atlantic Chief of Staff until his retirement in the spring of 2009.

Ms. Jackie Goff, deputy technical director for SSC Atlantic, and SPAWAR Vice Commander Rear Adm. Charles "Grunt" Smith share a laugh at the New Orleans reception to celebrate the stand up of SSC Atlantic Sept. 29, 2008.

Welcome to SSC Atlantic's New Orleans Office

Through organizational changes, hurricanes and tough challenges, New Orleans staff remain focused on Navy mission

By Maria L. Tolleson

Navy history buffs may find the legacy of the Space and Naval Warfare Systems Center Atlantic's New Orleans office interesting, but others may be more impressed with its unbeatable spirit and ingenuity.

SSC Atlantic's New Orleans office is located on the campus of the University of New Orleans Research and Technology Park. The office includes a workforce of about 435 full-time military, government and contractor personnel who provide information technology capability, decision support and accurate data to Navy, Defense Department and other government agencies.

The genesis of the New Orleans command began in 1986 when Commander, Navy Reserve Force (COMNAVRESFOR) established an Information Systems Office. In 1995, this office was officially designated as the Naval Reserve Information Systems Office (NAVRESINFOSYSOFF). It became the central design agency (CDA) for Navy Reserve manpower, personnel and training systems.

In 1997, due to its excellent record of customer service and rapid deployment of systems, NAVRESINFOSYSOFF was also designated the CDA for many active Navy manpower and personnel systems and assumed responsibility for managing dozens of Navy legacy programs.

In 1997, the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)) designated COMNAVRESFOR as the Systems Executive Office for Manpower and Personnel (SEO-MP), with assigned responsibility for acquisition and program management of all Navy manpower and personnel information resources, as well as designated DoD personnel and pay systems.

Collocated at the Naval Support Activity in New Orleans, NAVRESINFOSYSOFF worked closely with the SEO-MP staff, providing technical expertise, systems engineering and systems operation and maintenance.

Because critical Navy work performed in New Orleans continued to increase, federal, state and local officials obtained approval from the Navy to partner with the local academic community and private industry to establish an Information Technology Center in the University of New Orleans Research and Technology Park. Groundbreaking ceremonies were held in 1998, and NAVRESINFOSYSOFF and SEO-MP personnel began moving into the center in 1999.

In 2000, Navy officials decided the Information Technology Center would best serve the needs of the entire Navy by migrating from a Navy Reserve-aligned organization to the SPAWAR claimancy. In November 2000, NAVRESINFOSYSOFF officially became the SPAWAR Information Technology Center and both SEO-MP and NAVRESINFOSYSOFF were disestablished.

Then, in November 2004, the SPAWAR Information Technology Center was renamed SSC New Orleans to better reflect its alignment within SPAWAR.

In October 2008, due to the Defense Base Closure and Realignment legislation, SPAWAR realigned its field activities into SPAWAR Systems Center Atlantic and SPAWAR Systems Center Pacific. In the realignment, the former SSC New Orleans was consolidated with the field activities at SSC Norfolk and SSC Charleston to become part of SSC Atlantic.

The New Orleans Office has three core capabilities: systems engineering, shared services and a Customer Support Center. Disciplined systems engineering efforts ensure experienced, competency-based software engineering focused on the customer and backed by demonstrated success in meeting cost, schedule and performance requirements. Complete life cycle management is provided — from requirements and design — to delivery and maintenance.

New Orleans adheres to engineering best practices and is assessed at Capability Maturity Model for Software Level 2. Work continues toward Capability Maturity Model Integration Level 4.

Additionally, Lean Six Sigma practices are embedded in all organizational processes.

The New Orleans office offers a fully integrated state-of-the-art application hosting environment, rigorous security policies and standards, redundant and high bandwidth data paths and continuity of operations plan (COOP) failover protection for robust and reliable shared services.

The Customer Support Center's Help Desk is the largest Global Distance Support Center in the Navy, serving 538,000 active and Reserve members on pay and personnel issues. This centralized call-in facility operates 24 hours a day, 7 days a week and boasts a 97 percent customer satisfaction rate.

The former commanding officer of SSC New Orleans, and now chief of staff for SSC Atlantic, Capt. Mark Krause, with the deputy technical director for SSC Altantic and liaison between SSC Atlantic headquarters and the New Orleans office, Ms. Jackie Goff. Krause took command of the facility post-Hurricane Katrina in 2006.

The New Orleans office provides a myriad of IT products and services that include: software engineering; software application development; systems migration; systems integration; systems maintenance; Navy Marine Corps Intranet-approved shared services; security accreditation; and help desk and data operations center monitoring.

SSC Atlantic's New Orleans office is located on the campus of the University of New Orleans Research and Technology Park. The office includes a workforce of about 435 full-time military, government and contractor personnel who provide information technology capability, decision support and accurate data to Navy, Defense Department and other government agencies.

Navy history buffs may find the legacy of the SSC Atlantic's New Orleans office interesting, but others may be more impressed with its unbeatable spirit and ingenuity …

Perhaps one of the greatest examples of the hardy resilience and resourcefulness of the New Orleans staff occurred in the aftermath of Hurricane Katrina.

Although the facility itself was not flooded, as a result of a nearby levee breach, the buildings suffered extensive roof damage, which allowed rainwater to get inside the walls of the building causing widespread mold and water damage.

By implementing its COOP, which allowed operations to continue at alternate sites, work continued at full speed and many employees assumed tasks outside of their normal functions to continue to maintain critical Navy pay and personnel systems.

Even though the majority of the workforce sustained personal loss and severe damage to their homes, operations continued, and in the weeks and months that followed Katrina, many employees had to deal with hardships and attempt home repairs from hundreds of miles away because they were still displaced.

Relocated personnel worked at alternate work sites at Naval Air Station Joint Reserve Base Forth Worth, Texas, Naval Education and Training Command, NAS Pensacola, Fla., and Millington, Tenn. Others telecommuted from the greater New Orleans area and Washington, D.C.

Yet, in those first bleak weeks in September 2005, the single-minded goal of the command's leadership was to return the workforce to New Orleans, and they did just that.

In July 2006, 11 months after Katrina hit, New Orleans employees were able to return to a newly renovated facility, thus demonstrating extraordinary professionalism and initiative in an environment of enduring hardship and devastation.

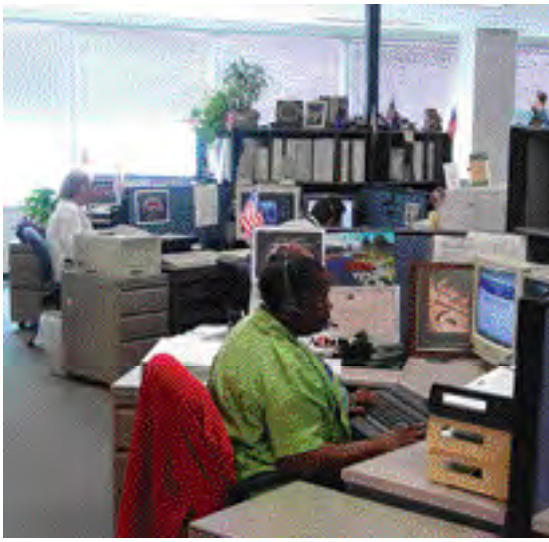
Among the New Orleans office customers are the U.S. Navy and Navy Reserve, U.S. Marine Corps and Marine Corps Reserve, Air National Guard, Department of Homeland Security and the Department of Veterans Affairs.

The former commanding officer of SSC New Orleans, who is now the chief of staff for SSC Atlantic's New Orleans office is Capt. Mark Krause who took command of the facility post-Hurricane Katrina in 2006. The senior civilian liaison to SSC Atlantic headquarters is Ms. Jackie Goff, who is also the deputy technical director for SSC Atlantic.

Maria L. Tolleson is the public affairs officer for SSC Atlantic's New Orleans office.

CHIPS

The main pillar of New Orleans' success is in the cutting-edge shared services virtual computer hosting environment which has seen major growth since its post-Katrina rebuild.



Among the New Orleans office customers are the U.S. Navy and Navy Reserve, U.S. Marine Corps and Marine Corps Reserve, Air National Guard, Department of Homeland Security and the Department of Veterans Affairs.

SSC Atlantic sites partner to provide services to VA

Modernizing legacy systems for an enterprise approach to delivering veterans benefits and services

By Maria L. Tolleson

The Space and Naval Warfare Systems Center Atlantic's New Orleans office, in partnership with SSC Atlantic's Charleston office, will be providing assistance to the Department of Veterans Affairs.

This new business initiative comes as a result of the Health Systems Mission Area Team (HS MAT), a collaborative effort between SSC Atlantic's New Orleans, Charleston and Norfolk sites.

The HS MAT is an example of a successful partnership between the former system centers that realigned Oct. 1 under SSC Atlantic as a result of the 2005 Defense Base Closure and Realignment law.

The HS MAT team combines the common interests of SPAWAR managers and their health systems customers in the areas of information technology; network systems and software engineering; information assurance; software development; and the communication infrastructure domains.

These common interests include: enabling technologies; policy and regulations review and formulation; enterprise architectures; privacy and security practices; technical implementation issues; enterprise program management; and end-user requirements validation.

The Department of Veterans Affairs includes three administrations that provide the delivery of veterans services and benefits: Veterans Health Administration (VHA), Veterans Benefits Administration (VBA) and National Cemetery Administration. The New Orleans office will be providing support to the VHA and VBA. Support for the VHA will be provided by Jodi Ketry and Gregg Travis.

The command will be assisting the VA's Office of Enterprise Development with information management/information technology project management and technical support for the scheduling and common services projects. This support will include performance engineering, system administration, software quality assurance, technical writing and testing.

The replacement scheduling application (RSA) will replace a legacy scheduling application that is based on care concepts that are 25 years-old. The goal for the RSA project is to deploy an enterprise-level scheduling application to support the view of a "One-VA patient record," regardless of point of care. A tiger team will be formed to address critical defects with the RSA.

The Common Services Identity Management (CS/IdMS) program manages the identity of persons and organizations for the VA.

As the VA moves toward seamless veteran care, its ability to effectively maintain and share unique identifiers across an enterprise will improve healthcare delivery and data, as well as eliminate inappropriate merges of patient data.

CS/IdMS is comprised of organization services and person-centered services and peripheral applications and services. The New Orleans office will provide project management for both the organization and person services projects.

Beginning in fiscal year 2009, all contractor support for person services, organization services and the master patient index will be provided through a contractor workforce of approximately 40 to 50 people centered at the New Orleans office.

The Nationwide Health Information Network is the critical portion of the health IT agenda intended to provide a secure, nationwide, interoperable health information infrastructure that will connect providers, consumers and others involved in supporting health and healthcare.

The New Orleans office will provide project management for the NHIN, as well as project support in a variety of other areas. The NHIN will enable health information to follow the consumer, be available for clinical decision making, and support appropriate use of healthcare information beyond direct patient care so as to improve health.

The NHIN is designed as a "network of networks," built out of state and regional health information exchanges (HIEs) and other networks to support the exchange of health information by connecting these networks and the systems they, in turn, connect.

The New Orleans office will provide support for integration efforts performed by the VA to consolidate and modernize legacy systems within the Veterans Benefits Administration. Under this umbrella, Lucy Colangione will spearhead support to the VBA specifically for the Benefits Delivery Network.

The BDN is the legacy system em-

The HS MAT is an example of a successful partnership between the former system centers that realigned Oct. 1 under SSC Atlantic ...

ployed by the Veterans Benefits Administration to process entitlements for three of its five business lines: Compensation and Pension, Education, Vocational Rehabilitation and Employment.

The primary services of the BDN are: receipt, processing, tracking and disposition of veterans applications for benefits; requests for assistance and general administration of legislated benefit programs.

The compensation program provides monthly payments and ancillary benefits to veterans in recognition of the loss of earning capacity caused by a disability or disease incurred in or aggravated during military service.

The pension program provides monthly payments to wartime veterans who are permanently and totally disabled as a result of a disability not related to military service.

The educational assistance benefit provides opportunities for higher education and restores lost educational opportunities and vocational readjustment.

The Vocational Rehabilitation and Employment program helps service-disabled veterans achieve independent life skills and employment. This program provides service to enable veterans, with service-connected disabilities, achieve independence in daily living, become employable and obtain and maintain suitable employment.

The Benefits Delivery Network provides interface to the Veterans Benefits Administration's other benefits delivery systems such as the VBA Office of Information Management.

The scope of the work will include engineering services associated with the BDN documentation support project providing resources and labor to document the BDN application suite.

This effort will consist of four phases: discovery, application documentation, process documentation and standard procedures documentation.

The work will include:

• Establishing a thorough requirements baseline for the interfaces into and out of the Benefits Delivery Network application suite resident on the mainframe, as well as the applications and processes (jobs/batches) running in support of the BDN application suite.

• Documenting the functionality, configuration and external communications related to the Benefits Delivery Network application to include interfaces and module relationships.

• Documenting the various applications/batch processes of the Benefits Delivery Network application suite.

• Documenting the standard operating procedures in use by support staff of the Benefits Delivery Network application suite.

The work, which actually involves 15 projects, will be performed at various SPAWAR offices, VA headquarters in Washington D.C., and other VA activities worldwide.

Maria L. Tolleson is the public affairs officer for SSC Atlantic's New Orleans office.

CHIPS

The business initiative for the Veteran's Administration will improve VA nationwide healthcare networks with secure and interoperable connectivity for delivery of veterans services ...

Gregg Travis

Jodi Ketry

Lucy Colangione

Presenting SSC Pacific: A new name for a stronger organization

The Space and Naval Warfare Systems Center San Diego officially changed its name to SSC Pacific in a ceremony held Sept. 29 in front of its main administration building on Naval Base Point Loma in San Diego. During the ceremony, Commanding Officer, Capt. Mark T. Kohlheim, and Technical Director, Ms. Carmela Keeney unveiled the new sign and logo.

The ceremony, which featured the Navy Band and the formal unfurling of the command flag, included a message by SPAWAR Commander Rear Adm. Michael Bachmann via live video. Other speakers included SPAWAR Deputy Commander Mr. Rod Smith, Cmdr. Boyd Zbinden, commanding officer of the Navy Center for Tactical Systems Interoperability (NCTSI) San Diego, and Cmdr. Baron Jolie, officer in charge of the SSC Norfolk detachment in San Diego.

The 2005 Base Realignment and Closure law directed the realignment and consolidation of SPAWAR claimancy echelon III organizations into two commands, SSC Atlantic and SSC Pacific. Under this realignment, SSC San Diego, not only had a name change, but was augmented with personnel from the SSC Norfolk detachment in San Diego and NCTSI San Diego. Both organizations were designated for disestablishment under BRAC 2005, with their mission and functions consolidated into SSC Pacific.

A small number of SSC San Diego's current surface and subsurface sensor projects have been realigned to Naval Surface Warfare Center Dahlgren, Va., and Naval Undersea Warfare Center in Newport, R.I.

"The resident genius of our workforce will have an increased role, along with Team SPAWAR's organizational alignments. We will remain the strategic advantage for warfighters and decision makers alike."

Capt. Mark Kohlheim
Commanding Officer SSC Pacific

SSC San Diego has been providing state-of-the-art command and control, communications and surveillance technology to the nation's military from its Point Loma location since 1940. The center manages more than 1,000 programs that develop and deploy capabilities to collect, process, display and transfer information critical to mission performance.

NCTSI San Diego has provided standards management and interoperability certification testing for tactical data systems for the Navy and joint communities since 1977.

SSC Norfolk Det San Diego has been one of SSC San Diego's partners in deploying worldwide, critical network applications to the fleet for both afloat and ashore systems.

With the combined capabilities of SSC San Diego, NCTSI San Diego and SSC Norfolk Det San Diego, SSC Pacific looks forward to making even greater contributions to the fleet.

Ed Budzyna is SSC Pacific's deputy public affairs officer.

Capt. Mark Kohlheim, commanding officer of SSC Pacific, with Carmela Keeney, technical director for SSC Pacific. Middle, the ceremony for the stand up of SSC Pacific on beautiful Point Loma, San Diego, Calif. Bottom, principal participants include: Carmela Keeney; SPAWAR Deputy Commander Rod Smith; Capt. Mark Kohlheim; Cmdr. Boyd Zbinden, commanding officer, NCTSI San Diego; Cmdr. Baron Jolie, officer in charge, SSC Norfolk Det San Diego; and Lt. Cmdr. Timothy Gordish, chaplain.

SSC Pacific Unveils Robotic Command and Control Breakthrough

New control paradigm significantly improves the functionality of robotic systems on the battlefield ...

By Ann Dakis

Space and Naval Warfare Systems Center Pacific's unmanned systems branch recently demonstrated a revolutionary new approach to robotic command and control that allows a warfighter and robot to synergistically interact, much like a canine team. The result is a significant reduction in the control burden associated with operating current robotic systems, which opens up a wide variety of new applications previously viewed as impractical.

Current man-portable robotic systems are too heavy for troops to pack during extended missions in rugged terrain and typically require more user support than can be justified by their limited return in force multiplication or improved effectiveness. As a consequence, today's systems appear organically attractive only in life-threatening scenarios, such as detection of chemical/biological/radiation hazards, mines or improvised explosive devices.

But SSC Pacific engineers are working to significantly increase robotic functionality to enable robotic systems to perform useful tasks and improve their autonomy. The underlying objective of this development is to eliminate the need for expensive, bulky robot-specific operator control units, and rely instead on emerging technology that will include markedly improved perception and reasoning algorithms on the robots themselves.

According to Bart Everett, chief engineer for robotics in SSC Pacific's advanced systems division, the path forward to this remarkable achievement was fairly long and difficult.

In April 2002, the very first man-portable robots deployed during Operation Enduring Freedom were provided by SSC Pacific in support of Navy Explosive Ordnance Disposal (EOD) Mobile Unit 3. SSC Pacific later played a key role in the large-scale fielding of such systems in February 2004, helping to procure 167 commercial EOD robots from seven different vendors. The number of robots employed in Iraq and Afghanistan today is estimated at 6,000, and the subsequent saving of countless lives has generated widespread user acceptance.

Everett often points out that the use of unmanned systems on the battlefield is not as revolutionary as one might think.

"What most people don't realize is that there were more robots used during World War II than we have in theater today across the operational domains of air, land and sea. Even more telling, ground vehicle technology has not really changed all that much in the past 65 years, in that our currently fielded systems are still tele-operated, remotely driven by a human operator," Everett said.

From a command and control perspective, however, there are a number of problems associated with tele-operation on the battlefield. Foremost among these is the need for a high-bandwidth line-of-sight radio frequency link for passing real-time video back to the operator which severely limits the achievable standoff. When communications are lost due to signal occlusion or multi-path interference, the mission is essentially over and, in some cases, it might not even be possible to recover the robot.

Second, operators may become so immersed in driving the robot that their situational awareness may diminish, much like a child engrossed in a video game, which can be extremely dangerous under hostile battlefield conditions.

"In a nutshell, today's warfighter considers the robot a major asset since it saves lives, but the associated operator control unit is viewed as a liability because it's heavy, awkward and very labor intensive [to operate]," Everett said. "Our approach has been to make the robot more functional and intelligent, so it becomes an even greater asset, while at the same time reducing the frustration associated with command and control."

In 1991, the unmanned systems branch took the first step toward easing the driving burden with the introduction of a new control paradigm known as "reflexive tele-operation." The operator steers the robot remotely using a joystick or steering wheel, but onboard sensors automatically detect and avoid any perceived obstacles in the robot's path.

An analogy, Everett said, would be like riding a horse versus riding a motorcycle. "Point a motorcycle at a tree and you're going to hit the tree, whereas a horse will change course to avoid impact."

Gary Gilbreath, an engineer in the unmanned systems branch, holds a joint patent with Everett on the reflexive tele-operation concept, which has since been incorporated into several automotive-size robotic vehicles, including the Army's Mobile Detection Assessment Response System. Size, weight and power

SSC Pacific's ARMS development team, from left, Bart Everett, Estrellina Pacis, Greg Kogut, Gaurav Ahuja, Donnie Fellars and Brandon Sights.

constraints associated with smaller man-portable robots, however, impose significant integration challenges that have only recently been overcome.

The unmanned systems branch is now collaborating with the Army Research Laboratory to make sensor-assisted collision avoidance available as an upgrade to legacy systems in theater. Meanwhile, rapid advancements in the supporting technologies over the last few years have enabled even more intelligent functionality on small robots.

The Autonomous Robotic Mapping System (ARMS), for example, can automatically explore an unknown or hostile environment while building a highly accurate and detailed map and, at the same time, stay precisely referenced within that map. A scanning laser range finder measures distance to all surrounding objects within a 360-degree field of view.

Stereo cameras assist with this three-dimensional mapping. A stereo camera is a type of camera with two or more lenses that can simulate human binocular vision. This provides the ability to capture three-dimensional images. No human guidance is necessary, other than initial high-level direction telling the robot where to search. Better yet, in the event communications with the warfighter are lost, the robot can still complete its search-and-map mission and return to the starting point to upload the results.

The ARMS prototype, which is scheduled for performance evaluation in late 2008 in California, is a significant improvement in human-robot interaction that addresses many of the disadvantages associated with current tele-operated systems. The robotic vehicle now handles all low-level driving and mapping tasks, freeing the warfighter to focus on what is happening in the battlespace.

Yet, while ARMS is clearly a major step in the right direction, project engineers such as SSC Pacific's Brandon Sights feel even more can be done.

"It's great that the robot can now search an unknown area on its own and provide the warfighter a detailed map of the floor plan," Sights said. "But it would be even better if that map were annotated with any items inside that space that were of tactical significance such as trip wires, weapons or human presence."

So with the basic navigation and collision-avoidance problems for the most part solved, the emphasis has now shifted toward development of modular sensor payloads that allow the robot to detect relevant features on the fly. To expedite this process, the unmanned systems branch recently teamed with the Center for Commercialization of Advanced Technology which is funded through the Office of Naval Research.

"Our partnership with CCAT has expedited the maturation of promising capabilities to enhance the robot's environmental awareness," said SSC Pacific's Estrellina Pacis, ARMS project manager.

In 2007, CCAT funded eight ventures, with five more contracts awarded in 2008.

"During this stage we were struck by a rather sobering observation, in that for decades we had been trying to emulate human perception and intelligence on a robot, yet we really had precious little insight into either," Everett said. "I spent about a year reading 30-plus books on both subjects, [and] then restructured our algorithmic approach accordingly."

Engineering students in the field of computer vision, the science and technology of machines that *see*, are generally taught that "vision" solutions must be insensitive to changes in image scale, rotation and intensity.

But this traditional approach makes the perception task unbelievably complex, particularly for the ever-changing visual scenery encountered by a mobile robot. Not surprisingly, robust image processing algorithms have been painfully slow in coming.

"If you think about it, that's not how we humans do it," Everett said. "We don't enter a room and consciously examine every single object in our field of view. Our subconscious perception takes everything in, but only flags those items of known interest to our conscious perception; otherwise we'd be too distracted by the minutia to ever accomplish anything."

Computer vision can also be described as a complement (but not necessarily the opposite) of biological vision. In emulating biological vision, the visual perception of humans and various animals are studied, which results in models of how these systems operate in terms of physiological processes.

Top, controls engineer Brandon Sights follows the ARMS robot as it autonomously enters and maps a building. In the photo below, the ARMS prototype, based on iRobot's PackBot, automatically assumes a defensive screening maneuver between Sights and the perceived threat.

Using a biological model on the robot, the scanning laser is the analogy to subconscious perception, precisely surveying the robot's surroundings to build a map and keep the system geographically referenced. The robot's video camera can then be cued to "consciously" investigate any anomalies detected by the laser such as an opening in a nearby wall. Is it a doorway, a window, bomb damage?

Greg Kogut, SSC Pacific unmanned systems branch's vision expert, summed up the vision concept: "Instead of constantly trying to classify everything in the scene across an infinite spectrum of possibilities, vision is now given discrete tasks bounded in terms of both scope and location. The results have been quite impressive."

If the vision system identifies a laser-detected wall opening as a doorway, for example, it next looks to either side of that feature to see if there is an associated room sign. If such a sign is found, the camera lens zooms in to read it and links any relevant descriptive information, such as room number, purpose or occupant, along with the "X, Y" coordinates of the door opening. Each of these scripted tasks is both focused in objective and physically constrained to the appropriate portion of the overall field of view, thus significantly reducing complexity.

The robot also *learns* important information about its environment with no human assistance that allows it to later execute high-level voice commands such as "Go to room 102" or "Enter the generator room."

In 2004, the ARMS team presented a landmark paper at the Society of Photo-Optical Instrumentation Engineers Mobile Robots XVII Conference in Philadelphia. *(SPIE is an international membership society, serving scientists and engineers in industry, academia and government. SPIE members work in a wide variety of fields that utilize some aspect of optics and photonics, which is the science and application of light.)*

The concept, presented in the paper, "Towards a Warfighter's Associate: Eliminating the Operator Control Unit," envisions the proximal interaction of a human-robot team, similar to the pairing of police officers and their canine partners in law enforcement.

One of the biggest challenges is finding a robust means of command and control for scenarios where the warfighter and the robot work side by side.

"... we were struck by a rather sobering observation, in that for decades we had been trying to emulate human perception and intelligence on a robot, yet we really had precious little insight into either ... I spent about a year reading 30-plus books on both subjects, [and] then restructured our algorithmic approach accordingly."

– Bart Everett

"In looking back over the past few years, we have progressed from joystick control to mouse control — and now even voice control," explained SSC Pacific's Gaurav Ahuja.

Mr. Ahuja is working with a CCAT awardee, Think-a-Move, Ltd., to integrate Think-a-Move's patented earpiece into the robot's design. The earpiece captures the sound waves created in the ear canal when people speak.

"But if the human-robot team walks into an ambush," Ahuja continued, "even voice control is not good enough. There is no time to talk to a robot in this situation [because] the warfighter must instinctively react to ensure his or her survival."

For the robot to provide any value in this scenario, it must similarly infer what it should do based on what it sees the human doing and the perceived threat level in the surrounding environment.

According to SSC Pacific project engineer Donnie Fellars, "A good analogy here would be a hunter and a bird dog. The dog knows what to do during the hunt by watching the hunter, and changes modes without direction to find the game, point out the game, and then retrieve the game. We want the robot to follow that same model."

"What we're trying to do is give the robot some degree of artificial empathy, which is a tall order," Everett added. "It's hard enough to emulate human behavior, and animals are far more adept at reading body language and judging intent than humans."

To get around this problem, the team tapped information similar to the data collected by the Warfighter Physiological Status Monitor (WPSM) which is being developed under the Army's Future Force Warrior program. WPSM is a wearable physiological sensor suit that monitors body temperature, heart rate, blood pressure, hydration, stress levels and body position. An Airsoft M4 serves as a laboratory surrogate for the Soldier's weapon, instrumented to indicate orientation as well as safety and trigger status. *(Airsoft guns resemble real guns but shoot small plastic BBs.)*

Passing all this valuable information to the robot enables some fairly sophisticated human-robot interaction with no additional control requirements imposed upon the warfighter.

In one potential scenario, for example, the robot automatically follows or precedes a dismounted Soldier using a combination of ultrasonic, laser and video sensors. If the human stops, the robot also halts and begins using its video camera to search for potential threats. Should the warfighter unlock the safety on his or her weapon, the robot redirects its gaze in the direction the weapon is pointing. If a firefight ensues, the robot can reposition itself between the warfighter and the nearest detected threat.

All these supporting behaviors are seamlessly invoked in response to changes associated with the threat environment allowing the human partner to put far more focus on survival. This revolutionary new approach to human-robotic interaction should facilitate a multitude of mission capabilities now considered impractical due to the control burden imposed by current tele-operated systems.

While much work remains to be done before the "Warfighter's Associate" concept is formally vetted for operational use, initial reaction from the user community has been very favorable.

Ann Dakis works in the SSC Pacific public affairs office.

CHIPS

End-to-End Systems Engineering Lab

SSC Pacific opens new lab for C4ISR capabilities

By SSC Pacific Public Affairs

A new End-to-End (E2E) Systems Engineering laboratory, equipped to develop, test and integrate applications and communications systems across multiple platforms, was unveiled at Space and Naval Warfare Systems Center Pacific, (formerly SSC San Diego) Aug. 21, 2008, in San Diego, Calif.

This, and additional labs located at SPAWAR headquarters in San Diego, and SSC Atlantic headquarters in Charleston, S.C., will be linked via common networks, creating a collaborative environment for conducting E2E development and testing of command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) applications and systems.

Chris Miller, who heads the Program Executive Office C4I organization, and Dr. Rich Jaffee, head of the command and control department in SSC Pacific, and project members, were on hand for the dedication ceremony.

PEO C4I and SPAWAR are working toward a shift in strategy as the Department of the Navy moves to service oriented architecture (SOA) and common computing environments which offer enhanced flexiblity and interoperability.

It has become clear that traditional, application-centric development and testing models are not sufficient to support the warfighter in today's dynamic environment. A paradigm shift from traditional systems with dedicated hardware and software to a net-centric, enterprise approach needs to occur so that C4ISR products meet mission and fleet requirements.

PEO C4I developed a strategic plan in September 2007 to ensure its business and technical approaches are more responsive to fleet readiness requirements, and enlisted the support of SSC Pacific and SSC Atlantic to address programmatic, engineering, test and sustainment coordination.

E2E integration, test, certification, and installation design validation are key components supporting the overarching E2E strategy that also includes a collaborative, distributed engineering environment and governance structure.

The labs in San Diego and Charleston will operate at all classification levels and provide shared enterprise resources, including: reference implementations; test fixtures; networks; instrumentation; a test environment with mission scenarios, simulation/stimulation and test control; support services with security, configuration management and engineering support; and test management capabilities.

A core set of C4I application, network and radio frequency systems will be implemented with the ability to connect to other test facilities.

SPAWAR headquarters and SPAWAR Systems Centers Pacific and Atlantic will provide one seamless environment for integrated support and expertise to develop and execute risk mitigation strategies and implement capability acceleration. System of systems capabilities will work together in a collaborative environment to support SOA enterprise development where the "system" is a collection of components and services developed by multiple programs.

Further, developers, testers and users will have access to systems and components without having to procure them by way of a collaborative networking environment. Collaboration will also result in accelerated development. The desired end state will be that technical solutions are designed, developed, tested and delivered through a cost-effective, E2E approach across the PEO portfolio of C4I applications and systems. CHIPS

SAN DIEGO (Aug. 21, 2008) Dr. Rich Jaffee, Chris Miller and Steve Musson cutting the ribbon to the new End-To-End Systems Engineering Lab at SSC Pacific with lab project members. A core set of C4I application, network and radio frequency systems will be implemented that will connect the lab to other test facilities.

Navy's New Broadband Satellite Program Provides Greater Reliability, Tenfold Increase in at-Sea Throughput

By SPAWAR Public Affairs

The Navy has begun procuring the next generation commercial satellite communications terminals to augment its military satellite communications. The procurement is designed to significantly increase throughput to ships at sea. Throughput is the amount of data transferred in a specific amount of time, usually expressed as bits per second.

The Commercial Broadband Satellite Program (CBSP) is sponsored by the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)) and executed by the Communications Program Office within the Navy's Program Executive Office for Command, Control, Communications, Computers and Intelligence (C4I).

The CBSP is a rapid deployment capability (RDC) acquisition to expedite replacement of Inmarsat B high speed data (HSD) channel and Commercial Wideband SATCOM Program (CWSP) capabilities. The current RDC fielding requirement is to install CBSP terminals on up to 49 ships.

Navy ships currently use Inmarsat B HSD (128 kbps) or CWSP (2.048 Mbps). CBSP terminals will be capable of delivering up to a near tenfold increase in throughput from 881 kbps for the small ship variant (SSV)-equipped ships to 21.6 Mbps for the force level variant (FLV)-equipped ships.

Throughput received by individual fleet units will depend on each ship's actual satellite allocation of CBSP bandwidth, which will be procured by PEO C4I in coordination with the Defense Information Systems Agency.

The increased throughput capability will enable ships to transmit voice, video and data faster and in greater volume. Additionally, the quality of life for Sailors will be increased by their ability to communicate using wideband SATCOM.

Chris Miller, who heads PEO C4I, the organization charged with acquiring, installing, and supporting communications and information technology systems for the Navy said, "Our warfighters need the added capability in order to ensure decision superiority — the ability to make informed decisions in critical situations — faster than the enemy."

According to Navy Capt. John W. Pope III, communications program manager, the Navy is acquiring three variants of the commercial terminals, depending on the size and mission of the ship for which it is destined.

"Each terminal variant is capable of receiving differing satellite spectrum bands depending on their use," said Pope. "The SSV is a Ku-band terminal intended for ships operating in littoral waters. The unit level variant (ULV) terminal will be commercial X and Ku capable and will be the size and weight to fit on unit level ships. The FLV terminal will access the C and Ku satellites and will be large enough to provide high data rate to force level ships."

Pope said his program office's goal is to deliver the capability as quickly as possible while balancing cost, schedule and performance, in addition to the challenges inherent in an RDC acquisition.

"This program plays a key role in the Navy's SATCOM roadmap strategy as we consolidate from five SATCOM terminal programs of record to two: CBSP and the Navy Multiband Terminal. This effort should allow the Navy to take advantage of newer technology and reduce overall life cycle costs."

The Navy recently completed a developmental test and quick reaction assessment of the first CBSP terminal, installed aboard the mine countermeasures ship USS Champion (MCM 4), under the command of Navy Lt. Cmdr. John Callaway.

"CBSP SSV is a significant improvement in capability and reliability," said Callaway. "It's the first time I have been able to surf the SIPRNET while at sea."

The increased bandwidth provided by CBSP was welcomed by Information Systems Technician Senior Chief (Surface Warfare) Jim Crewse, USS Champion communications division chief.

"Overall the system has been performing great and had added capability and performance for the ship," explained Crewse.

According to Melinda Ratz, the assistant program manager for CBSP, the Navy's first priority is to install CBSP terminals on the most "bandwidth disadvantaged" users, a group that includes frigates, mine countermeasure ships and coastal patrol ships.

"Additional SSV terminals were ordered after the successful developmental testing and quick reaction assessment aboard USS Champion for installations beginning as early as September," Ratz said.

"ULV terminals are being produced for installation and testing in spring 2009 to ensure the frigates receive this mission essential capability. The next priority will be to install CBSP on force level ships to replace CWSP."

At sea aboard USS Champion (MCM 4) - Sailors aboard the mine countermeasures ship prepare to lower the AN/SLQ-48 "Mine Neutralization Vehicle" into the water. The remotely operated vehicle uses sonar and video cameras to find and identify underwater objects. If the operators find a mine, the vehicle can place small explosive charges near the mine to neutralize it. U.S. Navy photo by Lt. Marc Boyd.

PEO C4I acquires, fields, and supports C4I systems that extend across Navy, joint, and coalition platforms. Supported by Team SPAWAR and industry partners, PEO C4I annually completes more than 2,000 C4I installations to fleet and coalition customers.

For more information about PEO C4I, go to www.peoc4i.navy.mil. CHIPS

SSC Norfolk Workforce Excellence Continues Under SSC Atlantic

By Sharon Anderson

The Space and Naval Warfare Systems Center Norfolk realigned under SSC Atlantic, along with SSC Charleston and SSC New Orleans, in a ceremony marking the occasion Sept. 29, 2008.

The stand up of SSC Atlantic, as a result of the 2005 Base Closure and Realignment law, demonstrated the synergy created by combining the East Coast systems centers into a single provider organization committed to delivering superior C4ISR products to the fleet and warfighter. A similar effort was executed for the West Coast systems center realigned under SSC Pacific.

Capt. James C. Cox, former commanding officer of the disestablished SSC Norfolk at the stand up ceremony for SPAWAR Systems Center Atlantic. Cox is now the executive officer for the newly commissioned SSC Atlantic organization. SSC Atlantic Commanding Officer Capt. Bruce Urbon and SSC Atlantic Technical Director Phillip Charles are shown seated behind Cox.

But the disestablishment of SSC Norfolk was also bittersweet said Capt James C. Cox, who relinquished command of SSC Norfolk at the ceremony. Cox, who is now the executive officer for SSC Atlantic, recalled the many successes of the systems center along with its outstanding military and civilian workforce of about 270 personnel.

SSC Norfolk is noted for its fleet focus and unbeatably engineered products. With more than 2,400 customer organizations and 500,000 application users, SSC Norfolk leadership and personnel continually exceeded customer expectations.

In September 2007, SSC Norfolk received CMMI Maturity Level 3 competency as assessed by the U.S. Air Force Software Technology Support Center. In the same year, SSC Norfolk received the Captain Joan Dooling Award for Information Professional Team of the Year, presented by the Navy Bureau of Medicine and Surgery, for its work on the Theater Medical Information Program-Maritime.

TMIP-M provides clinical data collection and a data transport capability in a combat or hostile environment involving deployed forces. TMIP-M provides improved casualty tracking and patient care and medical supply management. TMIP-M is a component of TMIP, which is a Department of Defense-directed joint program.

SSC Norfolk uses a strong business approach reinforced by the use of the Balanced Scorecard methodology and Lean Six Sigma for project management and continuous process improvement. SSC Norfolk's core competencies include distance and on-site support; help desk; software engineering and database conversion; system installation; verification and validation; and acceptance and certification.

These core competencies aligned within SSC Atlantic will not only increase organizational efficiencies, but will also provide clarity to customers and a refined focus to the SSC Atlantic workforce.

The transition to SSC Atlantic will be seamless to customers, according to Patricia Fuller, who was SSC Norfolk's technical director.

"SSC Atlantic will certainly bring change across our new organization, and we welcome that change. We had pockets of excellence in each of our three systems centers, but it was not easy to transfer that knowledge across the three centers in the past.

"With a single command that is striving for competency alignment and competency maturity, we are certainly set to take the 'best practices' from each of the systems centers and create that knowledge transfer using our competency alignment model as an execution tool.

"Our commitment to our team is that we will do this in an orderly fashion," said Fuller, who is now the deputy technical director, Tidewater, for SSC Atlantic.

The SSC Atlantic ceremony was performed *virtually* linking SPAWAR sites in New Orleans, La., San Diego, Calif., Charleston, S.C., Washington, D.C., and Norfolk, Va. In Norfolk, the event was hosted by Ms. Fuller and Jennifer Watson, head of SSC Charleston's C4ISR/ISE department, who is now the head of the Business Systems/Enterprise Information Services (EIS) department and the national competency lead for Business Systems/EIS under SSC Atlantic. Cmdr. Todd Black, SSC Norfolk's executive officer was the master of ceremonies for the Norfolk site.

Rear Adm. J. Clarke Orzalli, commander of the Regional Maintenance Centers, said he was not surprised by the way SPAWAR chose to conduct the ceremony — via a video teleconference.

"I was impressed with the ceremony because SPAWAR is the owner of all the VTC capability that we have, and it came off without a hitch, which was good. I thought it was very well done when the individual sites were incorporated.

"It's one of the principal interfaces with SPAWAR because of the Regional Maintenance Centers on the waterfront execution of not only modernization upgrades but also technical support issues. I work very closely with the activities, so I felt it impor-

tant to be here to show my support and because of our teamwork. I also know a lot of guys that work at SPAWAR so I am here to support them," Orzalli said.

Invited guests included industry partners, customers, community and Congressional leadership and SPAWAR employees, supporters and friends.

"SPAWAR Systems Center Atlantic is in the ideal position to bring together the superb capabilities of our three systems centers in such a way that we are better connected to the warfighter.

"BRAC is often seen as a negative event; but in this instance, we are seizing the opportunity to create one organization that is stronger, more unified in purpose, better aligned and focused to deliver current and future capabilities," Fuller said.

While speaker comments discussed the distinguished legacy of the former systems centers, the anticipation for SSC Atlantic's stand up was palpable. Jeannie Evans, who represented Virginia Senator Jim Webb, said that she was impressed by the way that SPAWAR embraced the change.

"Consolidation is not always an easy thing. No one likes change, but efficiency in government is very important. What happened today is very exciting. It goes to show that the SPAWAR folks know what they are doing. I think it is rather unique, and I think we are going to see more of this kind of consolidation as our military missions change. Efficiency in government is very important, and Congress is demanding that there be efficiency in government.

"These people in this room and up and down the East Coast, as well as the West Coast, know how to deliver to their customer, and they will continue to do that. The Norfolk presence will still be a very important component no matter where the consolidation takes effect. Obviously, the proximity to the fleet is extremely important because the customer base is here.

"Norfolk will continue to grow, and it will continue to be a very important part, but the consolidation was a necessary thing, and I think peoples' attitudes show that today," Evans said.

Ms. Fuller said she was eager to tap into the expertise afforded by the collective SSC Atlantic organization.

"During the past few years, I've had opportunities to work with some of the bright and dedicated professionals that now make up SSC Atlantic; this is an extraordinarily talented group of people. By uniting this group and creating one command, I believe we are knocking down some of the walls that separated us in the past. We will be able to provide additional opportunities to our team members, and those opportunities will be across our different locations," Fuller said.

"Consolidation is not always an easy thing. No one likes change, but efficiency in government is very important. What happened today is very exciting. It goes to show that the SPAWAR folks know what they are doing ... the consolidation was a necessary thing, and I think peoples' attitudes show that today."

Jeannie Evans
representing Va. Senator Jim Webb

SPAWAR Commander Rear Adm. Michael Bachmann, who addressed the consolidating Atlantic sites via VTC, said the realignment of the systems centers will move SPAWAR closer to a Competency Aligned Organization (CAO) structure and even greater accomplishments as an engineering and acquisition leader.

The realignment of the East and West Coast systems centers is just one of the many improvements in organizational effectiveness that the SPAWAR community has enthusiastically taken on through the years.

"SSC Atlantic has been in the making for two years. I am excited about where we are going and what we can do with this powerful team. This is the beginning of something really wonderful, and I am happy to be a part of this journey," Fuller said.

Visit http://enterprise.spawar.navy.mil for more information about SSC Atlantic and SPAWAR. CHIPS

Jeannie Evans, who represented Virginia Senator Jim Webb, at the SSC Atlantic stand up ceremony with Rear Adm. J. Clarke Orzalli, commander of the Regional Maintenance Centers.

Jennifer Watson, head of the Business Systems/Enterprise Information Services (EIS) department and the national competency lead for Business Systems/EIS for SSC Atlantic with Patricia Fuller, deputy technical director, Tidewater, for SSC Atlantic, hosting the SPAWAR Systems Center Atlantic commissioning ceremony on Naval Station Norfolk, Va. The streamlined SPAWAR Systems Center Atlantic organization will consist of a network of teams organized by competencies that cross organizational and geographical boundaries to deliver superbly engineered and acquired products to the fleet and warfighter.

DON DIACAP Transition

Transitioning from DITSCAP to DIACAP involves much more than policy changes; it requires whole new ways of looking at information security

By Ms. Yuh-Ling Su

Process and Security Improvements under DIACAP

On November 28, 2007, the most significant change in security policy in 10 years occurred when the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) replaced the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

The Department of the Navy commenced full transition to DIACAP on March 31, 2008, with the release of a naval message issued by the DON Chief Information Officer, "Department of Navy's Transition Plan from DITSCAP to DIACAP." The message (311917Z Mar 08) is available on the DON CIO Web site at www.doncio.navy.mil, under the "Information Assurance" topic area.

All DoD and DON information systems are required to go through rigorous testing for certification and accreditation (C&A) prior to deployment on operational networks. Under DITSCAP, this process involved four review phases spanning several years of system development time before a system could obtain an approval to operate (ATO) in an operational environment.

Under DIACAP, a much greater emphasis is placed on key security stakeholder collaboration early in a system's development and the standardization of a robust, flexible, end-to-end C&A process, which results in a much shorter development cycle for a system to obtain an ATO and be fielded. The five key life-cycle phases for any system under the new DIACAP are summarized in Figure 1.

The changes ushered in by DIACAP don't stop with process improvements. DIACAP also provides a much needed net-centric approach to security risk determination and evaluation with expanded inheritability options relating to information assurance (IA) controls between systems, networks, sites and enclaves. It also forces IA to be built in from a system's concept stage through its entire life cycle. Not only will this yield improved security for fielded systems, but it will minimize the need for rework as C&A documentation proceeds through the independent government review process.

In fact, with this improved up-front security engineering, only a single security test will be required, either in a controlled development environment, or in the field to support an ATO decision.

DIACAP Transition

The DON CIO's goal is to ensure a smooth and successful migration of all DON information systems from DITSCAP to DIACAP. To adequately plan for DIACAP transition and the requisite automation of the C&A process, the DON DIACAP working group (DWG) is chartered to develop a unified departmental transition plan to implement DIACAP.

Key aspects of this plan include:

- Establishment of a DON DIACAP Transition Program to develop detailed guidance for implementing DIACAP throughout the DON;
- Procurement and implementation of a commercial off-the-shelf tool to support the DIACAP process; and
- Guidance to assist personnel, such as program managers, information assurance managers and system managers, involved in the security of information systems in developing DITSCAP to DIACAP transition plans.

DON DIACAP Tool Solution

To ensure the DON realizes efficiencies and improved speed to security capability, the DON CIO established the DON DIACAP transition effort to procure an automated tool to support the entire end-to-end C&A process for the DON enterprise. Appro-

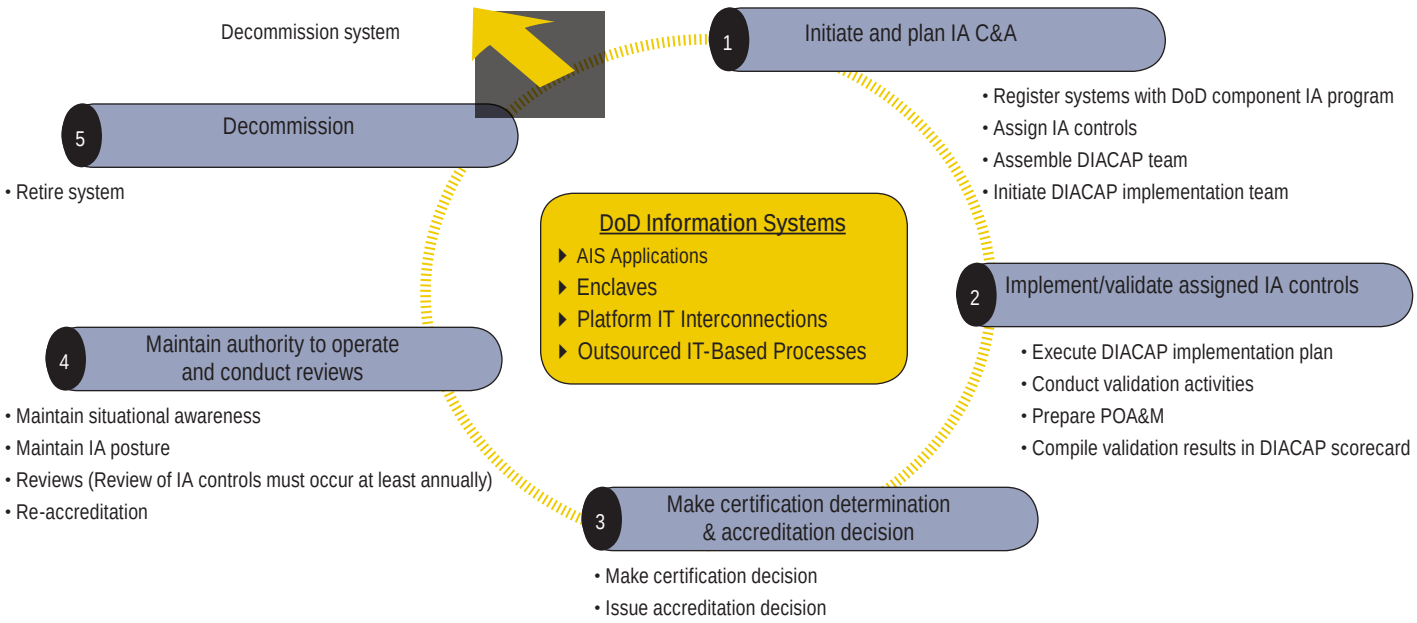


Figure 1. DIACAP life cycle phases.

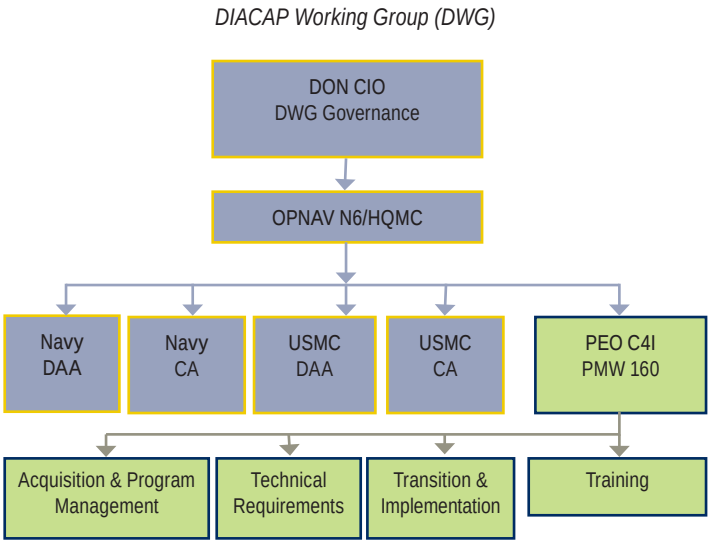


Figure 2. DIACAP Transition Governance Structure.

priately, this tool is named the C&A Support Tool. Without CAST providing C&A automation, from initial system registration to eventual system decommissioning, the benefits resulting from DIACAP would be dramatically limited.

The increased DoD emphasis on system security, as a result of recent Federal Information Security Management Act (FISMA) mandates, makes it critical to automate the entire C&A process. A DON automated tool to improve and standardize the C&A process was recognized in early fiscal year 2007 and is now well underway. The plan indicates the procurement of CAST will occur in late 2008, with initial operational capability available in early 2009.

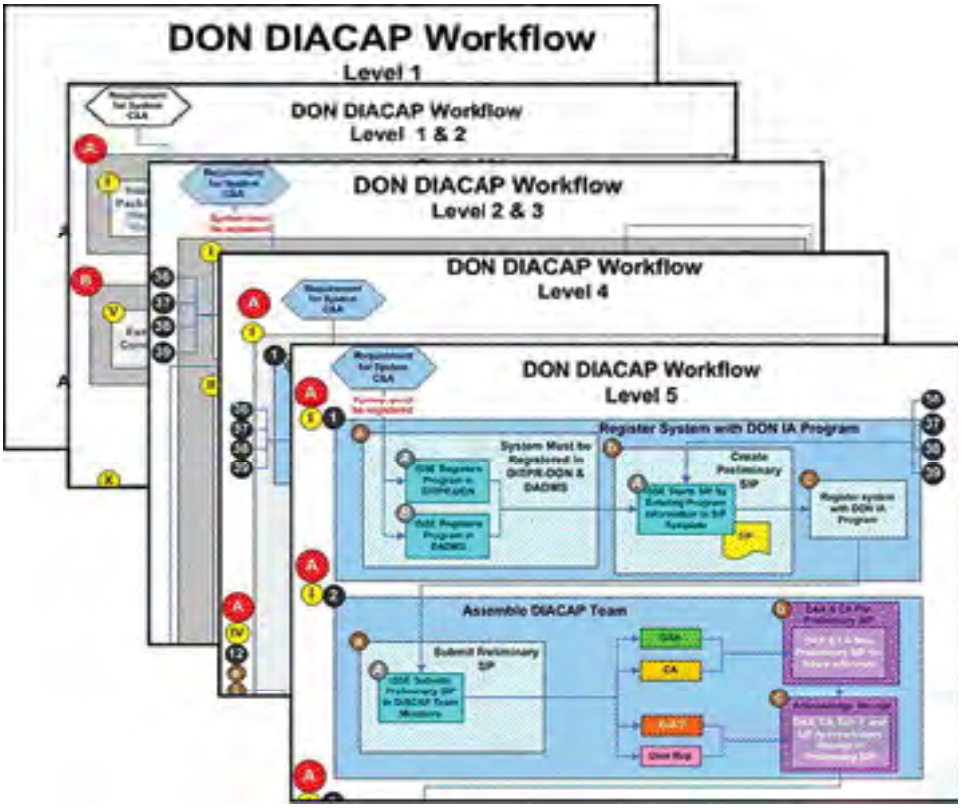


Figure 3. DIACAP workflow illustration.

Governance

Figure 2 identifies the organizations and the major functional components of the DON DIACAP transition effort managed by Program Management Warfare (PMW) 160, Networks, Information Assurance and Enterprise Services, under Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I).

PMW 160, as the technical agent for the DON CIO, will develop a standardized end-to-end C&A process and acquire and implement CAST, thus enabling the DON to fully transition from DITSCAP to DIACAP in a robust, controlled manner. In fulfilling this role, PMW 160 is providing the strategic planning, subject matter expertise and acquisition competency needed to not only fulfill DON CIO objectives, but to ensure a well-engineered, comprehensive and supportable tool is provided in a timely manner to support the entire C&A community.

DON DIACAP Transition Execution

The preliminary work in the DON DIACAP transition effort began in October 2007. To capture relevant requirements, a series of tabletop exercises and process walkthroughs were conducted with representatives from virtually all C&A stakeholder perspectives. The result was a C&A community understanding of the complexities of the DIACAP process, the respective roles and responsibilities of each level of interest and a very detailed process workflow chart characterized by five levels of fidelity.

This detail is illustrated in Figure 3, where Level 1 entails the process overview, Level 2 defines all activities, Level 3 assigns all tasks that must be performed, Level 4 delineates each task and the estimated time for completion, and Level 5 defines how each task is completed.

This workflow chart has been the basis for all follow-on efforts associated with requirements definition, procurement guidance, the training approach and community implementation.

To fully migrate from DITSCAP to DIACAP, four key program components must be successfully executed:

- C&A package generation and requirements estimation;
- Provision for DIACAP transition technical support;
- Acquisition of CAST to support end-to-end C&A processes; and
- CAST training to familiarize the C&A community with the tool's capability.

As envisioned, CAST must support up to 25,000 users ashore and afloat, with a minimum of 2,500 concurrent users. This rate is estimated for NIPRNET, with up to an additional 5 percent of this activity level expected on the SIPRNET.

The architectural approach will not only accommodate this level of activity, but will also allow seamless expansion should greater access be required in the future.

CAST requirements include the ability to collect metrics on all aspects of processing and management of C&A information so that a continuous process improvement program can be supported as the nature and requirements associated with C&A continue to evolve.

With CAST, automating major DIACAP requirements will be met for all information systems, including information technology systems; networks; circuits; sites; infrastructures; enclaves; and environments and assets that require security certification and accreditation within the DON, regardless of current accreditation status.

Specific goals for CAST include:

- Ensuring IA is built in from the concept stage through the life cycle;
- Accounting for inheritance of information assurance controls;
- Enforcing annual reviews for all systems and sites; and
- Providing enterprise-wide visibility into security posture and risk.

By facilitating standardization and quality improvement for C&A packages from the initiation of the process, significant reductions in review times, rework and learning curves are expected immediately.

In addition, early collaboration by stakeholders will ensure adequate identification and resolution of security risk issues early in the process and not later during formal C&A reviews.

Once the CAST procurement award is made, the tool will be initially implemented during a pilot phase with the objective of testing processes, procedures and templates. The pilot will build the necessary databases, verify process steps and proper tool configuration, conduct test and evaluation, and process selected DIACAP C&A packages to verify tool effectiveness in a controlled environment.

Training

At the same time, training will be provided to the C&A community on the tool and detailed DON processes and policies. It is expected that training will be an ongoing requirement throughout the life of CAST. Once CAST is fully implemented, DIACAP training will target personnel performing activities in the three main tiers of the C&A process: package creation, review and approval.

Training will focus on required tasks and how to perform these using the tool. Each tier of training will contain an overview of the DON process flow and build upon the activities accomplished by all members of the C&A team.

Since transition from DITSCAP to DIACAP will be gradual over the next three years, there is a phasing out of systems' C&A documentation from DITSCAP to DIACAP. The DIACAP transition team will provide subject matter experts to support program and system managers, as well as IA managers, in planning each system transition to DIACAP. This will include assistance in developing transition plans and answering any related questions.

Finally, because systems will begin transitioning to DIACAP prior to full implementation of the DON automated tool, all submissions of C&A packages will continue using existing C&A package systems in the near term.

The transition to DIACAP is great news for DoD and DON system developers, program managers and security managers!

Additional Information

The C&A process has undergone major changes over the last several years. These were driven by increased awareness of security vulnerabilities, shrinking resources and the pressing operational need to field new and improved capabilities to support the warfighter.

The movement from DITSCAP to DIACAP has provided an opportune time to both automate and standardize the entire end-to-end C&A process to conserve resources and ensure security risk is managed at acceptable levels.To stay abreast of the information being developed during this transition time, readers are encouraged to periodically access the DON CIO Web site at www.doncio.navy.mil.

For now, programs desiring to make use of DIACAP templates can access them from the Fleet Forces Web site under the View All Site Contents/Documents tab on the left side of the page at https://www.fleetforces.navy.mil/netwarcom/navycanda/default.aspx.

For the Marine Corps, users can access the Marine Corps Xacta Information Assurance Manager tool available at https://hqtelosweb.hqmc.usmc.mil/.

The primary contact for DITSCAP to DIACAP transition technical support can be reached by e-mail at SPSC-DON-DIACAP@navy.mil.

Secondary contacts for transition technical support are:

Navy - Operational Designated Approving Authority (ODAA) - e-mail: Navy_ODAA@navy.mil or (757) 417-6719 x0.

Marine Corps - Programs of record (not yet fielded), contact the Marine Corps Systems Command (Systems Engineering, Interoperability, Architectures & Technology (SIAT)) at (703) 437-3824.

All other systems (including fielded programs of record), contact the Marine Corps Enterprise Network Designated Approving Authority (MCEN DAA) by e-mail: M_MCEN_DAA@usmc.mil or (703) 693-3490.

Resources

- DON DITSCAP to DIACAP Transition Guide, version 1.1, June 9, 2008 - under the Information Assurance topic area at www.doncio.navy.mil.
- DON DIACAP Handbook, version 1.0, July 21, 2008 - under the Information Assurance topic area at www.doncio.navy.mil.
- DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), Nov. 28, 2007 - www.dtic.mil/whs/directives/corres/pdf/851001p.pdf.
- Secretary of the Navy Manual, SECNAV M-5239.1, Information Assurance Manual, November 2005 - http://doni.daps.dla.mil/SECNAV%20Manuals1/5239.1.pdf.
- DoD Directive 8500.01E, Information Assurance (IA), Oct. 24, 2002 - www.dtic.mil/whs/directives/. Certified as current April 23, 2007.
- DoD Instruction 8500.2, Information Assurance (IA) Implementation, Feb. 6, 2003 - www.dtic.mil/whs/directives/corres/pdf/850002p.pdf.

Ms. Yuh-Ling Su is the DON DIACAP transition assistant program manager under PMW 160.

CHIPS

CAN YOU HEAR ME NOW?

PLOTTING A SPECTRUM REVOLUTION

By Tom Kidd, Director, DON Strategic Spectrum Plans and Policy

Evolution and revolution are very different processes …

Adm. Vern Clark wrote about "revolution" while serving as Chief of Naval Operations. Today, the retired CNO still refers to revolution when publicly speaking about his efforts to change and improve business processes within the Navy. He confessed that, even as the second longest serving CNO, he didn't have time for "evolution," which is why he unapologetically chose revolution.

Evolution and revolution are very different processes. While evolution is a process of gradual and relatively peaceful social, political or economic advance, revolution is a sudden, radical and absolute change.

Evolution in business processes provides time for people to accept slow methodical changes. On the other hand, revolution is generally difficult for people to accept due to rapid change and is often viewed negatively.

Revolution is used to describe change in many business processes. In fact, modern computers and software are results of a revolution that led to the Silicon Valley high-tech empires in Northern California.

The convergence of cellular technology, the Global Positioning System (GPS) and a long list of services, technologies and devices are setting the stage for a wireless revolution that will influence our personal lives, business processes and the capabilities of the Marine Corps and Navy, in such a way not seen since the introduction of modern warfare.

The Marine Corps and Navy have global responsibilities, and they require a significant number of radio frequencies to conduct their worldwide operations. All radio frequencies are recognized by international law as belonging to each and every nation.

U.S. forces face access issues in each country in which they operate due to competing civilian or government users of national spectrum allocations. For example, when the Marine Corps and Navy are operating in Japan, the Japanese government regulates the radio frequencies U.S. naval forces can use. The same is true for Australia, Republic of Korea and all sovereign nations.

But even though radio frequencies are allocated, a large portion of the assigned spectrum is used sporadically, and there are wide variations in the use of assigned spectrum. The limited available spectrum and the inefficiency of its usage demands a new methodology to exploit existing wireless spectrum "opportunistically."

The wireless revolution is just beginning. A number of radical changes in the use of the electromagnetic spectrum, or radio frequencies, will soon have "dynamic" effects on naval capabilities. Dynamic Spectrum Access (DSA) refers to radios and other wireless capabilities that dynamically adjust to the spectrum environment and access radio frequencies that are unused or underused.

Access to spectrum, along with the corresponding capabilities and bandwidth may, by today's standards, be almost limitless. The Defense Advanced Research Projects Agency (DARPA) has developed DSA capability known as "Next Generation" or "XG," which promises significant benefits to forward deployed Marines and Sailors. Commercial companies are also developing DSA capabilities.

The goals of the XG program are to develop both the enabling technologies and system concepts, along with new waveforms to provide dramatic improvements for assured military communications in support of worldwide operations, according to DARPA.

The XG program approach plans to investigate methods to leverage the technology base in microelectronics, with new waveforms and medium access and control protocol technologies, to construct an integrated system.

The proposed program goals are to develop, integrate and evaluate the technology to enable equipment to automatically select spectrum and operating modes to minimize disruption to existing users and to ensure that U.S. forces can fully exploit their superiority and investment in information technology.

DSA will revolutionize naval wireless capabilities by providing greater access to limited spectrum resources. Today, there are considerable obstacles to employing DSA. International and national spectrum governing bodies control spectrum use through rigid radio frequency allocations that often result in one frequency per wireless use.

The benefits of DSA to the Marine Corps and the Navy will be impressive, but changes to national and especially international spectrum governance are inexplicably slow.

The DON Spectrum Team is "plotting a spectrum revolution," and we are not alone. We are part of a global spectrum revolutionary movement of industry, private consortia and other progressive nations on the leading edge of technology.

A revolution is seldom accomplished alone.

For more information, please go to the DON CIO Web site at www.doncio.navy.mil, or contact the team at DONSpectrumTeam@navy.mil. CHIPS

Success Stories from Naval Surface Forces and the Surface Warfare Enterprise

By Naval Surface Forces Public Affairs

Management of Naval Surface Forces (NAVSURFOR) is organized under the Surface Warfare Enterprise (SWE), an organizational construct established in 2005 that seeks to optimize warfighting readiness of the Surface Fleet.

Continuous process improvements support the SWE mission accomplishments in each core area of maintenance, modernization, logistics, manning and training.

Under the SWE, Class Squadrons, or CLASSRONs, were developed as functional command organizations that represent each major class of ship. CLASSRONs are responsible for the manning, training, equipping, modernizing and maintenance of the ships in their class.

CLASSRONs work directly for the Current Readiness Officer, Naval Surface Force Atlantic. They provide the warfighter perspective from the waterfront to the Cross-Functional Teams that help prioritize SWE efforts to meet NAVSURFOR's primary objective of "Warships Ready for Tasking."

The enterprise approach aligns multiple organizations to function as a single entity delivering the right force — at the right places — at the right time — and at the right cost through the careful stewardship of resources.

SWE efforts to increase warfighting readiness have direct impact on the waterfront.

Seattle, Wash. (May 20, 2008) A Landing Craft, Air Cushion hovers over the surface of Elliot Bay behind the amphibious dock landing ship USS Rushmore (LSD 47) during a parade of ships in commemoration of the 100th anniversary of Theodore Roosevelt's Great White Fleet. U.S. Navy photo by Mass Communication Specialist 2nd Class Jason Beckjord.

Diesel Engine Lube Oil Purifier Cleaning

Fast-track development leads to resource and manpower savings

A collaborative initiative, between LSD/LPD-17 Class Squadrons, Naval Sea Systems Command's PMS 470, Expeditionary Warfare, and Naval Ship Systems Engineering Station (NAVSSES), fast-tracked the development and subsequent implementation of a new diesel engine lube oil purifier cleaning process that changes the way Navy ships usually do the job.

In this case, the new process of purifier cleaning means that a considerable number of Navy resources will be saved, including costs for labor, maintenance and repairs. The new process will also reduce the collateral damage associated with improperly maintained diesel engines.

The old method had Sailors hand-cleaning individual purifier assembly discs, a process that had to be done daily, and then reassembling the discs in the correct order so the purifiers would meet maintenance and safety clearances.

LSDRON learned that Military Sealift Command (MSC) ships don't disassemble their lube oil purifier strainer assemblies for routine cleaning. Instead, they remove them as a unit and dip them for one hour in a special commercial phosphoric acid-based solvent, and then rinse them clean. The disc packs emerge from the solvent gleaming as if they were new. The method is safe, effective and cuts the time for maintenance and reduces the risks for damaging equipment significantly.

"Though the old method is the way it had always been done, the process had to be improved as it took too much time and manpower, and we found that ships were breaking the purifiers at high rates and spending a lot of money to fix them. Through research and talking to people we found that MSC ships used this nonobtrusive way to clean the purifiers.

"We found it to be highly efficient in regards to saving time, ship parts and money. We knew this was a better way to work and began the fast-track push towards getting it approved and implemented," said Capt. Michael Hill, the LSD/LPDRON deputy commander.

With Capt. Craig Kleint, LSDRON commodore, and PMS 470 personnel watching, a successful cleaning demonstration was held aboard the dock landing ship Fort McHenry (LSD 43) last summer in Norfolk, Va.

Capt. Kleint said that Fort McHenry Sailors using the MSC procedure were impressed with how easily and quickly they could clean the discs. They were also excited because the new process would reduce cleaning time and improve mission effectiveness.

LSDRON engineering representatives were onboard USS Rushmore (LSD 47) to observe engineering evolutions and during the visit, LSDRON staff told Rushmore engineers about the recently approved new procedure.

Engineman Senior Chief Bryan Richards said, "Currently, it takes four hours to clean our main engine lube oil purifiers. If this new process and cleaner will help cut the time to one hour, then I'm all for that!"

The development and implementation of the new process took a bit of time, but CLASSRON personnel remained motivated because they well understood its advantage to the fleet, according to Hill.

"We fully expect this information to be widely shared and the process to hit the fleet in the next six months. Once implemented, the process will be exported to other ship classes such as the San Antonio amphibious transport dock and the Avenger-class mine countermeasure ships. The benefits will be long-reaching and long-term," Hill said. CHIPS

Technology Keeps FFG Resources in Stock

Efforts mean vital circuit card assemblies will not become obsolete

Members of the Naval Surface Forces (NAVSURFOR) N41 group made significant headway in identifying repair options for guided missile frigate (FFG) circuit card assemblies (CCAs) that are in danger of depletion because repair and replacement capabilities for the CCAs did not exist. But the N41 group's careful analysis has already led to some repair solutions.

FFG 7-class Engineering Plant Control System (EPCS) reported deficiencies in performance and systems supportability in regard to the CCAs that are among the EPCS components. There are 64 CCAs that are unique to the FFG-class EPCS.

"The goal of the analysis project is for officers and contractors to use new technologies to find better ways to maintain and repair the CCAs that will save the fleet money, improve ship efficiency and resource management for all of the Navy's FFG-class EPCS CCAs," said Capt. Harry W. Davis, force supply officer for NAVSURFOR. "We estimate that once Gold Disk program developers and staff conclude the analysis we can implement a new repair capability and find the solution for repair and restocking."

To date, 29 of the 64 circuit card assemblies were identified as part of the Gold Disk program with fleet and shore microminiature (2M) repair sites identified with the capability to repair these CCAs. Gold Disk routines are diagnostic troubleshooting aids used in conjunction with 2M repair to isolate and repair faulty components on circuit card assemblies and electronic modules.

A testability/reparability analysis has been completed for the remaining cards and eight to 12 CCAs can be "Gold Disk" developed by year end which includes the capability to repair the parts. There are 15 CCAs that have less than one year to depletion, 18 CCAs that have two to three years to depletion, eight CCAs with three to five years to depletion and 23 CCAs with five years to depletion.

Yet to be identified are any CCAs which may not be repairable. Once the analysis is completed, NAVSURFOR can then prioritize which CCAs to develop first and plan for the way ahead.

"We estimate [that] we will save the FFG class EPCS community about $85,000 the first year," Davis said. "The new repair capabilities will impact CCA part replacement and repair with tangible and money-saving results."

Sailors will also have specific written instructions for the CCAs resulting in a higher repair capability rate. Eventually the changes will be in effect for all FFG 7-class Engineering Plant Control Systems.

CHIPS

USS Thatch (FFG 43) steams through the Indian Ocean waiting to participate in a replenishment at sea with the Military Sealift Command fast combat support ship USNS Bridge (T-AOE 10). U.S. Navy photo by Mass Communication Specialist 2nd Class Joseph M. Buliavac.

Naval Surface Forces Hires Executive Director

By Naval Surface Forces Public Affairs

Senior Executive Service member Mr. Jeffrey A. Klein began working as the first civilian executive director for Naval Surface Forces Aug. 18. Klein will serve as the principal civilian advisor to Commander, Naval Surface Forces Vice Adm. D.C. Curtis, and as the chief financial officer of the Surface Warfare Enterprise (SWE).

"Mr. Klein will be a valuable asset to the Surface Warfare Enterprise because the executive director position will maintain continuity of leadership at the executive level," Curtis said.

Klein's position as the CFO for SWE puts him in charge of all matters related to Naval Surface Forces warfare programs and requirements. He will ensure that all surface force commands function as a single business enterprise in regard to operational readiness, acquisition, research and development, and manning requirements. As the senior civilian within the Naval Surface Forces he will also lead and professionally develop the civilian workforce.

Prior to accepting this position, Klein served for more than 20 years in the acquisition community, most recently as the director of logistics and fleet support within the Space and Naval Warfare Systems Command (SPAWAR). He also brings extensive enterprise experience as a member of the Board of Directors for the Naval NETWAR FORCEnet Enterprise (NNFE) and the SWE Surface Board. He has served as a government employee for 22 years.

"I am looking forward to working with our talented surface leaders across the force to continue to improve efficiency, identify and prioritize our requirements, and to ultimately deliver warships ready for tasking not only in the near term, but in the future," Klein said.

CHIPS

SAN DIEGO (Aug. 25, 2008) - Naval Surface Forces Executive Director, Mr. Jeffrey A. Klein speaks to staff members following his introduction by Commander, Naval Surface Forces Vice Adm. D.C. Curtis. Mr. Klein will serve as the principal advisor to Curtis and as the chief financial officer of the Surface Warfare Enterprise (SWE). He will ensure that all surface force commands function as a single business enterprise in regard to operational readiness, acquisition, research and development, and manning requirements. U.S. Navy photo by Mass Communication Specialist 3rd Class Joanna Rippee.

SWE Takes Action in Support of Surface Warriors

Improving warfighter readiness through open communications

By Naval Surface Forces Public Affairs

Mine countermeasure ship Sailors will soon see a fix to correct the design flaw on the diesel engine exhaust flanges which have caused smoldering fires on their wood-hulled ships; guided missile frigate Sailors will soon see the results of a study to investigate options for repairing or upgrading aging FFG engineering plant control systems; and patrol coastal Sailors will see work begin on more effectively maintaining their corrosion-prone forward gun mounts.

These are just a few of the fleet issues addressed at the latest face-to-face conference of Surface Warfare Enterprise (SWE) stakeholders held in Washington D.C., Sept. 23-24 in which action was taken on a variety of issues affecting every class of ship in the Surface Force.

Led by Vice Adm. D.C. Curtis, commander, Naval Surface Forces and commander, Naval Surface Force, U.S. Pacific Fleet and the entire SWE Surface Board, the conference brought together major surface warfare stakeholders representing the Naval Sea Systems Command, Naval Supply Systems Command, the staff of the Chief of Naval Operations and the Class Squadron commanders.

The centerpiece of the conference was a series of briefings on the first day from each of the CLASSRON commanders outlining their top priorities for the SWE's Sustainment and Modernization Team (SMT). Those briefings were followed by SMT briefs addressing actions already taken and possible courses of action for each issue.

According to Curtis, breaking down barriers to free and open communication across the enterprise and the resulting dialogue are what makes the SWE successful.

"Having all the stakeholders either in the room or online via teleconference resulted in lively but productive conversations that made it possible the very next day for the SMT to outline the way ahead on each and every one of the issues discussed. Our goal is to increase warfighting readiness!" exclaimed Curtis.

"It was the best face-to-face conference we've had in the 18 to 24 months that I've been associated with the CLASSRON," said LHDRON Commander Capt. Bill Valentine. "Communicating between the myriad and complex activities associated with Surface Force maintenance, identifying requirements, then beginning to match scarce resources to the most important issues. It was a requirements and resource-focused discussion that was really bottom-up, from the issues originating at the deckplates to solutions developed and implemented up the chain all the way to NAVSEA and even the CNO."

All told, conference attendees reviewed 30 fleet issues from all eight CLASSRONs. Most of the issues sought improved capability and reliability, as well as improved safety on the waterfront.

According to SMT Flag Lead Rear Adm. Jim McManamon, about 30 percent of the issues raised can be addressed or largely mitigated with existing resources, while 70 percent of the issues will require longer term efforts and prioritization within the enterprise.

In addition to the specific issues mentioned above, others falling into the 30 percent that will receive immediate attention include:

• Implementation and sustainment for LCSRON ship-to-shore distance support programs;

• Conducting corrosion control surveys and identifying work that needs to be done across the CGRON in future availabilities to maintain the ships for their expected service lives;

• Implementing changes to how LHDRON Continuous Maintenance Availabilities (CMAV) are scheduled with an eye toward minimizing interference with training schedules and adapting the process to other classes;

• Addressing LSD diesel engine formal periodic assessments ensuring smart scheduling practices which consider the ships' schedules and updating the supporting technical documentation; and

• Investigating options to possibly give a higher priority and earlier implementation of the planned phased replacement of Aegis large screen displays onboard DDGRON ships.

Many of the issues discussed were important not only to the CLASSRONs that brought them up, but to all ships in the force. An obvious example is the issue of corrosion.

"If I had to pick a single issue that cuts across all classes, it's corrosion," said McManamon. "We have to get the identification and fixes in place for all classes, in order to get to 313 ships in the Navy."

According to the commander of the PCRON, Cmdr. Steve Coughlin, that's one of the great benefits of the face-to-face conference format used by the SWE. He said he learns lessons and solutions to common problems from the other ship classes.

"It's about the big picture," Coughlin said. "I learned things about FFGs that I had no idea they were doing. The engineering control problems that they're having are very similar to some issues with our main propulsion diesel engines. For me, right now, it's not as important as my other issues.

"But I can appreciate their challenges, and if I start seeing similar issues on my ships, I'm going to consult these guys and find out what path they went down. So there's a lot of potential for future work getting done on my ships just by the work being done by these other guys."

The SWE's Chief Readiness Officer Rear Adm. Kevin Quinn says surface Sailors have strong advocates in the CLASSRON commanders.

"They get up in front of a crowded room and explain issues with confidence to the program managers, senior civilians and flag officers," said Quinn. "They go over their issues — the fleet's issues — with an outstanding level of technical knowledge and competence backed up by good data. They explain everything in a high level of detail.

"The credibility they've built up here inside the beltway, and certainly out in the fleet, makes them powerful, impact players. It struck me as clear as a bell as I was watching these guys that they're the best, and they're really making a difference. I'm proud of what they've done in their squadrons and I'm proud of what they did here — all of it designed to improve warfighting readiness!"

For more information, visit Naval Surface Forces and the SWE online at www.swe.surfor.navy.mil.

CHIPS

Electronic documentation for patient encounters during USNS Comfort's humanitarian assistance deployment

Calling on the technology community to develop more effective handheld devices

By Navy Lt. Cmdr. Deirdre O. Smith, Retired Air Force Lt. Col. Kevin Riley, Keith Curley, Jeffery Zimmerman and Retired Navy Capt. Claire Pagliara

Soft Power

The U.S. military has been performing humanitarian missions since the end of the Cold War, sometimes in a support role to other agencies, often as the lead agency. Medical missions are typically, short-term, occur outside of the continental United States and involve the U.S. military providing care to large numbers of patients.

These missions are an integral part of national security. They serve as a deterrent to conflict because a forward military presence enhances peaceful cooperation and contributes to regional stability.

Department of Defense Directive 3000.05, "Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations," states that stability operations have a priority status comparable to combat operations. It also mandates that we develop measures of effectiveness that evaluate progress in achieving the mission's goals.

But despite the large number of missions over the past decade, there is a dearth of information in the literature regarding patient encounters. The few publications that are available show that data collection techniques vary widely and are laced with problems.

In 2007, USNS Comfort (T-AH 20) completed a four-month humanitarian assistance deployment as part of the President's policy on "Advancing the Cause of Social Justice in the Western Hemisphere." This narrative will provide historical background, describe the method used by the crew to document patient encounters and discuss lessons learned.

Accurate clinical documentation is imperative to monitor and evaluate patient care and assess effectiveness. We welcome help from the technology community to develop tools to aid in this effort.

Problems Identified

In a "Descriptive analysis of patient encounter data from the Fleet Hospital FIVE humanitarian relief mission in Haiti," from the Naval Health Research Center (NHRC), San Diego, researchers describe using paper free-text forms and pencil to document the diagnosis and treatment of patients during a 1997 deployment to Haiti. The report outlines the limitations in this method, including illegible handwriting, lack of conformity of language and many form areas left blank.

For a later study from 2001, researchers collected patient encounter data from Naval Medical Center San Diego (NMCSD) physicians who traveled with a nongovernmental organization (NGO), HELPS International, on a humanitarian assistance mission to Guatemala. The completed forms were entered into an electronic database and analyzed by NHRC San Diego.

Although the study, "Documenting Patient encounters during a humanitarian assistance mission to Guatemala," showed that a revised, forced-choice patient encounter form alleviated the problems of illegibility and nonstandard language often found in free-text forms, there were still problems because this method did not successfully link diagnostic data with treatment and prescription information, and often diagnoses were miscoded. Data were collected on diagnoses, treatments, medications, surgeries and type of provider specialty.

In the experience of the 48th Combat Support Hospital's 2003 deployment to Afghanistan, an eponymous report revealed similar findings. Data were collected using a paper and pencil method. Demographics were collected at the nursing triage station. The medical care providers documented the chief complaint, examination, diagnosis and treatment on the reverse side of the same form after each encounter.

Data were later compiled, and the results entered by hand into an electronic database. Limitations included incomplete forms, subjective analyses of patient conditions and small sample size.

In January 2005, West Coast-based USNS Mercy (T-AH 19) sailed to the Philippines and Indonesia where care was provided to 100,000 victims of the catastrophic tsunami. Various tools were used to capture patient data. Shipboard care data were captured without issue using the Composite Health Care System (CHCS).

Care data ashore were designed to be captured using the Army's Battlefield Medical Information System–Telemedicine (BMIS-T), the CHCS2-T system and NHRC's Access database. However, several problems were identified, including inadequate training for BMIS-T and a lack of appropriate data fields.

BMIS-T is similar to a handheld computer with special programming developed to assist deployed medical personnel with diagnosis and treatment. It can be used to record patient clinical encounters and transmit those records to a central repository.

BMIS-T is also programmed with healthcare reference manuals and can provide medical personnel with suggested diagnosis and treatment plans.

But BMIS-T was found to be inefficient when treating large numbers of patients. Reports indicate that an alternative paper-based system was created, but lack

Suriname (Oct. 4, 2007) - Ship's Serviceman Seaman Dominique Gray, assigned to hospital ship USNS Comfort (T-AH 20), checks in a patient at the Zanderij Clinic. Comfort is on a four-month humanitarian deployment to Latin America and the Caribbean providing medical treatment to patients in a dozen countries. U.S. Navy photo by Mass Communication Specialist 2nd Class Brandon Shelander.

of ownership of the process stalled implementation. An Excel spreadsheet was employed, but it only captured 9,500 patient encounters. The lesson learned from this experience is the need to continue to experiment with the various tools for documenting patient encounters during humanitarian assistance missions.

The use of information management tools in the health care industry has exploded in the past decade. Electronic documentation is rapidly replacing manual documentation due to multiple advantages. Electronic medical records (EMR) offer increased access, patient confidentiality and integration with other information sources, such as laboratories and radiology consultants.

In addition, EMR eliminates the issue of lost or forgotten charts, illegible handwriting or fragmented care. Handheld platforms also offer the advantages of simplicity and portability over a desk or laptop computer.

Handhelds are ideal documentation collection devices because they are small in size, low in cost and easy to use. Handheld tools for surveillance activities are invaluable in the field because they allow providers to collect large amounts of data with immediate access.

A field comparison of handheld devices for data collection was completed in Uganda in 2004 by the World Health Organization. The evaluations measured reliability, accuracy, logistics and ease of data transfer and showed that handhelds were far superior to any other method of collecting patient data.

Further Investigation

To advance the body of research, Comfort, the Center for Disaster and Humanitarian Assistance Medicine (CDHAM) and the Western Reserve Systems Group (WRSG) jointly tested and evaluated the military application and usability of patient encounter forms uploaded into a handheld hardware platform when Comfort sailed to Latin America and the Caribbean on a four-month deployment to provide medical treatment to patients in a dozen countries in June 2007.

OpenSurvey (Opensurvey.net), a service provided through a collaborative development effort between WRSG and CDHAM, was used to analyze findings. Using a simple form-based interface, which can be accessed globally through a secure Internet interface, OpenSurvey users can design custom surveys and easily distribute these surveys to a Pocket PC platform.

Handheld users were asked to evaluate and assess interface and collection performance in the following areas:

- Ability to collect and consolidate data;
- Test data transmission (ship-to-shore, shore-to-ship and OCONUS-to-CONUS); and
- Adaptability of user-developed survey and patient collection forms.

We also hoped to establish a baseline for power and logistical requirements for extended humanitarian assistance missions with the results from the survey.

Comfort's joint forces crew included personnel from Military Sealift Command, U.S. Navy, U.S. Air Force, U.S. Coast Guard, U.S. Army and Canadian Forces, and NGOs, Project Hope and Operation Smile. Twenty-five handheld devices were received through a grant from CDHAM.

Patient encounter forms were designed for medical (adult and pediatric) primary care patients, dental and ophthalmology. Patient encounter forms were recorded using an interface developed by Case Western Reserve University. The interface was edited and approved by the administrative command of Comfort and the heads of the medical, dental and optometry departments.

Key members of the crew who used the tool were trained by a representative from CDHAM. They were given opportunities for hands-on training with follow-up sessions with the CDHAM trainer for questions and feedback. Minor modifications were made to the format based on user suggestions and group consensus.

Once underway, users were asked to provide feedback and suggest content modifications. The director of Medical Operations was also available to answer questions and troubleshoot problems. A resource manual was provided by Case Western,

ESSEQUIBO, Guyana (Sept. 25, 2007) - U.S. Public Health Service Lt. Cmdr. Jamal Gwathney, a family medicine physician attached to Military Sealift Command hospital ship USNS Comfort (T-AH 20), speaks with a 3-year-old girl and her mother at Charity Hospital. U.S. Navy photo by Mass Communication Specialist 2nd Class Steven King.

GEORGETOWN, Guyana (Sept. 30, 2007) - Hospital Corpsman 1st Class Seana Gauger, attached to Military Sealift Command hospital ship USNS Comfort (T-AH 20), gives a patient an immunization shot at the Project Dawn Health Care Center. U.S. Navy photo by Mass Communication Specialist 2nd Class Joshua Karsten.

Republic of Suriname (Oct. 5, 2007) - Lt. Cmdr. Andrea Petrovanie, attached to Military Sealift Command hospital ship USNS Comfort (T-AH 20), calms a pediatric patient at Flustraat Clinic in Paramaribo, Suriname. U.S. Navy photo by Mass Communication Specialist 2nd Class Steven King.

and representatives were available via electronic or phone communications. A quality assurance program was established to ensure user reliability and data validity.

At each of Comfort's destinations, multidisciplinary teams were deployed ashore. The number of teams sent ashore varied depending on the nation's requests and capabilities of the host nation and Comfort's crew. Each team had an assigned tracker who was responsible for documentation of the patient encounter.

After the teams returned to Comfort, the handheld was placed in a docking station to upload the data. Stored data from the day's activities were then downloaded into a spreadsheet. The data were tabulated for the daily report requested by Comfort's commanding officer.

Evaluation

The handheld's utility in documenting patient encounter performance was measured using the Logical Framework Matrix initially developed in the 1970s in concert with CDHAM and the Defense Department's HIV/AIDS Prevention Program.

LogFrame is a tool used to clarify objectives, design activities, monitor progress and review accomplishments. Using 16 cells in a four by four project table, the LogFrame flows according to the following progression: Inputs, Activities, Outputs, Purpose and Goal. To conduct a comprehensive evaluation this log flow was integrated with the five basic concepts of monitoring and evaluation: Relevance, Effectiveness, Efficiency, Impact and Sustainability.

Simply stated, LogFrame uses a "temporal logic model" that runs through the matrix which forms a series of connected hypotheses:

• If these Activities are implemented, and these Assumptions hold true, then these Outputs will be delivered.

• If these Outputs are delivered, and these Assumptions hold true, then this Purpose will be delivered.

• If this Purpose is achieved, and these Assumptions hold true, then this Goal will be achieved.

After establishing the relevance of the project, inputs were identified which included all resources required for the mission: equipment, training and personnel.

Since the handheld devices are lightweight and portable they are ideal for field work. The waterproof encasements were important due to climatic conditions. Because use of handhelds is increasing, user training was easy.

Initial findings showed that the handheld provided a comprehensive platform obtaining all the data elements needed to accurately capture the population served (demographics) and the services provided. The interface provided area for free-text and allowed reasonable modifications.

A shortcoming identified is the need for a clear-cut definition of what constitutes a patient encounter and how that will be quantified. But while resources were used in the best possible way, there were many factors that contributed to the inefficiency of this method due to the scale of the mission.

Comfort's crew served a staggering number of 98,000 patients, conducted 1,170 surgeries, performed 380,000 procedures, administered 32,322 immunizations, dispensed 122,245 pharmaceuticals and issued 24,242 eyeglasses. The dental department alone treated 25,000 patients.

Because of the size of the handheld's screen the crew could only record data for one patient at a time, and they were not able to keep up with the high patient volume. After several countries were visited, the crew was directed to revert to written documentation, and the staff assigned to record data had to be increased.

Additionally, due to periodic lapses in the advanced infrastructure required to sustain connectivity, the amount of time involved in uploading data from the handheld averaged 9 minutes and frequently one-third of the devices needed to be uploaded twice each day. Both conditions were unacceptable and contributed to inefficiencies.

Discussion

Although we did not meet all of the objectives, we feel that we contributed to the body of evidence that tests the use of handheld devices for patient care in humanitarian assistance missions. By utilizing a handheld device, empirical data can be efficiently recorded and then downloaded for coding, analysis and interpretation.

However, the problems of connectivity that were encountered threaten their utility. Since humanitarian assistance missions are a Navy priority, it is imperative that we continue to plan, train and prepare to conduct and support stability operations.

A vital component in mission preparation and implementation is the ability to monitor and evaluate productivity and the effectiveness of outcomes. We feel that it is essential to pursue this trajectory of exploration and encourage and welcome assistance from the technology community.

Navy Nurse Corps Lt. Cmdr. Deirdre O. Smith is the assistant medical operations officer for USNS Comfort. She has a master's of science degree, is a Ph.D. candidate and is adult nurse practitioner board-certified.

Retired Air Force Medical Service Corps Lt. Col. Kevin Riley is the deputy director for the Center for Disaster and Humanitarian Assistance Medicine Uniformed Services University of the Health Sciences. He has a Ph.D. in international health.

Keith Curley is a principal with Western Reserve Systems Group, LLC.

Jeff A. Zimmerman is an information technology manager in the Center for Disaster and Humanitarian Assistance Medicine Uniformed Services University of the Health Sciences.

Navy Nurse Corps Retired Capt. Claire Pagliara has a Ph.D. in nursing, and is head of Research Resources in the National Naval Medical Center. She was the medical operations officer for USNS Comfort at the time the study was conducted. CHIPS

Data as a Service

The new paradigm for decision making in the DoD acquisition community

By Martin Fairclough

On July 25, 2008, the Honorable John Young, Under Secretary of Defense for Acquisition, Technology and Logistics (AT&L), signed a memorandum for service acquisition executives that represents a fundamental reengineering of acquisition management systems. The memo "Implementation of Service Oriented Architecture (SOA) within DoD Acquisition Community," aims to significantly improve accurate, timely and coherent data use within the acquisition community to enable better decision making. How we got to this decision and what it means for Defense Department managers and the military services is the subject of this article. The story is remarkable, not only because of its success, but the speed at which it was executed.

Figure 1 represents the data model currently used by the DoD to make acquisition decisions — and a proposed model — a model many businesses have used since the 1980s. Actually, Figure 1 fails to highlight one of the most troublesome flaws of the current system: data is provided via the conduits indicated on an extraordinarily slow basis. At each level, data is reviewed and forwarded to the next level but may no longer be accurate by the time it is reviewed at the next level.

One of the most desirable features of the new DoD model is that each request for data from the indicated SOA server generates a separate call from authoritative sources for the data element. In this concept called "data as a service," a data request invokes an action that immediately returns the authoritative data element with a clear origin.

The question is: *How do we move DoD's many and varied systems to a model that separates data from these systems for a streamlined approach to data management?*

SOA Demonstration

Feb. 29, 2008, marked the start of a change in the way DoD manages defense acquisition data. On that day, three business tools displayed authoritative data from 12 Major Defense Acquisition Programs on demand for the Weapon Systems Lifecycle Management (WSLM) Core Business Mission (CBM) senior steering group and invited DoD executive leadership.

Data for 12 MDAPs, four from each service, were obtained from the authoritative source for each data element in real time. To further prove the flexibility of this new data management model, the Air Force changed one of its authoritative data elements at the program management source for the B-2-EHF SATCOM program. Business tool displays were refreshed, and the revised program data element was properly reflected in each display and available for use by DoD in less than two minutes.

This demonstration of data governance and technical capability offers acquisition officials the ability to make informed acquisition decisions based on timely and authoritative data.

USD (AT&L) initiated this effort with a memorandum issued Oct. 5, 2007, mandating a Service Oriented Architecture (SOA) Demonstration Project (AT&L SOA Demo). The demo, which later successfully expanded to a pilot project, was co-led by Gary R. Bliss, Deputy Director of Enterprise Information and OSD Studies in the office of Acquisition Resource and Analysis (ARA), and Mark E. Krzysko,

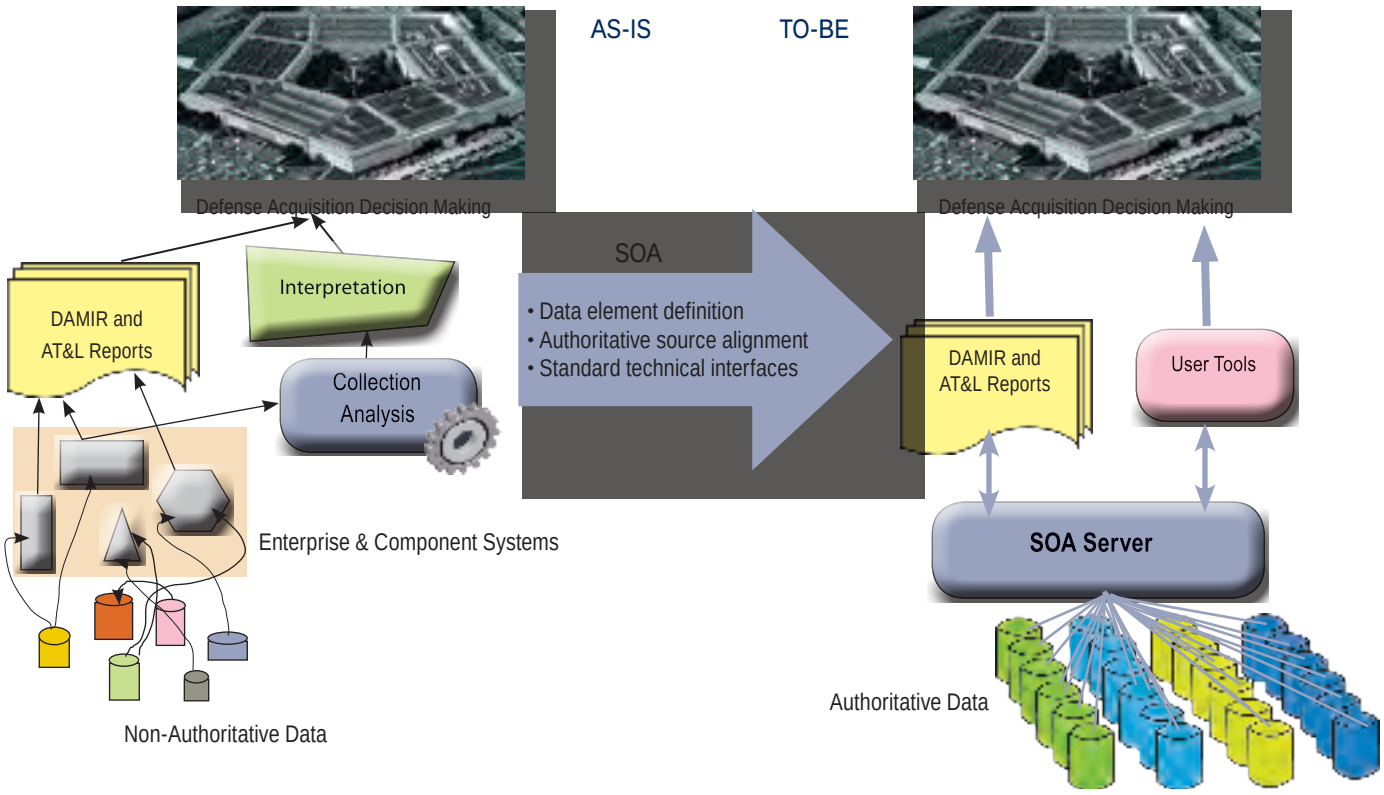


Figure 1.

Assistant Deputy Under Secretary of Defense for Business Transformation (AT&L(BT)), both within AT&L, and with participation by the military services and the Business Transformation Agency.

Providing strategic functional vision and leadership, Bliss established the foundational data governance and management concepts and methodologies to be employed and Krzysko provided technical vision and leadership, establishing the SOA middleware framework and SOA infrastructure required for the demonstration.

AT&L ARA staff developed functional requirements and the policy framework. The Business Transformation Office published a straightforward technical approach and arranged to host the SOA infrastructure.

In the proceeding months, Bliss and Krzysko led all aspects of the AT&L SOA demonstration to triumphant completion.

SOA Framework

SOA is not just an architectural style of services seen from a technology perspective, it encompasses the policies, practices and business processes through which governance ensures the right information is provided to, and consumed by, users.

SOA separates data governance from the tools that use the data, thus making authoritative data immediately available to users. Under SOA, data is pulled directly from sources the military services and other data providers designate as "authoritative." These data elements are then "federated" and made available for consumption by any authorized user through any authorized tool.

A federated database, or virtual database system, is a type of meta-database management system which transparently integrates multiple autonomous database systems into a single federated or merged database. The databases are interconnected via a computer network and can be geographically decentralized.

The problem that needs to be overcome is not simple. For the most part, current data systems were implemented to electronically mimic pre-existing paper-based systems. SOA is reaching for a profoundly different data model; one in which data is transparently available throughout the enterprise to whomever has a legitimate need for the data as soon as it is developed.

The existence of a well-functioning SOA infrastructure does not eliminate periodic program reviews and the data displays associated with them. On the contrary, it profoundly transforms program reviews. Instead of just providing raw data, data will be interpreted for decision making by senior acquisition managers. This change is immense!

SOA Governance and Data Elements

SOA requires a SOA governance institution. The creation of the governance structure during the AT&L SOA Demo, shown in Figure 2, among others, includes acquisition officials from AT&L(ARA), AT&L(BT), Army, Navy, Air Force and Defense Acquisition Management Information Retrieval.

DAMIR is a DoD system that provides enterprise visibility to acquisition program information. The primary goal of DAMIR is to streamline acquisition management and oversight by leveraging the capabilities of a net-centric environment.

In its current configuration, the tool must encompass all the means for obtaining and purifying its own data. Even so, maintaining data coherence with sources is a perpetual — and losing struggle. Under SOA, DAMIR is re-plumbed to extract data from the SOA server, which is already authoritative. The difference for DAMIR will be immense (almost no data effort), and perhaps new tools of unanticipated sophistication and functionality can be easily plugged into the SOA data server, and all the tools will be using the same data at any point in time.

The WSLM CBM data governance structure has a charter to address the three key elements of data infrastructure management: data definitions, technical standards and unambiguous assignment of institutional responsibility to maintain the single authoritative copy of each governed data element.

The SOA Demonstration leveraged 61 data elements associated with the management of 12 MDAPs. The results showed that commercial information technology tools, with careful regulation of the definition and technical standards, permit secure and transparent use of data from disparate sources that facilitate an acquisition user-defined operating picture (UDOP) for business systems, similar to use in warfighting systems.

Data brought under governance for the subsequent pilot include 140 elements in the following major categories:

- EV (Earned Value) Data – Elements used in the demo plus additional contract elements included in DAMIR's "Contract Data Point" and/or reported on the Contract Performance Report (CPR).
- Nunn-McCurdy Unit Cost – Current Estimate, Current Acquisition Program Baseline (APB) and the original APB Unit Cost Data reported at the total appropriation level (i.e., RDT&E, Procurement, MILCON and O&M).
- Budget Submission – Last president's budget and Program Objective Memorandum (POM)/Budget Estimate Submission (BES) by appropriation and fiscal year to provide a reference point for POM 10 analysis.
- Milestone – Program acquisition milestones as agreed from APB(s).
- Science and Technology – Key Performance Parameters, thresholds, objectives and current measurement.
- Program Management (General) – General program administration elements.

Through this governance body, agreement to data definitions, identification of authoritative sources for the required data, and achievement of data availability for on-demand access were accomplished for the demonstration and pilot. A central management focus is required to coordinate business processes and information requirements to avoid duplicative efforts and costs while

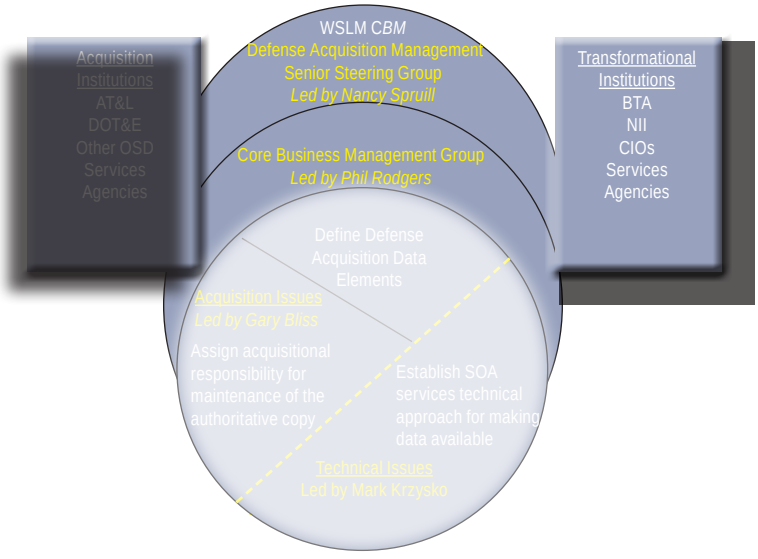


Figure 2. AT&L SOA Governance Structure.

encouraging the reuse of information services to promote more efficient acquisition management decisions. Cost avoidance will present a return on investment. Other potential long-term benefits of SOA are:

- Establishing managed authoritative DoD acquisition data sources;
- Improving data availability and reliability to decision makers;
- Improving situational awareness of the acquisition status of each MDAP;
- Separating data from business tools and applications;
- Improving program management and oversight efficiencies;
- Reducing burdensome oversight reporting; and
- Reducing the acquisition cost for future business systems.

A critically important governance function is to identify where responsibility for maintaining the single authoritative copy of an individual data element should reside. For those data elements for which the service acquisition executives and program executive offices are responsible, there is no problem with the services controlling their own data.

The vast majority of data for a program, however, is what may be called "state data" such as the program name, fiscal year, department code and contract number. Under SOA, these data would be transparently visible throughout the enterprise.

For users, there is one place to go for any data element governed by the SOA middleware server. Each data element would come with date and time stamps: the "pull date" when the data was accessed and the "shelf date" when the data was last updated.

Data maintainers will have a streamlined method of updating data. The SOA governance mechanism will issue documents that explicitly identify what offices are responsible for maintaining each individual data element. In general, data maintainers will be able to ensure that a specific spreadsheet, for example, is kept current with the correct values and stored in a specific server directory. The result will be the elimination of continuous management requests for updated data tables.

SOA Pilot Project

Based on the success and lessons learned from the AT&L SOA Demo, a two-phased pilot project is underway led by Bliss and Krzysko. Phase 1 was initiated in April 2008, and the initial capabilities will be completed by fall 2008. An additional 25 MDAPs have been added to the original 12 for a total of 37 which equates to acquisition data representing 75 percent of existing MDAPs — a $1.3 trillion portfolio.

The technical center for the SOA Acquisition Visibility pilots was established at the Space and Naval Warfare Systems Center Atlantic, formerly SSC Charleston, with David Howard as the infrastructure lead, supporting Bliss and Krzysko.

Through Phase 1 efforts, defense acquisition decision making will move to a new paradigm of "seamless authoritative data transparency" based upon underlying governance provided by the WSLM. Figure 3 illustrates the technical approach.

Phase 2, performed concurrently with Phase 1, involves developing an initial operating capability for a DoD-wide SOA infrastructure compliant with pertinent DoD IT standards to include full competitive source selection for technical products or solutions.

Going Forward

The primary goal of this effort is to make ACAT I programs data consistent across the DoD. As this is accomplished, the WSLM CBM, which includes representation from other communities, such as systems engineering, science and technology, test and evaluation and contract management, will work to align data using WSLM definitions. The result will be the establishment of a durable data governance mechanism for regulating DoD's acquisition data, as well as the provision of a data infrastructure and SOA services, which makes data as a service a reality in the acquisition domain.

Martin Fairclough is a senior principal consultant supporting the AT&L SOA Team.

CHIPS

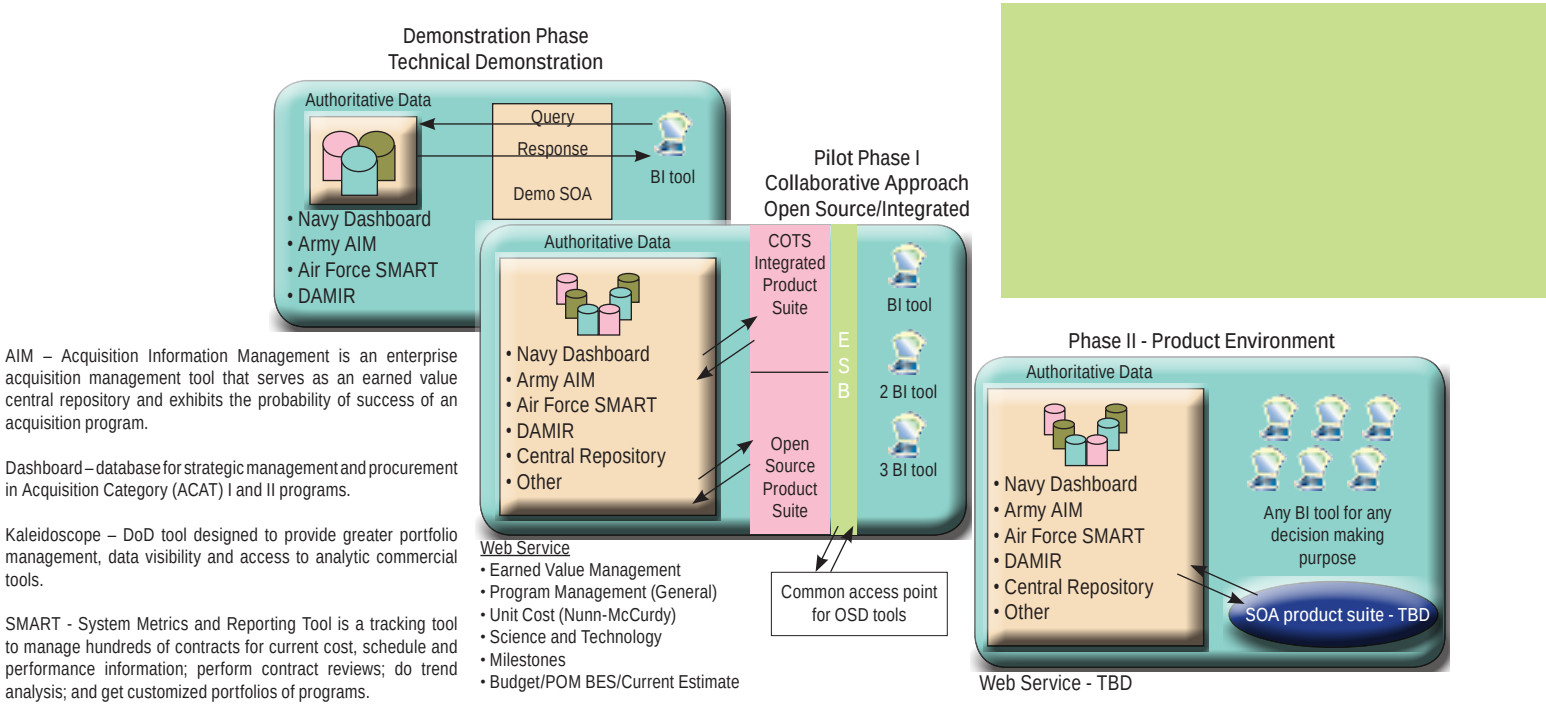


Figure 3. Acquisition Data Technical Approach.

Hold Your Breaches!

All Department of the Navy personnel should continue to increase their level of awareness about properly safeguarding personally identifiable information (PII). To learn more about properly safeguarding PII, go to www.doncio.navy.mil.

The following is the July 2008 summary of recently reported losses or breaches of PII involving laptops or thumb drives. Laptop security continues to be the foremost vulnerability in the Department of the Navy. Incidents such as these will be reported in each subsequent CHIPS magazine to increase PII awareness. Names have been changed or removed, but details are factual and based on reports sent to the Department of the Navy Chief Information Officer (DON CIO) Privacy Office.

1 Jul 08	Government laptop stolen from locked hotel room.
7 Jul 08	Laptop stolen from locked rental car while employee on TAD.
11 Jul 08	Government laptop stolen from locked government vehicle.
14 Jul 08	Government laptop stolen from locked government vehicle.
16 Jul 08	Government laptop stolen from guarded staging area.
17 Jul 08	Personally owned vehicle stolen with government laptop in trunk.
25 Jul 08	Government laptop stolen while on foreign travel.
28 Jul 08	Personal thumb drive stolen from government office.
30 Jul 08	Government thumb drive stolen from government office.
31 Jul 08	Personal laptop stolen from locked personally owned vehicle.

Lessons Learned

The majority of these thefts could have been prevented had the safeguards below been followed. Refer to the naval message issued by the DON CIO, "Safeguarding Personally Identifiable Information (PII)" of April 2007, available at www.doncio.navy.mil (search for "safeguarding PII"), for detailed guidance.

• Storage of any form of PII is prohibited on personally owned laptop computers, mobile computing devices and removable storage media.

• When removing portable electronic equipment from a government-controlled workspace for compelling operational needs, the device must be signed in and out, with a supervising official designated in writing by senior leadership, when it contains 25 or more records containing PII.

• Laptop computers and mobile computing devices and the data stored on removable storage media must be password protected. Refer to DoD Instruction 8500.2, "Information Assurance (IA) Implementation," of Feb. 6, 2003, available from the Defense Technical Information Center (DTIC) Web site at www.dtic.mil/whs/directives/corres/html/850002.htm.

• Most thieves steal electronic equipment for its street value, but smart thieves know they can make significantly more money — if they can access privacy information to commit identity theft.

• Automobiles are easy targets for thieves looking to make a quick buck. Locking your car is not sufficient protection for the contents inside or your personally identifiable information. Do not leave PII in your car; this includes personal mail and your vehicle registration. Thieves especially like to target ball fields, shopping malls and health club parking lots because they know that vehicles will be unattended for lengthy periods. If you must leave your laptop in the car, remove it from view. Be careful not to be seen locking a laptop in the trunk and park in a well-lit area.

• A good theft deterrent is placing a warning label on laptop computers that specifies the laptop contains hardware security controls which render the machine unusable.

• Encryption of data on all portable electronic devices is another good deterrent. If your laptop is not protected by the DON enterprise encryption solution, the use of WinZip software is authorized. WinZip is available on most Navy Marine Corps Intranet desktops.

• Train personnel on the security and safety risks associated with portable electronic equipment and the DON requirements for safeguarding PII.

Additional laptop security information can be found on the DON CIO Web site at www.doncio.navy.mil (search on "laptop") and also on the Federal Trade Commission Web site at www.ftc.gov.

Steve Muck is the DON CIO privacy team lead.

CHIPS

Operationalizing Military Support to Civil Authorities

CNIC prepares Navy regional and installation managers for emergency management

By Capt. BJ Keepers and Dr. Raymond Roll

During the wildfires in California last October, at least 1,500 homes were destroyed and more than 500,000 acres of land burned. Nine people died as a direct result of the fires while 85 others were injured, according to media reports.

Over 900,000 residents evacuated to escape the projected path of the fires, far exceeding the number evacuated from New Orleans during Hurricane Katrina, reported the San Diego Union Tribune.

Many of these evacuees were San Diego-based military members and their families. In response, Naval Bases Point Loma, San Diego and Coronado set up evacuation centers designed to help Navy families that fled their homes.

Additionally, nonessential personnel from Naval Base San Diego barracks were moved onto nearby vessels to accommodate additional Department of Defense displaced personnel.

The Defense Department provided a variety of support services to civil authorities to help battle the California fires. March Air Reserve Base was the primary staging area for relief supplies that were coordinated by the Federal Emergency Management Agency.

The National Guard called up 1,500 troops to man the fire lines, and another 100 California National Guard medical personnel provided medical assistance, according to CNN.

The Navy's Helicopter Sea Combat Squadron 85, based at Naval Air Station North Island, made more than 1,100 water drops on the fires in San Diego County, while more than 100 Sailors and federal firefighters battled the fires on the ground using trucks, fire engines and bulldozers.

Marine Corps Air Station Miramar and Camp Pendleton contributed several bulldozers, aircraft and firefighting trucks. A total of 12 fire engines from local bases were assigned for firefighting efforts.

Additionally, Commander, Navy Region Southwest, led by Rear Adm. Len Hering, stood up a Region Operations Center and Crisis Action Team for seven days of sustained operations. The team synchronized the shore force response of more than 5,000 Sailors and federal employees in disaster relief operations and provided Navy liaison officers to the county's Office of Emergency Services for full coordination with civil authorities.

In sharp contrast from the criticism voiced after Hurricane Katrina, the response and relief efforts by federal, state and local agencies involved in the California wildfires were widely praised. While the response was not without communication and coordination difficulties, the overall improvement in emergency management was not accidental; it was the result of a determined effort to integrate governmental efforts in preparing for and responding to major incidents.

This effort began in earnest after 9/11 with Homeland Security Presidential Directive/HSPD-5. HSPD-5's stated objective is *"to ensure that all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management."*

A significant feature within this national approach is the mandate that DoD has the responsibility to prepare for domestic emergencies, through measures taken in advance and during an incident, to reduce loss of life and property and to protect the nation's institutions.

Commander, Navy Installations Command (CNIC), has actively embraced this concept by aggressively establishing and manning regional and installation emergency operation centers (EOC) throughout the CNIC enterprise. This effort is driven by CNIC's foresight to operationalize shore forces and align them with fleet warfighting capabilities.

To further this strategic vision an emergency management classroom and war gaming center of excellence for the shore force enterprise was built on Naval Base Coronado. This center, the Shore Force Training Center (SFTC), opened in September 2008 and will be the cornerstone of CNIC's vision to transform Navy installations and specifically address HSPD-5's

Two MH-60S Seahawks from Sea Combat Squadron 85 retrieve water from a lake near a wildfire in San Diego County. An MH-60S Seahawk helicopter assigned to HSC 85 dumps 420 gallons of water on wildfires burning in San Diego County. HSC-85 teamed up with the San Diego Department of Forestry and Fire Protection to help put out the wildfires blazing across Southern California. U.S. Navy photos by MC Seaman Jon Husman.

objective to ensure that all levels of the government have the capability to work efficiently and effectively together using a national approach to incident management.

To accomplish this objective the SFTC will provide an emergency management learning continuum focused on both regional and installation emergency managers and EOC personnel. This continuum will include classroom instruction, an information library, SFTC-generated individual and unit-level distributed learning, self-paced interactive computer-based war gaming scenarios and all-hazards exercise events that are scalable from the unit-level to the full CNIC enterprise.

Additionally, emergency management training and exercises will be enhanced by leveraging and incorporating realistic synthetic training methods.

"The challenge in meeting the Chairman JCS (Joint Chiefs of Staff) high interest training issues is developing a realistic training environment that matches the operational environment. The SFTC is a key capability in our CNIC adaptive enterprise that will sense and respond to unpredicted changes in the netted command and control ashore.

"It will provide the live, virtual and constructive 'hub' that will be linked to the Navy Continuous Training Environment and the Joint National Training Capability," said Randy Morgan, training and readiness program director in CNIC N7.

SFTC classroom instruction initially consists of four courses: Emergency Manager (EM); EOC Incident Management Team; Installation Training Officer (ITO); and Crisis Action Planning Team Leader. The EM course prepares an individual to be the emergency management program manager at the regional or installation level. Emphasis is on developing, coordinating and executing the Navy installation EM program within the assigned geographic area.

The Emergency Operations Center Incident Management Team course prepares individuals to serve as members of an EOC incident management team by introducing the principles, components and characteristics of a risk-based emergency management program.

Emphasis is placed on the functions of an EOC, the activation and operation of the installation's EOC in support of a disaster or emergency that includes reporting requirements, documentation and record keeping/log maintenance, and the criteria for EOC deactivation.

The ITO course provides individuals the foundation required to technically manage and execute installation training and readiness programs. Emphasis is placed on preparing the ITO to develop a strategy to provide continuous evaluation of installation training inputs, processes and outputs to assess training effectiveness and to improve training quality.

The Crisis Action Planning Team Leader course prepares the crisis action team leader to validate and assess command, control and communications (C3) training effectiveness and to provide effective feedback to improve training quality and efficiency. The instruction provides the knowledge required to technically manage and execute C3 regional training and exercise programs.

The SFTC is completely compatible with the Navy Warfare Training System process and ensures the alignment of training to mission essential tasks to meet the needs of Navy installations. The SFTC will provide a training process that supports the Shore Response Training Plan. This process will first build a solid foundation of basic training that is conducted at the individual and unit level.

Then the SFTC will provide training opportunities with multiple units and installations that are integrated. Next, using the existing exercise schedules, training and assessment will be aggressively honed and evaluated. The complexity and tempo of the training are increased for certification and sustainment.

The overall aim of the SFTC is to help facilitate the Navy Emergency Management Program mission to serve as a force multiplier and service provider, as well as support the integration of the Navy's response to emergencies across the shore force enterprise.

This purpose is compatible with Commander, Navy Installations Command Vice Adm. Conway's desire to align the shore forces' functional responsibilities and processes to support the fleet, fighter and family.

While it is true that the SFTC will train personnel to provide support for civil authorities when required, its primary focus will be on ensuring that Navy installations are prepared to shelter Navy personnel and their families and to protect Navy property during times of catastrophic emergencies.

"My intent is that Navy Installations Command will enable the Navy's operating concept through the enterprise alignment of all shore installation support to the fleet, fighter and family."

Vice Adm. Robert T. Conway Jr.
Commander, Navy Installations Command

SAN DIEGO (Oct. 23, 2007) – Gunner's Mate 3rd Class Bryan Marsh, assigned to guided-missile destroyer USS Russell (DDG 59), hands out a toy to an evacuee at the Naval Station San Diego Gym. More than 30 Russell Sailors volunteered assistance in response to the devastating wildfires in Southern California. U.S. Navy photo by Ensign Theresa Donnelly.

Capt. BJ Keepers is the shore response plan officer in CNIC N72.

Dr. Raymond Roll is the director of training for CNIC.

CHIPS

DoD ESI Celebrates its 10th Anniversary

More than $3 billion in cost avoidance achieved by ESI in first decade

By Chris Panaro

When the Department of Defense Enterprise Software Initiative (ESI) working group met for the first time in the fall of 1998, little did they know that 10 years later they would be responsible for more than $3 billion in cost avoidance for the DoD. In acknowledgment of its 10th anniversary, the ESI working group went back to some of those early ESI visionaries and some current users to get their thoughts on the initiative over the years.

ESI began as a collaborative effort among the DoD chief information officers (CIOs), but it has turned into an award-winning, DoD-wide initiative with more than 75 enterprise software agreements (ESAs) with more than 50 software publishers for thousands of software products and services.

"ESI changed how the entire department acquires and licenses commercial software," said Dave Wennergren, Deputy CIO for DoD. "Without ESI, we would never have leveraged our buying power, understood our department-wide requirements, significantly reduced the labor required to manage software licenses, or have achieved the dramatic reduction in costs of several billion dollars. I applaud the ESI team for its success and contributions over the past 10 years."

During the first DoD CIO conference in July 1998, CIOs from across the military departments and defense agencies discussed ways to reduce the amount spent across the department on commercial software. At this meeting, the CIOs made a commitment to acquire and manage commercial software as an enterprise asset, consolidate requirements, coordinate acquisitions and present a unified front to the software industry. Figure 1 on the next page illustrates the ESI timeline from its inception.

Four core goals were established to guide the ESI mission:

- Obtain buy-in for DoD enterprise-wide software agreements;
- Reduce the acquisition and support costs of software by leveraging DoD buying power;
- Provide the best, most flexible suites of Joint Technical Architecture-conforming software to the DoD enterprise; and
- Create a funding mechanism that incentivizes the use of DoD-wide software initiatives.

To guide ESI efforts, a governance structure was established to include a steering group and the ESI working group. The steering group established operating principles for ESI, and the working group carried out the ESI mission on a daily basis.

"Our core operating principles allowed us to make progress quickly and focus on tangible results rather than bureaucratic issues," said Rex Bolton, the first chairman of the ESI working group and former team leader in the Commercial IT Policies Directorate, Deputy CIO Staff, in the Office of the Assistant Secretary of Defense for Networks and Information Integration (ASD (NII)).

"Our mission was clear — we needed to save money on commercial software, and we could all do it better if we worked together. From day one, we fostered a collaborative atmosphere on the team to overcome biases and preferences and avoid duplicative effort. Good culture and teamwork were our top priorities. It was hard going at first, but with perseverance and enlightened leadership, it paid off."

"The first ESA we signed was in 1999," noted Floyd Groce, current co-chair of the ESI, team lead for enterprise IM/IT planning for the Department of the Navy CIO and part of the ESI working group since 1998.

"This set in motion our process to identify, acquire and manage enterprise software licenses and maintenance agreements on behalf of the entire DoD. Since the start, we've relied on expertise and resources contributed from across the military departments and defense agencies to serve on the virtual ESI negotiation and management team."

To help guide its effort, ESI commissioned a study to identify the best practices for the acquisition and management of enterprise software agreements within the DoD and industry. The 23 best practices yielded from this research have been used throughout the ESI tenure, guiding each negotiation and acquisition.

"In the early stages of ESI, product categories were assigned to a software product manager (SPM), who would be familiar with all the products and associated licensing practices within that category, such as databases," Bolton recalled. "The SPM would advise customers and help them negotiate more effectively for all products in that category. As we grew our inventory of enterprise agreements, the role of the SPM has become less specialized, as they manage agreements that include all assigned software companies' products, rather than just software in product categories."

Licensing experts and dedicated SPMs ensure that ESI agreements continue to provide best value to customers.

"Our best practice research dictates that we only use experienced and knowledgeable license experts in negotiating enterprise licenses," Groce said. "Our team of SPMs stays in constant contact with each other through regular team meetings to share information and lessons learned and discuss trends. They've established templates for ESAs and checklists and guides for negotiation with software publishers. To stay on top of industry trends and practices, our team regularly meets with technology providers and third party analysts."

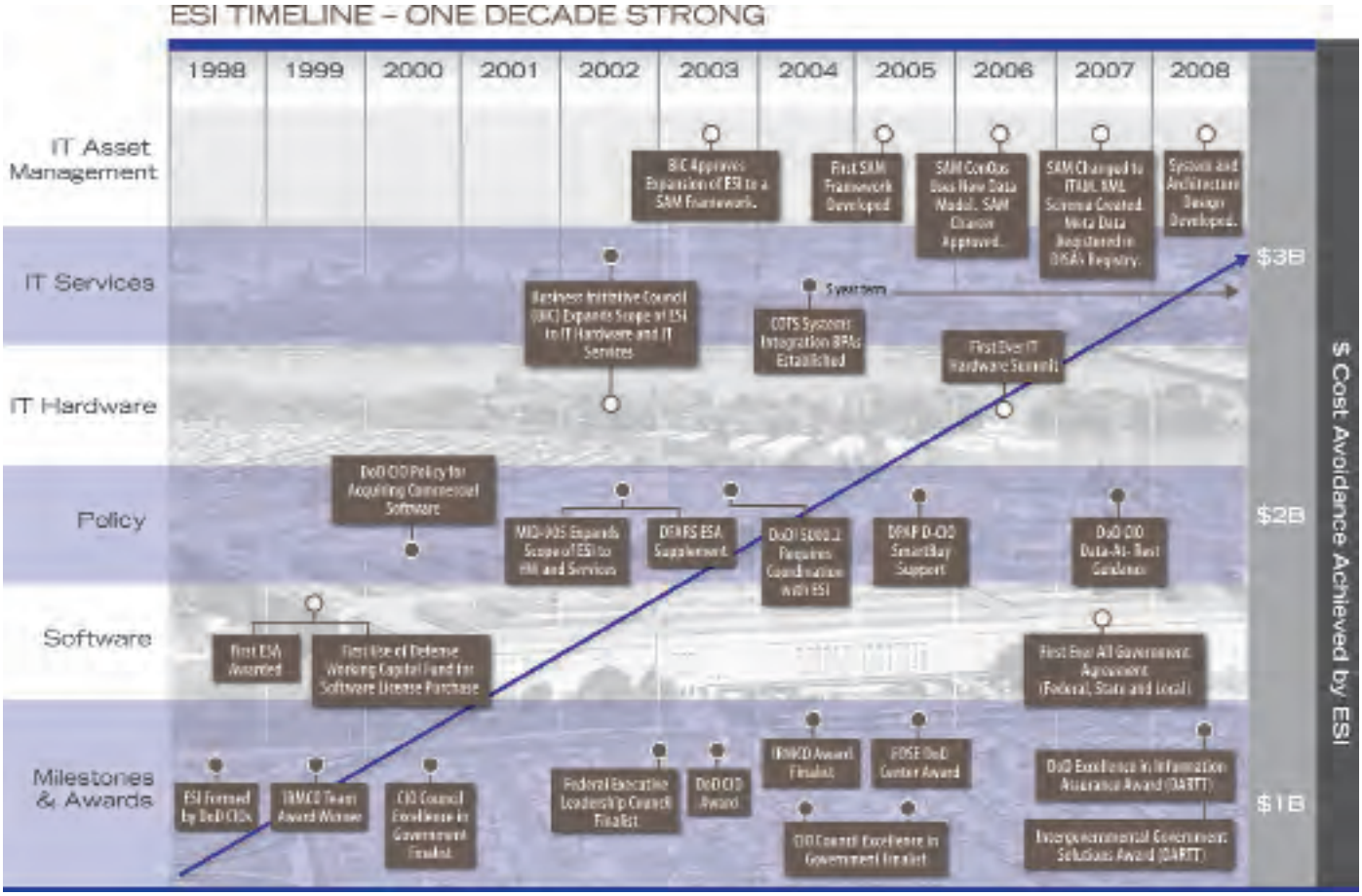


Figure 1. The ESI Timeline.

Many DoD programs have come to rely on more than 75 pre-negotiated software and service agreements, as well as an inventory of licenses, all available on the ESI Web site (www.esi.mil).

Using ESI Saves Time and Money

Many DoD programs have come to rely on more than 75 pre-negotiated software and service agreements, as well as an inventory of licenses, all available on the ESI Web site (www.esi.mil). The ESAs provide favorable terms and conditions for the department as an enterprise — not just as a one-time buyer. Most ESAs allow licenses to be transferred between users within the DoD component, and many also permit transfer of licenses across the DoD.

Almost all ESI agreements include the right to deploy needed software during a period of national emergency for a specified period of time at no extra cost. The ESA requirement for software publishers to regularly report their sales under the ESI allows DoD to identify the software it licensed through the ESA.

"Managing license inventory is the result of ESI's initial software asset management effort," said Jim Clausen, co-chair of ESI and the IT specialist for ASD (NII). "Over the years, our effort broadened to all IT assets through our ITAM (IT Asset Management) program, identifying and making available licenses and other IT assets that have been paid for but are not being used. Managing this inventory wisely through IT asset management helps satisfy requirements and avoid duplicative, wasteful purchases."

ESI leverages the DoD's Working Capital Fund to secure short-term bridge funding for purchases on a reimbursable basis. This enables a larger number of participants to take advantage of scheduled purchases, even if funds are not immediately available to that program. This facilitates more rational buying behaviors during the fiscal year and makes scheduled buying the norm rather than the exception.

Richard Cromley, director of the Contracting Services Office for the Defense Logistics Agency, has used ESI agreements repeatedly for both software and systems integration service acquisition. "The orders placed against ESI contractual instruments have definitely saved DLA dollars through reduced product prices and labor rates," Cromley said.

ESI negotiates an initial discount off General Services Administration (GSA) schedule pricing as a starting-point price level. Individual customers and program offices that use an ESI vehicle are encouraged to seek further discounts based on transactions and cumulative volume size, as well as market conditions and timing.

"The use of the ESI contractual vehicles saves time and effort of contracting personnel and reduces the procurement lead-time to acquire needed products and services," Cromley said. "The major benefit is having both pricing and usage terms

and conditions pre-negotiated with a variety of sources for both products and services."

ESI Expands to Include Hardware and Services

ESI agreements extended to include technology services and hardware in 2002 at the request of the Business Initiative Council. In a collaborative effort with DoD Enterprise Resource Planning (ERP) programs and the Office of the Secretary of Defense, the first blanket purchase agreements for information technology services were awarded for systems integration projects using commercial software packages.

"ESI did such a great job negotiating commercial software licenses that DoD leadership asked ESI to secure relationships with hardware vendors and IT service providers who implement commercial software," Bolton said.

"This coincided with the business transformation effort by DoD ERP programs spending billions of dollars to modernize DoD back-office systems. Establishing relationships with IT service providers made a lot of sense because the cost of licensing commercial software is just a fraction of the cost to get the software up and running throughout the enterprise," Bolton added.

The ESI systems integration BPAs secured more than just labor hour discounts from service providers. The BPAs incorporated commercial best practices by capturing a firm's implementation methodology and enabling fixed-price methodologies for each phase and deliverable that led to results-based pricing, not just time-based pricing.

"Having access to the systems integrators' methodology and pricing framework for a software implementation project made us much wiser buyers when it came to choosing and negotiating with an implementation partner," Cromley said.

ESI Paves the Way for Federal-wide Software Licensing

One of the most significant changes for ESI was its expansion to support the federal SmartBUY initiative. When the Office of Management and Budget (OMB) decided to create a similar initiative for the rest of the federal government through GSA in the fall of 2003, ESI participated in GSA's SmartBUY launch team to share ESI's lessons learned and best practices.

"GSA launched the SmartBUY program to leverage the software buying power of the entire federal government," said Tom Kireilis, acting deputy director of the Office of Infrastructure Optimization, in GSA's Federal Acquisition Service. "We knew that ESI achieved similar objectives for DoD and realized that the federal government could benefit from many of the disciplines and practices that ESI already had in place."

Since ESI and SmartBUY joined forces to collaborate, they have established 22 ESI/SmartBUY co-branded agreements that allow all federal agencies to procure software, leveraging the collective negotiating power of the federal government.

"OMB further raised the bar on the co-branded SmartBUY/ESI agreements when they decided in 2007 to include state and local government in the solicitations for products to protect data at rest," said Dr. Margaret Myers, former principal director for the DoD Deputy CIO. "The DoD-GSA team successfully overcame many challenges to make this happen and awarded the first-ever agreements that include state and local governments."

In September 2003, the director of Procurement and Acquisition Policy for the DoD and the DoD CIO jointly signed a SmartBUY policy to designate the DoD ESI as the implementation agent for SmartBUY throughout the DoD. This policy was updated in December 2005.

"ESI changed how the entire department acquires and licenses commercial software. Without ESI, we would never have leveraged our buying power, understood our department-wide requirements, significantly reduced the labor required to manage software licenses, or have achieved the dramatic reduction in costs of several billion dollars. I applaud the ESI team for its success and contributions over the past 10 years."

DoD Deputy CIO Dave Wennergren

ESI Achieves Central Role for IT Asset Management

From the inception of ESI in 1998, the ability to manage technology assets across the entire DoD has been a key objective. Just as investors must know and manage financial assets to be successful, the DoD must have an accurate inventory of its IT assets to make better, faster and smarter strategic sourcing decisions — and to make available ESAs that support the warfighter and ultimately help to "optimize the enterprise."

The ITAM program managed by ESI will use a net-centric service oriented architecture solution that allows DoD asset data to be pulled into a single repository that will include software and hardware (desktops, laptops, servers and routers).

Industry analysts predict that organizations that systematically manage the life cycle of their IT assets will reduce the cost per asset by as much as 30 percent in the first year and between

5 and 10 percent annually during the next five years. To make this happen, ESI provides policy and guidance and is developing a net-centric proof of concept to aggregate and report asset data.

ESI and the DoD components are working together through an ITAM integrated product team to develop a net-centric ITAM framework that will be the foundation for making components' IT asset data visible and discoverable using Web services and XML standards.

This will allow ESI to report on IT assets at the DoD and federal government level to make better decisions for current and future expenditures, as well as support the goal of lowering DoD's total cost of ownership on IT investments.

The Look Ahead

The first 10 years of ESI have proven to be very successful, and the next 10 years should yield even greater results. To do so, the ESI will need to enhance and maintain the right skill sets and knowledge given anticipated technology changes and evolving licensing and pricing models, such as software-as-a-service, software-on-demand and software capability delivered under a service oriented architecture (SOA).

"DoD ESI is essential to delivering effective and efficient information technology capability across all mission areas at least cost. ESI must continue to flourish as we transform and rely on commercial software more than ever to run the business of the DoD."

DON CIO Rob Carey

Already, the ESI is coordinating the development of net-centric software licenses to allow DoD components to share information with any potential authorized user, regardless of the user's organization. The DoD and the Office of the Director of National Intelligence (ODNI) adopted this approach to manage software licenses that give authorized IT users the license rights for immediate, unobstructed access to information. The aim is to eliminate information-sharing roadblocks, such as institutional boundaries or license limitations.

"This effort leverages the collective bargaining power of DoD and the intelligence community to ensure that our nation realizes the significant operational benefits of information sharing at a reasonable cost," Wennergren said.

The push is for a paradigm shift from the traditional model of purchasing agreements.

"A major challenge for ESI is to transition the DoD from enterprise agreements to enterprise licenses," Myers explained. "Most of the ESI agreements today work like corporate discounts: ESI negotiates the ESA and any DoD purchaser can request the DoD price. Each vendor has multiple DoD customers, so the vendors' overhead costs are included in the price the customers pay.

"If ESI could negotiate a single agreement with a single DoD point of contact, the vendors' overhead costs would be significantly reduced and DoD would avoid additional cost. ESI successfully negotiated an Oracle enterprise license for the Navy, but it took more than a year to transition all of the legacy contracts to one common license. The potential impact of doing this for all of DoD is huge, but extremely challenging," Myers concluded.

To stay ahead of these challenges, ESI will be undertaking a Lean Six Sigma effort aimed at improving DoD's software licensing processes, according to Groce. "This effort should result in streamlined and improved enterprise software licensing practices used across the entire DoD," he said.

"If ESI could negotiate a single agreement with a single DoD point of contact, the vendors' overhead costs would be significantly reduced and DoD would avoid additional cost. ESI successfully negotiated an Oracle enterprise license for the Navy, but it took more than a year to transition all of the legacy contracts to one common license. The potential impact of doing this for all of DoD is huge, but extremely challenging,"

Dr. Margaret Myers
former principal director for the DoD Deputy CIO

DON leadership support for ESI remains strong. "DoD ESI is essential to delivering effective and efficient information technology capability across all mission areas at least cost," said DON CIO Rob Carey. "ESI must continue to flourish as we transform and rely on commercial software more than ever to run the business of the DoD."

ESI's success can be attributed to the visionary leadership of the CIOs within DoD, its focused and dedicated working group, hardworking and smart SPMs, and the ability to make good things happen despite no central funding source. Congratulations to the entire ESI team and best wishes for continued success for many years to come!

For more information, go to the ESI Web site at www.esi.mil or turn to the CHIPS Under the Contracts section beginning on page 69.

Chris Panaro provides contract support to the DoD ESI.

CHIPS

Navy Ship-to-Shore via Wireless Connection

SPAWAR Systems Center Atlantic and Commander, Navy Installations Command collaborate with Joint Interoperability Test Command

By Heather Meredith, Greg Blanche, Jackie Mastin and Chris Watson

For many years, Navy ships pulling into port had to drape fiber optic "umbilical" cables over the side from the ship deck box to a pier riser for access to the shore infrastructure. Secure transport of shipboard voice and data communications from Navy ships to the Network Operations Center occurs through these cables.

But corrosion and mishandling of the cables and damage to pier risers have caused communication outages and recurring maintenance costs, and during bad weather, ship communications could be delayed for hours if not days.

But a solution to this problem is underway — the Wireless Pier Connection System. WPCS was developed by the Space and Naval Warfare Systems Center (SSC) Charleston (now realigned under SPAWAR Systems Center Atlantic) and sponsored by Commander, Navy Installations Command (CNIC).

WPCS focuses on installation effectiveness and improvements in shore installation management. This in turn reduces manpower and support costs, as well as installation costs.

Wireless Technology

The WPCS uses 802.11a and 802.11g technology to provide a reliable Wi-Fi bridge between ships and shore networks. Wi-Fi provides a viable means of extending communications between points where wired connections are restricted due to costs, difficulty, or areas where wire deployment is just not feasible, for example, in locations near airfields, or across battlefields and expanses of water. Utilizing this wireless solution, WPCS allows Navy ships to initiate connectivity to the pier while still up to three miles out at sea.

The WPCS system includes three radios located on the ship: a dedicated bridge radio, attached to an omnidirectional antenna for scanning, and two additional radios for primary and secondary connections to shore. It uses auto-configuration mesh software that facilitates a reliable and continuous connection with the shore network.

Shore-side equipment includes several BelAir wireless nodes that provide connectivity into the shore network architecture. Each WPCS system fits in a six-unit hard case and requires one electrical outlet. The size and mobility are ideal for the limited space onboard ships.

The dockside unit is movable and easily mounted. Designed for all-weather conditions, BelAir wireless nodes are water and dust-proof and can withstand temperature extremes from -40 to 122 F.

Defense-in-Depth

Security can be a problem with wireless technology. Radio frequencies can be intercepted by anyone within range with the right equipment. Because wireless nodes can allow possible unauthorized access to networks, network and data security must be incorporated into the wireless solution.

The WPCS addresses this issue with a comprehensive defense-in-depth strategy utilizing wireless security solutions that include Air Fortress Gateway devices and the AirDefense Wireless Intrusion Prevention System. Figure 1 illustrates the WPCS topology.

Type I encryption, proprietary frame structures and a specific IP assignment are used before applying 256-bit Advanced Encryption Standards (AES) layer 2 encryption. AES is the encryption standard for the U.S. government and National Security Agency.

Type 1 encryption refers to a device or system certified by the NSA for use in cryptographically securing classified U.S. government information. Type 1 certification is a rigorous process that includes testing and formal analysis of cryptographic security, functional security, tamper resistance, emissions security (EMSEC/TEMPEST) and security of the product manufacturing and distribution process. Layer 2 encryption introduces virtually no latency or overhead to the network.

Network security considerations include: MAC filtering, fixed MAC address scheme, Remote Authentication Dial In User Service (RADIUS), BelAir proprietary frame structure and WPA2 AES over-the-air encryption using Wi-Fi Protected Access Pre-Shared Key (PSK) authentication.

MAC, also known as Medium Access Control, is a sublayer of the data link layer specified in the seven-layer Open System Interconnection model (layer 2). The MAC layer addressing mechanism is called physical address or MAC address. This is a unique serial number assigned to each network adapter, making it possible to deliver data packets to a destination within a subnetwork.

Network protection features include monitoring and locating rouge nodes (rogue devices or data packets) and interference sources within the WPCS airspace. The AirDefense Enterprise Wireless Intrusion Detection System provides intrusion scanning detection with continuous alarm notification.

To comply with Defense Department policies, SSC Atlantic requested the assistance of the Defense Information Systems Agency's Joint Interoperability Test Command to assess and certify WPCS. For more than two decades, SPAWAR has partnered with JITC during the development, acceptance testing and subsequent

During the WPCS Forum at Indian Head, Md., attendees discuss topics such as the use of commercial waveforms, military frequencies and bridging devices within the DoD. At the forum, subject matter experts provide a demonstration of WPCS capabilities to Capt. Jon Kennedy, chief of the OSD Wireless Directorate.

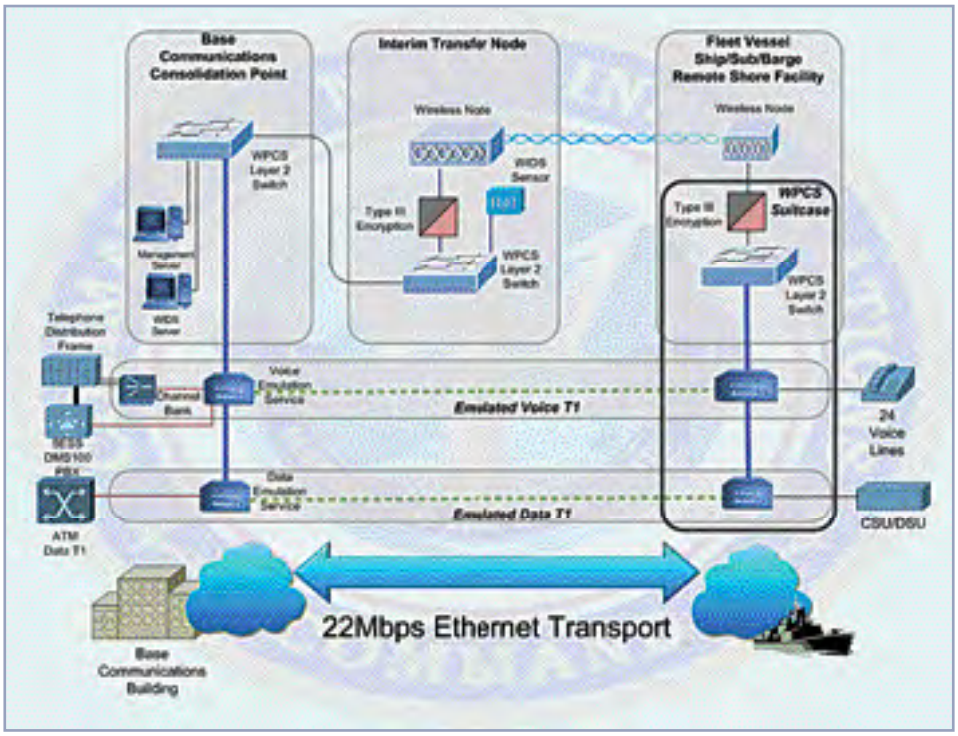


Figure 1. WPCS topology.

fielding of critical shipboard and shore-based communications systems.

As designated by the Joint Chiefs of Staff, JITC is the only DoD organization with the mandate and authority to certify that DoD IT and National Security Systems (IT/NSS) meet interoperability and net-readiness requirements for joint military operations.

To do this, JITC follows the processes outlined in Chairman of the Joint Chiefs of Staff Instruction 6212.01D, "Interoperability and Supportability of Information Technology and National Security Systems." This document establishes policies and procedures for developing, coordinating, reviewing and approving IT/NSS interoperability needs.

In addition, JITC employs testing methodologies that conform with DoD Directive (DoDD) 8500.01E, "Information Assurance" which states that all DoD information systems "shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation and availability that reflects a balance among the importance and sensitivity of the information and assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost-effectiveness."

WPCS assessment activities were conducted at the JITC Indian Head, Md., test facility from November 2007 through January 2008. During this period, JITC teamed with SSC Atlantic developers and integrators. To ensure that WPCS met DoD requirements, JITC's evaluation consisted of standards conformance, performance, interoperability and information assurance test scenarios.

During the standards conformance phase, JITC evaluated WPCS components in an isolated environment and used test equipment to generate traffic through the WPCS to ascertain whether it conforms to applicable standards contained in the Defense Information Standards Registry.

During the performance and interoperability phases, JITC integrated the WPCS into a representative DoD network, and again used unique test tools to generate traffic across the network to assess the system's ability to exchange information within an integrated architecture.

During the information assurance phase, the JITC assessment team tested WPCS security and its compliance with IA policies and requirements to allow connection to a combatant command, DoD network and the Global Information Grid.

This test effort validated that the WPCS can interoperate with both the GIG and Navy legacy messaging networks in accordance with DoD doctrine and policy. The assessment also verified that the WPCS architecture follows a robust defense-in-depth design methodology with careful attention given to maintaining a clear separation of user traffic from management traffic.

In June 2008, JITC hosted a "WPCS Forum" at the Indian Head facility with representation from the Office of the Assistant Secretary of Defense (Networks and Information Integration)/Chief Information Officer (ASD(NII)/CIO) Wireless Directorate, Office of the Chief of Naval Operations, SSC Atlantic, CNIC and NSA.

During the meeting, discussion points included DoD's use of commercial waveforms and military frequencies within wireless implementations; the use of bridging devices in the DoD; future changes to the overarching DoD wireless policy; as well as WPCS testing milestones.

JITC testers and subject matter experts also provided a demonstration of the WPCS capabilities in the JITC wireless laboratory.

At the forum, Navy Capt. Jon Kennedy, chief of the wireless directorate, stated that it appears WPCS meets all the DoD wireless local area network requirements in accordance with DoDD 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)." He indicated that the Navy should move forward with the implementation of the system.

Kennedy also encouraged JITC and the forum attendees to participate in future OSD-sponsored wireless working groups.

All attendees agreed that the recent WPCS assessment effort clearly serves as a model for future WLAN test events. As a result, SPAWAR and CNIC will continue to collaborate with JITC for the development and certification of future versions of the WPCS configuration.

Heather Meredith serves as a corporate communications support assistant to the JITC outreach director.

Greg Blanche is the lead test engineer for the WPCS interoperability assessment, as well as other wireless LAN evaluations.

Jackie Mastin is an information systems project officer within the JITC GIG infrastructure branch and test lead for WPCS interoperability test efforts.

Chris Watson is the JITC outreach director. He performs initial oversight of new programs and agreements between JITC and the DoD, federal government and industry partners.

CHIPS

Navy Warfare Training System

By U.S. Fleet Forces Command

Commanders need to understand the warfare tasks they are required to perform and the conditions and standards that govern accomplishing them.

They must train to perform tasks to complete specific steps and reach clear milestones. Those tasks are defined as Navy mission essential tasks, and captured in Navy Mission Essential Task Lists (NMETLs), the backbone of tackling tasks during mission analysis, gathering lessons learned and improving the process of producing readiness through training and other tools.

NMETLs collect a world of mission data, categorize it by who can do what and also describe the conditions in which missions take place.

This system for task accomplishment knowledge and improved decision making needs to be understood and used, according to David K. Brown, a retired naval officer who advocates the importance of NMETLs for U.S. Fleet Forces Command's training requirements and assessments branch.

"The big idea is called the Navy Warfare Training System," Brown said, explaining that the process is based on a joint training system installed in the 1990s as part of the Department of Defense training transformation.

The Navy Warfare Training System is a means of sharing the knowledge base of NMETLs, judging readiness and improving the training and readiness processes. Information from different groups pursuing training tasks can be shared and compared by using the Navy Training Information Management System.

NTIMS is an application that makes task lists and associated lessons learned within the Navy Warfare Training System more easily available.

"The application itself, NTIMS, is a Web-based application that manages NWTS for the Navy," said Rod Davis, who oversees training standards for the training requirements and assessments branch at Fleet Forces Command, which is headquartered in Norfolk, Va.

"It lets the user build a training plan and curriculum," added Bryan Nelson, a database developer assigned to Fleet Forces Command.

Earlier this year, the training requirements and assessments branch won an award from Cognos for using technology to make the process of using NMETLs more effective via the Navy Warfare Training System.

"U.S. Fleet Forces Command can tie training activities to mission essential tasks to quickly and efficiently measure the relative readiness gains for each dollar it spends on a particular training program," read the award citation.

"It's the Navy's authoritative source for NMETLs," said Mark Morrison, deputy branch head for training requirements and assessments. "It allows the fleet to document, in a consistent format, training plans and training resource requirements."

"This is all intellectual capital," Brown said. "What NTIMS does is it gives us a place to pack that intellectual capital."

Mission essential tasks are not just measurements of executing an action; they encompass the ways of accomplishing a set of tasks to standards under certain conditions. NTIMS is effectively a searchable, interactive database and library of all of those tasks and lessons learned.

Brown is the "Johnny Appleseed" of NWTS. "I call myself the 'NMETL advocate' for Fleet Forces Command," he said. "So far I've gotten away with it. The concept is so powerful, in my mind, that when I see guys wringing their hands, most of them haven't sat down to do their mission analysis."

Brown teaches the importance of using NMETLs and the Navy Warfare Training System in regular seminars aimed to make other advocates out of attendees, who will in turn spread the word. To amplify his message, Brown wears a card around his neck that prompts passers-by to ask him about NMETLs and NWTS.

"When I get going about this stuff, I usually get too excited to keep sitting down," Brown said while introducing a class at the Naval Postgraduate School Annex in Norfolk.

Brown's classes, NMETL 101 and 201, are geared toward leaders involved in mission capabilities and performance-based readiness. He said NMETLs, combined with properly updating and managing the data associated with tasks, lead to better training and, ultimately, better decisions.

"After the fall of the Soviet Union, we had to find ways to have a much more flexible and responsive force," Brown said. "What we want to show is the value we add to our commanders and the value our supporting commands add to us."

For example, training can be tailored to meet response needs to changing world situations — from responding to a natural disaster — to fighting a major war.

NMETLs, he said, "visualize the mission, value contributions, verify progress and validate courses of action. … If you get the requirements right, everything else flows from there. When we do NMETLs right, they drive training, performance and resources."

These are performance-improvement tools, Brown said. The lists help commanders understand that they do a certain task under certain conditions and meet a standard.

By incorporating lessons learned, commanders and mission planners who tackle the same task in the future benefit from the experience of others. Though they are generally used for training plans and certifications, the lists have other applications.

Brown, and Capt. Brian Barrington, formerly of Fleet Forces N72, wrote that the NWTS "really can become the Navy's performance improvement engine." CHIPS

David K. Brown of U.S. Fleet Forces Command teaches a seminar on NMETLs and the NWTS, while Barbara McCarthy, a program analyst assigned to Fleet Forces, takes notes. U.S. Navy photo.

U.S. Second Fleet Successfully Tests Modular Approach to Joint Task Force Capability During JTFEX 08-4

By Cmdr. Eric Johnson

Introduction

U.S. 2nd Fleet was the first numbered fleet to successfully test a modular command and control (C2) suite, commonly known as the 2nd Fleet Demonstrator (2FD), during July's Joint Task Force Exercise (JTFEX) 08-4.

The 2nd Fleet Demonstrator was derived from the Deployable Joint Command and Control (DJC2) concept. *(See the textbox.)*

The 2nd Fleet Demonstrator, built by the DJC2 Joint Program Office as a cooperative venture with 2nd Fleet, was an important step in demonstrating a maritime variant of the DJC2 system.

Additionally, the 2nd Fleet Demonstrator met the commander's immediate requirements for a maritime joint task force (JTF) headquarters (HQ) to train and certify as a JTF, as well as performing the JTF afloat mission.

In 2006, 2nd Fleet was tasked to begin the certification process of becoming a designated JTF Capable Headquarters to perform as a JTF or functional component headquarters staff, on behalf of a combatant commander (COCOM).

With assistance from U.S. Southern Command (SOUTHCOM), and utilizing their DJC2 system, 2nd Fleet successfully certified as a ready JTF Capable HQ in September 2007 during the SOUTHCOM-sponsored multinational exercise, Fuerzas Aliadas/PANAMAX.

Following certification, 2nd Fleet partnered with the DJC2 Joint Program Office to develop and demonstrate a modular version of the DJC2 system and its joint C2 capabilities for use on a maritime platform of the commander's choosing.

Once completed, the modularized DJC2 maritime variant, the 2nd Fleet Demonstrator, was to be tested during JTFEX 08-4 aboard the amphibious assault ship USS Bataan (LHD 5).

In July 2008, the 2nd Fleet Demonstrator was delivered, installed and completed successful testing aboard Bataan.

During JTFEX 08-4, 2nd Fleet's C2 capability provided the primary means for the commander to fight the war, and resulted in the completion of four objectives, that included the commander's JTF Capable HQ certification sustainment event, certification of the deploying strike group and 2nd Fleet's Maritime HQ accreditation.

Capabilities

The demonstrator's capabilities included a fully certified and accredited network architecture, which supported 120 laptops, with back-end capacity capable of supporting more than 700, on four networks: NIPRNET, SIPRNET, the Combined Enterprise Regional Information Exchange System (CENTRIXS), and the nongovernmental organization (NGO) Internet.

Capabilities included: VoIP phones with Defense Switch Network (DSN) access, video teleconferencing and collaboration tools: SharePoint; IBM SameTime with buttons 1 and 2; DocuShare; a Jabber server supporting chat; Global Command and Control System-Joint (GCCS-J 4.1)/Internet Common Operational Picture; and all the associated joint planning tools needed to support a JTF commander.

Flag Ship-2nd Fleet Configuration

The 2nd Fleet Demonstrator included four climate-controlled ISO (shipping) containers/modules. Two 8 by 10-foot technical control modules and two 8 by 20-foot staff modules (10 seats each) were placed in the hangar bay aboard Bataan, requiring approximately 650 square feet of space.

Due to limited funding and the proof of concept approach to the 2nd Fleet Demonstrator build, the full complement of six staff modules, a Sensitive Compartmented Information Facility (SCIF) module, a command module, and standalone power to mirror a standardized 60-seat DJC2 system, were not built.

Instead, the staff leveraged existing "green" spaces to accommodate the additional seating requirements by running a fiber connection to switching equipment located in the Landing Force Operations Center (LFOC) and other spaces on the O-2 level.

2nd Fleet utilized intelligence assets and electrical power provided by Bataan. Furthermore, while the 2nd Fleet Demonstrator was equipped with two gyro-stabilized Sea Tel Ku Band antennas, mounted forward and aft on the flight deck, a fiber connection was run to the ship's Defense Satellite Communications System (DSCS) Enhanced Bandwidth Efficient Modem (EBEM) to provide an alternate path for connectivity.

This turned out to be a valuable

Deployable Joint Command and Control Program

The DJC2 program is a Secretary of Defense and Chairman of the Joint Chiefs of Staff priority transformation initiative that is providing a standardized, rapidly deployable, scalable, and reconfigurable joint command and control (C2) and collaboration combat operations center (COC) system to geographic combatant commanders (GCCs) and component commands.

The joint force commander can use DJC2 to execute operations ranging from a first responder or small early entry forward component up to and including full joint task force (JTF) combat operation center operations. The DJC2 system provides a unique capability required by the joint warfighter that did not exist prior to its development.

The DJC2 system is net-centric from inception, has an open architecture and is fully certified (including transportability and interoperability).

More information is available at www.djc2.org.

endeavor and worth the coordination required with Naval Network Warfare Command to get a TEMPALT (temporary alteration) for the installation.

Not only did the TEMPALT provide a reliable secondary path, but it provided NETWARCOM some testing data that proved you can bypass the ship's Automated Digital Network System (ADNS) entirely, connect directly to the (satellite communications) WSC-6 antenna, and pull Defense Information Systems Network (DISN) services from a Teleport/Standard Tactical Entry Point (STEP) site.

It is important to point out that the objectives of the 2nd Fleet Demonstrator experiment assigned the primary connectivity path for the demonstrator to be via the two Sea Tel Ku Band antennas provided by Combat Direction Systems Activity, Dam Neck. These Ku-band antennas were not the engineering choice of the Joint Program Office, but borrowed as an acceptable solution and cost-saving measure.

Shore-based testing at the Virginia Advanced Shipbuilding and Carrier Integration Center, prior to the underway period, showed the Sea Tel antennas to be a reliable option; however, once underway, the reliability was less than expected.

As a result, the aft Ku-band antenna was turned off in favor of the alternate path using the Defense Satellite Communications System, leaving just one Ku-band antenna operational.

Bandwidth/Wideband Configuration

Bandwidth for Bataan and the 2nd Fleet Demonstrator was allocated autonomously. The allocation of resources for the exercise is provided below in Figure 1. Bataan was given 1.536 Mbps on the Defense Satellite Communications System, 2.048 Mbps on Commercial Wideband Satellite Program (CWSP) and 512K on the extremely high frequency (EHF) Time Division Multiple Access Interface Processor (TIP).

The 2nd Fleet Demonstrator was allocated 2.048 Mbps on the Defense Satellite Communications System and leased two 2.048 Mbps shots on Ku.

Bataan's connectivity followed traditional paths via Northwest Teleport Facility/Holmdel Commercial Land Earth Station to Naval Computer and Telecommunications Area Master Station Atlantic (NCTAMS LANT) to pull in IP and Defense Information Services Network (DISN) services that included: SIPRNET; NIPRNET; VTC capability; the Joint Worldwide Intelligence Communications System; and plain old telephone service (POTS).

The 2nd Fleet Demonstrator, on the other hand, pulled IP and DISN services via Northwest from the Joint Communications Support Element (JCSE). In this instance, the joint 2nd Fleet Demonstrator was autonomously bypassing organic Navy network systems — Bataan's ADNS via its connection to the Defense Satellite Communications System Enhanced Bandwidth Efficient Modem — to pull DISN services for SIPRNET, NIPRNET, CENTRIXS, NGO Internet and DSN from the Joint Communications Support Element.

This is important because it proves interoperability among the services and provides a means to allow any service to board an X-band capable platform, with portable baseband and network equipment, and pull DISN services from resources supported by that service,

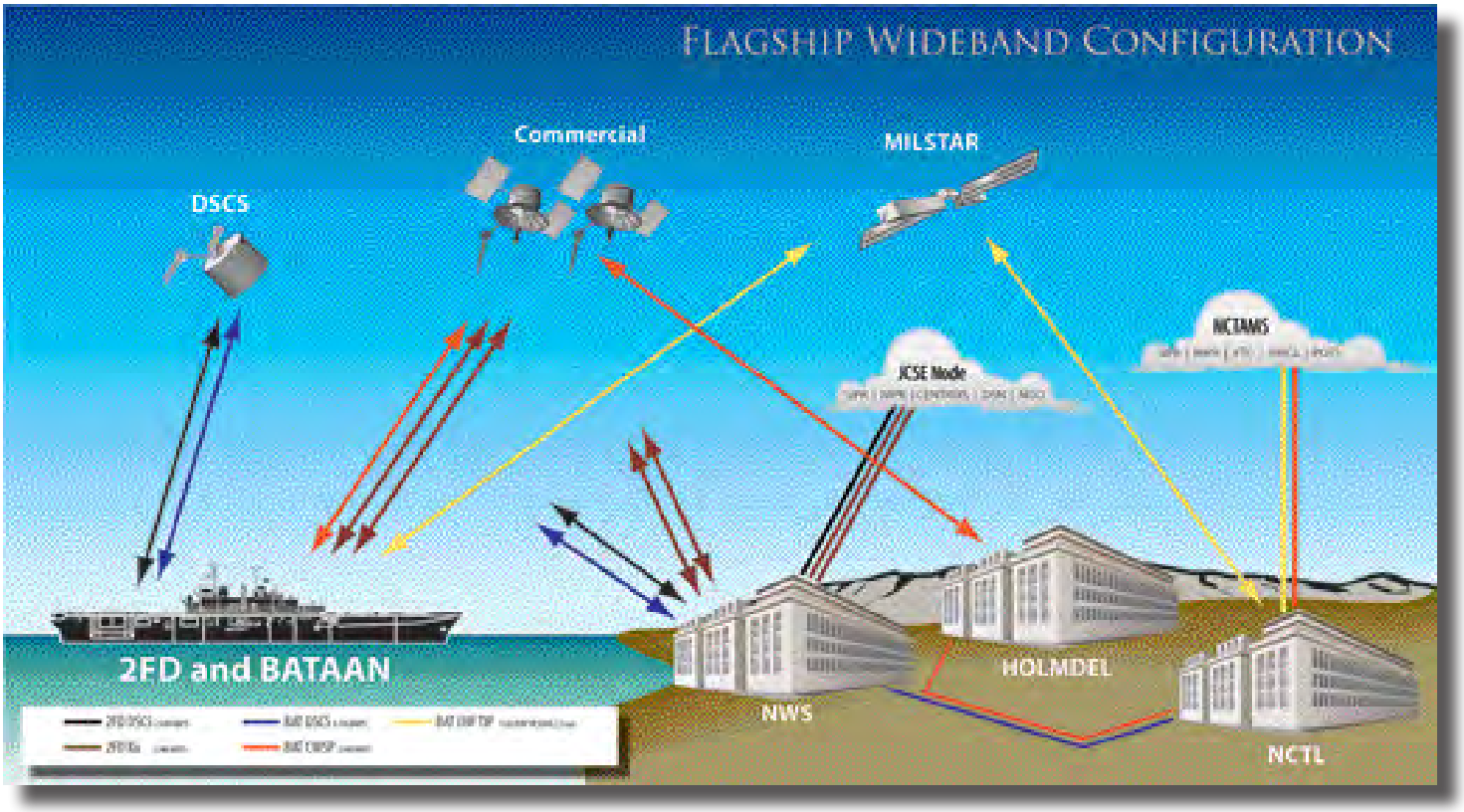


Figure 1.

without interfering with the ship's network configuration.

Conclusion

The 2nd Fleet Demonstrator delivered what the commander asked for: a modular C2 suite capable of providing the joint tools and connectivity necessary to fight the war in a maritime environment.

While the 2nd Fleet Demonstrator was space constrained, it was sufficiently robust and scalable enough, without a fully modularized 60-seat DJC2 equivalent, to be effective.

The combination of internal modular seating inside the 2nd Fleet Demonstrator and externally connected green space seating aboard Bataan proved the demonstrator's adaptability while maintaining a consistent, homogeneous environment from seat to seat regardless of location.

The 2nd Fleet Demonstrator provided a cost-effective, scalable option for the commander with significant operational flexibility, capable of deployments aboard any ship able to host its space requirements.

While the demonstrator was used to test its maritime feasibility, it could easily be moved ashore, and used as a continuity of operations enabler, during contingency operations, or during exercises to provide the commander the ability to maintain training and certification as a JTF HQ.

All in all, the 2nd Fleet Demonstrator delivered the necessary joint tools, collaboration environment and IP services needed to successfully accomplish mission objectives and prove there is value in having a modular DJC2 maritime variant to perform JTF afloat missions.

Cmdr. Eric Johnson was the deputy director of the communication and information systems directorate and a member of the Second Fleet staff during JTFEX 08-4 prior to deploying as an individual augmentee to Afghanistan.

CHIPS

Deployable Joint Command and Control (DJC2)

The DJC2 system design is based on a "Core" 60-seat configuration using open systems architecture. The system is "reconfigurable" to permit the flexible addition of new capabilities with minimum interruption to the operational system. Key components of Core system configurations may be combined for large-scale operations.

The delivered system includes four configurations:

• Rapid Response: 5/15-seat standalone, light, highly mobile C2 capability transported by 1-2 persons as carry-on/checked baggage. Provides C2 for first responders and small control teams.

• En Route: 10/20-seat pallet, with airborne C4, basic situational awareness, essential mission planning and execution. Provides C2 capability while airborne.

• Early Entry: 20/40-seat sheltered fully capable C2 with additional limited C4 capability; 72-96-hour package supporting COC operations prior to arrival of full JTF (i.e., main body). Set up and operational in less than 6 hours.

• Core: 60-seat sheltered; small JTF scales to larger JTF. Set up and operational in less than 24 hours.

The components of a fully fielded DJC2 system include: shelters; infrastructure; power; environmental control; trailers; limited communications equipment (to support en route, early entry, and rapid response operations only); government off-the-shelf (GOTS) C2 and commercial-off-the-shelf (COTS) office automation and collaboration software applications with operator workstations; displays; intercommunications; local area networks; and access to wide area networks.

DJC2 enables a geographic combatant commander (GCC) to rapidly deploy and activate (in less than 24 hours) a JTF headquarters equipped with a common C2 package with which to plan, control, coordinate, execute, and assess operations across the spectrum of conflict and domestic disaster relief. The DJC2 system provides a unique capability required by the joint warfighter that previously did not exist.

Service: Joint program with Navy as Acquisition Executive.

General Characteristics:
Primary Function: C2 solution for JTF Headquarters
Five networks: SIPRNET, NIPRNET, JWICS, CENTRIXS, NGO
Bandwidth: X Band 6.0 Mb; Ku Band 2.0 Mb
C2 Applications: GCCS-J 4.0.2 (containerized)
Collaboration: Collaborative Information Environment (CIE); Defense Collaboration Tool Suite (DCTS); Information Workspace (IWS)
VTC with plasma video display system
Intelligence: Containerized Joint Worldwide Intelligence Communications System (C-JWICS)/Joint Deployable Intelligence Support System (JDISS)
Communications: USC-60A and -68, Global Broadcast System (GBS), DRSN Phones, Intercom
Infrastructure: Tentage, tables/chairs, generators, environmental control units, cabling
Information Technology: Servers, workstations (laptops), printers, shredders, fax
Tech Support: DJC2 Operations Support Center (DOSC)
Manned 24/7 when system deployed by COCOM
Fly-away teams available for troubleshooting
DJC2 Support Portal with online access to DOSC products/processes, https://djc2.org/support
Training: Delivery and Web-based training
25 days hands-on training at COCOM
75 Web-based training modules (through portal)
Job Aids: More than 60 laminated aids and interactive electronic technical manuals available online or by CD with search feature

---

– Assistant Secretary of the Navy for Research, Development and Acquisition
http://acquisition.navy.mil/rda/home/programs/information_communications/djc2

Tackling one of the most critical and challenging questions on the battlefield

BQ+ tests coalition combat identification and air-to-ground targeting technology

By Sharon Anderson

Eglin Air Force Base in Florida hosted an advanced concept technology demonstration (ACTD) that tested and refined tactics, techniques and procedures using a variety of air-to-ground combat identification technologies designed to improve U.S. and coalition combat effectiveness and reduce the potential for battlefield fratricide.

More than 600 participants came together in the event, called Bold Quest Plus, which included units from the Air Force, Navy and Marine Corps, and coalition partners from Canada and the United Kingdom.

U.S. military units participating in this exercise included: the Air Force's 422nd Test and Evaluation Squadron, Nellis Air Force Base, Nev.; 682nd Air Support Operations Squadron, Shaw Air Force Base in S.C.; 720th Special Tactics Group, Hurlburt Field; 16th Special Operations Wing, Hurlburt Field; Navy Strike Fighter Squadron 14, Le Moore, Calif.; Marine Corps Air Development Squadron 31, China Lake, Calif.; and the Marine Corps Systems Command Target Location Designation Handoff Team, Quantico, Va.

U.S. Joint Forces Command sponsored the two-week exercise in July with the help of its Joint Fires Integration and Interoperability Team (JFIIT) and the 46th Test Wing.

BQ+ builds upon work done during last September's Bold Quest, according to John Miller, who is USJFCOM's Bold Quest Plus operational manager.

"We have had 10 nations over the last few years enter the ACTD and actively participate with forces and technologies."

Miller said the nations that have been active in the ACTD are already developing concepts. The continued interest and participation of these nations are good indications of the value of past interoperability work in these USJFCOM-sponsored events. "Quest" events began in 2001.

Coalition Participation

Essentially, U.S. and coalition nations are focused on combat identification issues for ground target engagement by coalition aircraft — especially those tools developed for aircrew and ground controllers to enable them to coordinate attacks or drop bombs on targets more quickly and effectively than they can today.

Coalition partners included the Canadian Director General Land Equipment/Director Armoured Vehicle Program Management; the 425th Squadron, Quebec, Canada; and the British Forward Air Control Team, United Kingdom.

The coalition combat identification (CCID) technologies tested during the ACTD included the Battlefield Target Identification Device (BTID), CID server, Tactical Air Control Party Close Air Support System, Target Location Designation Handoff System, Air Support Operations Center Gateway, Battlefield Air Operations Kit and the BTID-equipped Forward Air Controller (BeFAC).

"These systems and techniques enable aircrews and forward air controllers on the ground to ensure that they have identified the same target, and they are attacking the right target," Miller said.

A Battlefield Airman Targeting Micro Air Vehicle is recovered July 25 after it successfully lands during exercise Bold Quest Plus at Eglin Air Force Base, Fla. U.S. Air Force photo by Casey Bain.

This is no small feat when you consider the complex nature of combat, said Canadian Forces Lt. Cmdr. Randy Mifflin, who represented the Chief of Force Development, the sponsor for the Canadian Forces participating in BQ+.

"This is especially true in the context of ongoing joint and combined 'ops' in places such as Afghanistan, where coalition forces of differing capabilities and methods of operation are coming face-to-face with high-speed, high-tech warfare in a continuously changing and uncertain environment," Mifflin said.

"Such an environment demands fast and accurate means to discriminate between enemies, friends and neutrals to enable timely, effective and safe deployment of our weapons systems."

Under the leadership of the Chief of Force Development, Canadian Forces is working to enhance its capabilities with better training, better doctrine and improvements to the technology assisting in combat identification, according to Mifflin.

"Canada understands that it cannot achieve this goal in isolation. Coordination and interoperability with our allies and coalition partners is essential for feasible solutions. Canadian Forces has been participating in the Quest series of demonstrations investigating combat identification technology led by U.S. Joint Forces Command through the Coalition Combat Identification ACTD since 2005 to gain information and experience and build our knowledge base to reduce the risk associated with investment decisions," he said.

This year Canada's focus is on investigating the cooperative Battlefield Target Identification Device or BTID. The device uses millimeter wave technology as defined by a NATO interoperability standard to create secure ad hoc networks in near-real time with positional location information.

The ground CID picture for BQ+ was generated by BTID. BTID

is a vehicle-mounted transmitter/receiver that sends a millimeter wave via a low probability of intercept/low probability of detection signal back and forth from an air or ground platform to identify a target.

"We are examining the potential of this technology to be integrated with clearance of fire decisions in ground-to-ground and air-to-ground scenarios. To achieve this, we integrated the BTID technology in a digitized BTID-equipped forward air controller application, a future BTID Transponder Airborne Platform Surveillance System (BTAPSS) application, a BTID cruiser weapons system application, as well as our land forces command and control system," Mifflin said.

Integration with the command and control system also facilitates exploring the potential of the BTID to enhance situational awareness for the land decision maker and to provide additional capacity for coalition interoperable secure voice and data communications.

Bold Quest Plus, the Coalition Combat Identification (CCID) advanced concept technology demonstration (ACTD), will exercise a variety of technologies like the Air Support Operations Center (ASOC) Gateway pictured here in a Humvee at Eglin Air Force Base. U.S. Air Force photo by Casey Bain of the JFIIT, a subordinate, functional command of USJFCOM, tasked with improving the effectiveness of joint fires.

Air Force Support

The 46th Test Wing is the Air Force's Test and Evaluation Center for air-delivered weapons, navigation and guidance systems, and control systems, said Air Force Maj. Keith Roessig, the assistant operations officer from the 46th Test Squadron.

Within the 46th TW, the 46th Range Group supplied coalition range escorts, aircraft instrumentation pods, vehicle instrumentation and drivers, and range infrastructure support for Bold Quest Plus. Network architecture design, system integration and the operations center were provided by the 46th Test Squadron.

The Datalinks Test Facility and Air Operations Center (AOC) lab at Eglin, both part of the 46th Test Squadron Command and Control Test Facility (C2TF), supported the multi-tactical datalink and C2 environment. These unique facilities enable the creation, instrumentation, and analysis of networks required for detailed message traffic and performance data.

"Santa Rosa Island range includes the Santa Rosa Tower, a 300-foot tower, a free-standing tower, overlooking the water ranges and the Gulf to the south, and Eglin land ranges to the north. The tower contains an extensive interoperative network and is used to integrate the BeFAC system into the Eglin Bold Quest network. Range C52 is being used in support of the 422nd Test and Evaluation Squadron digital data link and JFCOM's digitally aided close air support objectives," Roessig said.

The 46th Test Squadron's robust infrastructure for BQ+ included eight command and control labs equipped with more than 200 workstations with servers running at multiple security levels representing a complete range of C2 systems and network configurations.

The combination of range and C2 infrastructure within the 46th Test Wing, which traditionally is applied to developmental test objectives, was adapted to support BQ+ to generate test quality data in an operational venue, according to Roessig.

Test control data collection and analysis were conducted from the AOC lab. The lab is configured with 90 workstations for data collection and mission observation. The AOC can host multiple networks including SIPRNET and NIPRNET.

"The AOC lab accommodates over 154 servers and three full suites of systems software to simultaneously conduct theater level operations for current test events with minimal reconfiguration yet providing connectivity over multiple operational and test IP networks for distributed testing at other Air Force and joint test sites," Roessig said.

"They have automated this performance monitoring tool that is custom designed and used for data collection to assess and evaluate applications, systems, servers and networks. Multiple tools can be used to generate the common operating picture with the systems used by the various services and coalition partners," Roessig added.

According to Miller, 15 fixed-wing aircraft participated in BQ+, including Harriers, F-18s, F-16s, F-15s and helicopters.

BTID transmitted ground pictures between platforms via the BTAPSS through to the CID server, which then pumped data up to aircraft via Link 16 or the Enhanced Position Location Reporting System (EPLRS)-based Situational Awareness Data Link.

"The goal is providing that link. That partnership between BTAPSS and the CID server gets that ground picture, that key data back into the cockpit for the pilot, the shooter. That is one route," said Canadian Army Capt. Erik Esselaar, the execution lead for the Canadian Forces that participated in BQ+.

"The second route we are working with is the BTID-equipped Forward Air Controller, BeFAC. That system is in addition to a Close Air Support System, the DACAS (Digitally Aided Close Air Support), that we are evaluating within our ranges as well. The Forward Air Controller can see the various targets and will 'lase' with the laser range finder, see where the closest friendly is through his radio system, and pass it up to the pilot," Esselaar said.

Canadian Army Maj. Michael Groh, a technical lead at BQ+, said that there are two visions for the BTAPSS to monitor the battlefield: installation on a surveillance-type aircraft, a P3 Joint Surveillance and Target Attack Radar System (JSTARS), or an unmanned aerial vehicle.

"We are working with industry to put BTID's transponder antennas in fighter aircraft on a pod so they can do a direct interrogation of the area and not rely on the combat network," Groh said.

Ultimately, the goal of the ACTD is to eliminate friendly fire casualties and equipment losses and enhance situational awareness. An effective CCID will positively identify friendly and hostile forces, neutrals and noncombatants on the modern battlefield.

This article was compiled from a live interview and articles posted on the USJFCOM (www.jfcom.mil) and Air Force Link (www.af.mil) Web sites. CHIPS

In the last installment of the Lazy Person's Guide we looked at botnets, collections of computers corrupted by malicious software, dedicated to serving the whims of shadowy masters hidden within the vast unknown of the Internet. Now that we have some understanding of what botnets are, the next steps are to examine how a computer can be transformed into an unwitting cyberspace zombie and, hopefully, how to try and defend ourselves against the Cyber-Zombie Apocalypse.

To start, take a short quiz. Please note your answers now. We'll check them as we go along.

1. Most zombie computers are:
a. PCs owned by home users
b. PCs on large organizational networks
c. PCs on small organizational networks
d. PCs owned by the botnet owner

2. Your computer is at risk of becoming infected by malware if you:
a. Open your Web browser
b. Open your e-mail application
c. Open an Adobe Acrobat PDF file
d. Both a and b

3. An application that appears useful or entertaining but installs hidden software on your PC is called:
a. Rootkit
b. Trojan horse
c. Spyware
d. MP3 player

4. In 2008, which country was allegedly the largest source of zombie PC cyber-attacks?
a. United States
b. China
c. Russia
d. Brazil

5. Which of the following is the most effective computer security strategy:
a. Whitelisting: Allow only certain specified applications to run on your system and block all others
b. Penetrate and Patch: Attack your system repeatedly until you find security holes and patch them before hackers find them
c. Educate Users: Humans are the biggest vulnerability in any information system, so provide end users with more and better security training
d. Default Permit: Route identifiable attacks away from the system and allow all other applications to run

6. True or False: Antivirus software will keep you safe from malware infection

7. True or False: It is safer to run your computer in admin mode because it gives you more control

8. True or False: A rootkit is a useful application that can give you control over the core operations of a PC

9. True or False: Blocking incoming communications from foreign IP addresses is an effective way to defend your organization from cyber attacks

10. True or False: You will have a more secure system by adopting new technology as soon as it comes out – before hackers have a chance to find vulnerabilities

Bonus question: In 2004, what key change was made in the default settings of Windows XP?

Now, let's see how you did.

Uncle Zombie Wants You

And Uncle Zombie likes them big. The answer to No. 1 is c. Yes, home PCs may get infected daily, but it requires defeating the firewall on each computer. Networks represent a much higher return on the attack investment, and the larger they are, the better. There might be one or more computers on a home local area network, but that's slim pickings for a botnet that needs thousands of drones to be a real threat. However, if malware penetrates an organization's firewall it has hundreds, if not thousands, of targets to try and enlist to its cause.

No. 2 is tricky. I can remember back to a halcyon time when just opening an e-mail did not put you at risk of infection. At this time, Web pages were handcrafted line by line using Notepad and not by a scripting language that waits to load nasty stuff on your computer. However, you still cannot get infected just by opening an application — you have to open content from an external source to be at risk. So, the answer to No. 2 is c.

Adobe Portable Document Format files, generally considered safe and reliable for years, have been used as malware delivery platforms. If you're using a version of Adobe Reader earlier than version 8.1.2, for example, you may be vulnerable to PDFs carrying the Trojan.Zonebac which lowers Microsoft Internet Explorer security settings. *(Go to http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0655 for more information.)*

If PDF files are not safe, is anything? No, not really. You can get malware from graphics files, music files, document files and pretty much anything else capable of carrying a form of executable code. If you want a truly frightening picture of the ratio of bad to good applications, take a look at the list your antivirus software uses to identify malicious code.

A well-developed antivirus program will probably list at least 75,000 different dangerous items that it needs to keep out of our computers. On the other hand, we probably run only a few dozen "good" applications and maybe a few hundred useful bits of mobile code from Web sites. With that ratio of crud in mind it is not a stretch to say that the Internet may be more like a sewer system than a highway.

And the really disheartening part? There are more than 75,000 malware variants running loose, so if you are depending solely on antivirus software to keep you safe I wish you good luck. You will need it. *(That's giving away the answer to No. 6 a little early.)*

Beware of Geeks Bearing Gifts

The answer to No. 3 is b. It may look like a calculator. It may act like a calculator. But that cute calculator application adorned with tiny flying ponies that you downloaded from the Internet in hopes of luring your 6 year-old into a state of mathematical genius might really be a horse — a Trojan horse.

While rootkits *(discussed later)* and spyware *(discussed in the last issue at www.chips.navy.mil/archives/08_Jul/web_pages/botnets.html)* are not nice things to have on your computer, a Trojan horse is a sweet candy coating for something infectious on the inside. Beware of anything you can get for free — it might be worth less than you paid for it.

MP3 players are marginally less evil, but we can discuss their insidious effects the next time we look at forms of computer-mediated addiction.

Trojan horses, like their mythical Greek namesake, rarely carry anything good. When that innocent-looking calculator application triggers a security alert during installation, your computer will ask for permission to complete the job. There is usually a good reason for the computer to ask because the application is asking the computer to let it change things deep in the computer's cerebral cortex.

At this point, it is up to the operator to exercise good judgment and question why a calculator application needs to make changes to the Registry. Unfortunately, too many people inadvertently load bad stuff on their PCs, or use obsolete or *unpatched* software that allows malware on the system, thus contributing more zombies to the botnet army.

The first three questions should lead you to the answer to No. 4. If you know what country has the largest organizational networks, uses massive amounts of information daily, and whose populace is easily distracted by bright shiny computer-like objects, then the only logical answer is a, the United States.

Earlier this year, a company named SecureWorks published a report about the source of cyber attack attempts against its clients. At the top of the list was the United States, which hosted 20.6 million attack attempts. China was a distant second with 7.7 million, followed in descending order by Brazil, South Korea, Poland, Japan, Russia, Taiwan, Germany and Canada, which racked up between 100,000 and 200,000 each.

However, the last eight together only totaled around 1.6 million attacks, far short of either China or the United States, and more attacks were launched from U.S. computers than the rest of these nations combined. If you knew the answer to No. 4 then I am hoping you also got No. 9 correct.

The last of our multiple choice questions offers several strategies of varying attractiveness.

"Default Permit," or "Everything, not explicitly forbidden, is permitted," only works if you can identify every possible threat to your system. Like my earlier indictment of antivirus software, any new attack not in the profile list will walk right in and make itself at home.

"Penetrate and Patch" is a security approach used by many in the computer industry. We have been doing this for decades. We still do P&P, and therein is the problem. *If it were an effective way to secure our systems, why do we still need to keep doing it?*

Even if we could find all the holes in a particular system, as soon as we upgrade or replace software new groups of hidden vulnerabilities emerge. Granted, penetration testing is useful, but only if you, or the people you hire, are more skilled than the people trying to compromise your system.

"Educating Users" suffers from the same lack of results. Every year, millions of computer users in the United States take computer security training mandated by their organizations. Does it help? Well, according to SecureWorks' report, we have more attacks coming from infected PCs here in the U.S. These infected PCs serve as platforms (bots) that launch cyber attacks worldwide. So educating users, which is still something we should do, does not appear to be stemming the tide.

That leaves "Whitelisting" which is how most secure computers operate today. A whitelist is a list of accepted items or persons in a set. The list is inclusionary, confirming that the item being analyzed is acceptable. An e-mail whitelist is a list of contacts that the user deems are acceptable to receive e-mail from. Spam filters that come with e-mail clients have both white and blacklists of senders and keywords to look for in e-mails.

No one should be running in a mode where they can load software or change key system settings as a matter of routine. If you need to install new applications, turn off anything that might attract malware, log in as "admin" and make your changes, and then go back to running in a safer mode. This answers No. 7 a little early, but running your PC in admin mode only makes you more vulnerable to infection. Do not do it.

If you want to see an early description of whitelisting I will wind up the Wayback Machine to an article on computer security published in CHIPS almost 12 years ago at www.chips.navy.mil/archives/97_jan/file6.htm. It took many years for computer security to gain enough traction to be considered more than an inconvenience. For example, it was not until 2004 that most PCs were sold with the firewall turned on as a default setting instead of leaving it up to the user. And yes, that is the answer to the bonus question.

Got Root?

Since we have already discussed the answers to No. 6 (False) and No. 7 (False), let us move on to No. 8, which is True. A rootkit is a useful application for someone trying to hack into a system to gain control at the "root" level of a computer.

Early rootkits were developed to allow Unix administrators to take control of unresponsive systems and gain root access to the system, thus the name. However, they quickly became tools for hackers who wanted to gain administrative privileges and hide their activities from a system's legitimate owners. A rootkit can be a tool or a weapon depending on how it is employed.

Modern rootkits are like submarines: Their job is to disappear into the system and become invisible. In addition, they can also conceal the activities of other programs, like botnet applications or spyware. Rootkits can be difficult to find, particularly if

you are searching while the rootkit is running. The only reliable way is to shut down the system and reboot from a CD or write-protected external drive. The rootkit cannot hide itself if it is not running.

The only reliable way to *cure* a rootkit infection is to re-install the operating system and applications. If you save the data files, scan them until they are sterile to avoid re-infection. Make sure the firewall is on, never surf the Internet in admin mode, and never allow anything to install that needs administrative privileges unless you are very certain of what it will do.

Man the Barricades

Now to No. 9 which is False. If you remember that most zombie attacks appear to originate here in the U.S.A., blocking incoming packets from foreign IP addresses might stop a little over a third of the attacks. But what you really want is control over outgoing packets, particularly those heading to foreign IP addresses. Regardless of where the zombies are located, there is some consensus that the people operating botnets live in countries with lax law enforcement regarding computer crime, and possibly some countries may even encourage these nefarious activities.

While an infected PC might still be getting instructions from a foreign source, it will be far less effective if it cannot report back to its new master. Outgoing traffic, particularly to sites no one has actually visited, might be a sign that there are infected PCs inside the firewall.

No. 10 is False. Computer history is littered with the virtual bodies of early adopters who embraced version 1.0 (or beta versions) of an application, only to find that they had acquired the computer security equivalent of a cardboard flak jacket. Unfortunately, there are people who want the newest, brightest and "bestest" toys right now. Please resist the urge to rush a new system into operation unless there really is no other choice.

Malware Symptoms

How can you tell if your computer has been infected? Here are some typical symptoms:

• You get pop-ups at random when you are not searching the Internet.

• You get a *funny* video in e-mail and when you double click on it you get a security warning. When you click OK to let the video run, nothing happens.

• You click on a link in search results and immediately get pop-ups. You close the pages but get error messages.

• Your computer runs slowly and when you check system activity you see unexplained memory, central processing unit, or network bandwidth consumption.

• Your computer is sending or receiving data *(indicated by constantly blinking lights on your modem or router)* even though you do not have a browser, e-mail or other Internet program open.

Essentially, any time your computer does something that you did not tell it to do, you should be suspicious. Granted, the last example could be some type of auto-update program, but any reputable updater application should issue an alert and *ask* permission before proceeding.

We looked at Trojan horses earlier, but it also might be useful to look at the differences between a virus, worms and Trojans.

A computer virus is executable code that attaches itself to a executable file and is activated when a user runs the file it is attached to. Viruses range from annoying *(displaying a joke message at a set time)* to dangerous *(damage to your system or files*). Because almost all viruses are attached to executable files they generally cannot infect a computer until a user runs or opens the host file.

Please note that a virus cannot be spread without a human action such as running an infected program or e-mailing an infected file.

A computer worm is similar to a virus, with one important difference: It can travel without any help from users. Worms take advantage of the various file and information transport features on computers and networks to travel. Once a worm is active it can send thousands of copies of itself to any target it can find.

A common worm tactic is to e-mail itself to everyone in a user's e-mail address book, or just wait until an e-mail is sent. This feature can also help us detect worms because if they are too active and consume too many system resources, we may notice loss in memory or an increase in bandwidth consumption.

A worm may install a Trojan, or a Trojan may carry a worm or virus. While worms try to operate below the radar, Trojans can be more effective because they attempt to trick the system user instead of the built-in security of the system. Sadly, it seems that humans are easier to fool than computers.

Another infection method that deserves a look is the "Drive-by Download." This happens without knowledge of the user and occurs by visiting a Web page with malicious code, viewing an infected e-mail or clicking on a deceptive pop-up. The page may have only been open for a few seconds and nothing was installed, but if the code is there, and the browser is vulnerable, the computer can be compromised.

You do not even have to visit questionable Web sites to be attacked by a drive-by. In addition to looking for new PCs to infect, hackers probe legitimate corporate and government Web sites scouting for vulnerabilities to try to upload malicious code that will attack PCs that visit those sites.

Closing Words

The global reach of the Internet provides great opportunities. But leaving your network or computer vulnerable to people in faraway places who will cheerfully add your computer to their botnet without caring what damage they may do along the way can have catastrophic consequences, but if you do some fairly simple, sensible things, you can be safe.

So enjoy the Internet, but remember the words of President Ronald Reagan — "Trust, but verify."

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 resources management from the Air Force Institute of Technology. He currently serves as a telecommunications manager in the 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.

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:

Asset Discovery Tools

Belarc

Belmanage Asset Management - Provides software, maintenance and services.

Contractor: ***Belarc Inc.*** (W91QUZ-07-A-0005)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 30 Sep 11

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0005

BMC

Remedy Asset Management - Provides software, maintenance and services.

Contractor: ***BMC Software Inc.*** (W91QUZ-07-A-0006)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 29 May 09

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0006

Carahsoft

Opsware Asset Management - Provides software, maintenance and services.

Contractor: ***Carahsoft Inc.*** (W91QUZ-07-A-0004)

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components and authorized contractors.

Ordering Expires: 19 Nov 09

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0004

DLT

BDNA Asset Management - Provides asset management software, maintenance and services.

Contractor: ***DLT Solutions Inc.*** (W91QUZ-07-A-0002)

Authorized Users: This BPA has been designated as a GSA SmartBUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

Ordering Expires: 01 Apr 13

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0002

Patriot

BigFix Asset Management - Provides software, maintenance and services.

Contractor: ***Patriot Technologies Inc.*** (W91QUZ-07-A-0003)

Authorized Users: This BPA has been designated as a GSA SmartBUY and is open for ordering by all Department of Defense (DoD) components, authorized contractors and all federal agencies.

Ordering Expires: 08 Sep 12

Web Link: https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-07-A-0003

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.*** (W91QUZ-04-A-0002)

Ordering Expires: Upon depletion of Army Small Computer Program (ASCP) inventory

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/

www.it-umbrella.navy.mil

Mercury

Mercury Software - Provides software licenses, training, technical support and maintenance for Mercury Performance Center, Mercury Quality Center, Mercury IT Governance Center and Mercury Availability Center.

Contractor: ***Spectrum Systems, Inc.*** (SP4700-05-A-0002)

Ordering Expires: 21 Feb 09

Web Link: http://www.spectrum-systems.com/contracts/esi-hp.htm

COTS Systems Integration Services

COTS Systems

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

Contractors:

Accenture LLP (N00104-04-A-ZF12); (703) 947-2059

BearingPoint (N00104-04-A-ZF15); (703) 747-8854

Computer Sciences Corp. (N00104-04-A-ZF16); (856) 988-4505

Deloitte Consulting LLP (N00104-04-A-ZF17); (571) 480-7272

IBM Corp. (N00104-04-A-ZF18); (703) 424-7581

Ordering Expires: 03 May 09

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

Database Management Tools

Microsoft Products

Microsoft Database Products - See information under Office Systems on page 74.

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 the Navy project manager.

Contractors:

Oracle Corp. (W91QUZ-07-A-0001); (703) 364-3351

DLT Solutions (W91QUZ-06-A-0002); (703) 708-9107

immixTechnology, Inc. (W91QUZ-08-A-0001); Small Business; (703) 752-0632

Mythics, Inc. (W91QUZ-06-A-0003); (757) 284-6570

Ordering Expires:

Oracle: 30 Sep 11
DLT: 1 Apr 13
immixTechnology: 26 Aug 11
Mythics: 18 Dec 11

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

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 the NAVICP Mechanicsburg contracting officer at (717) 605-3210 for further review of the requirements and coverage.

This license is managed by the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Pacific 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: 30 Sep 09

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 Application Integration

BEA

BEA Products - Supplies integration and service-oriented architecture (SOA) software including: BEA WebLogic Server; BEA WebLogic Portal; BEA WebLogic Integration; BEA WebLogic Workshop; BEA JRockit; BEA AquaLogic; BEA Tuxedo and other BEA products.

Contractors:

CompSec (Computer Security Solutions, Inc.) (N00104-07-A-ZF43); Small Business; (703) 917-0382

immixTechnology, Inc. (N00104-07-A-ZF41); Small Business; (703) 752-0657

Merlin International (N00104-07-A-ZF42); Small Business; (703) 752-8369

Ordering Expires: 19 Dec 09

Web Links:

CompSec
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/CompSec/index.shtml
immixTechnology
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/immix/index.shtml
Merlin International
http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/Merlin/index.shtml

Sun Software - NEW!

Sun Products - Provides Sun Java Enterprise System (JES) and Sun StarOffice. Sun JES products supply integration and service-oriented architecture (SOA) software including: JES Identity Management Suite; JES Communications Suite; JES Availability Suite; JES Web Infrastructure Suite. Sun StarOffice supplies a full-featured office productivity suite.

Contractors:

Commercial Data Systems, Inc. (N00104-08-A-ZF38); Small Business; (619) 569-9373

Dynamic Systems, Inc. (N00104-08-A-ZF40); Small Business; (801) 444-0008

World Wide Technology, Inc. (N00104-08-A-ZF39); Small Business; (301) 731-8105

Ordering Expires: 24 Sep 12

Web Link:

http://www.it-umbrella.navy.mil/contract/enterprise/application_integration/SUN/index.shtml

Enterprise Architecture Tools

IBM Software Products

IBM Software Products - Provides IBM product licenses and maintenance with discounts from 1 to 19 percent off GSA pricing. On June 28, 2006, the IBM Rational Blanket Purchase Agreement (BPA) with immixTechnology was modified to include licenses and Passport Advantage maintenance for IBM products, including: IBM Rational, IBM Database 2 (DB2), IBM Informix, IBM Trivoli, IBM Websphere and Lotus software products.

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

Ordering Expires: 26 Mar 09

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: 22 Sep 09

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 Nov 08 (Call for extension information.)

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

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); (980) 776-8283

Ordering Expires: 30 Nov 08 (Please call for information about follow-on contract.)

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 software product provides the enterprise with a suite of solution specific applications for Capital Planning and Investment Control (CPIC) Budgeting (OMB 300/53); CPIC Process (Select/Control/Evaluate); IT Governance; FISMA (Federal Information Security Management Act) and Privacy Compliance; Project Portfolio Management; Application Rationalization; Research and Development (R&D) and Product Development; Asset Management; Grants Management; Vendor and Service Level Agreement Management; and Regulatory Compliance. ProSight products have been designated as a DoD ESI and GSA SmartBUY. 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 pricing, which is inclusive of software accumulation discounts. For maintenance, training and installation services, discount range is 3 to 10 percent off GSA pricing. Credit card orders are accepted.

Contractor: ***ProSight, Inc.*** (W91QUZ-05-A-0014); (503) 889-4813

Ordering Expires: 19 Sep 11

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

Quest Products

Quest Products - Provides Quest software licenses, maintenance, services and training for Active Directory Products, enterprise management, ERP planning support and application and database support. Quest software products have been designated as a DoD ESI and GSA SmartBUY. *ONLY* Active Directory Products have been determined to be the best value to the government and; therefore, competition is not required for Active Directory software purchases. Discount range for software is from 3 to 48 percent off GSA pricing. For maintenance, services and training, discount range is 3 to 8 percent off GSA pricing.

Contractors:

Quest Software, Inc. (W91QUZ-05-A-0023); (301) 820-4800

DLT Solutions (W91QUZ-06-A-0004); (703) 709-7172

Ordering Expires:

Quest: 14 Aug 10

DLT: 01 Apr 13

Web Links:

Quest

https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-05-A-0023

DLT

https://ascp.monmouth.army.mil/scp/contracts/viewcontract.jsp?cNum=W91QUZ-06-A-0004

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. (N00104-07-A-ZF48); Small Business Disadvantaged; (301) 352-7878, ext. 116

Spectrum Systems, Inc. (N00104-07-A-ZF46); Small Business ; (703) 591-7400

Ordering Expires:

Bay State Computer, Inc.: 14 Aug 10

Spectrum Systems, Inc.: 31 Jul 10

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 installation, maintenance, training and professional services.

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

Ordering Expires: 31 Aug 10

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 70.*

RWD Technologies

RWD Technologies - Provides a broad range of integrated software products designed to improve the productivity and effectiveness of end users in complex operating environments. RWD's Info Pak products allow you to easily create, distribute and maintain professional training documents and online help for any computer application. RWD Info Pak products include Publisher, Administrator, Simulator and OmniHelp. Training and other services are also available.

Contractor: ***RWD Technologies*** (N00104-06-A-ZF37); (609) 937-7628

Ordering Expires: Effective for term of the GSA FSS Schedule

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

SAP- NEW Contractors!

SAP Products - Provides software licenses, software maintenance support, information technology professional services and software training services.

Contractors:

SAP Public Services, Inc. (N00104-08-A-ZF41); Large Business; (202) 312-3515

Advantaged Solutions, Inc. (N00104-08-A-ZF42); Small Business; (202) 204-3083

Carasoft Technology Corporation (N00104-08-A-ZF43); Small Business; (703) 871-8583

Oakland Consulting Group (N00104-08-A-ZF44); Small Business; (301) 577-4111

Ordering Expires: 14 Sep 13

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

Information Assurance Tools

Data at Rest Solutions BPAs offered through ESI/SmartBUY

The Office of Management and Budget, Defense Department and General Services Administration awarded multiple contracts for blanket purchase agreements (BPA) to protect sensitive, unclassified data residing on government laptops, other mobile computing devices and removable storage media devices.

These competitively awarded BPAs provide three categories of software and hardware encryption products — full disk encryption (FDE), file encryption (FES) and integrated FDE/FES products. All products use cryptographic modules validated under FIPS 140-2 security requirements and have met stringent technical and interoperability requirements.

Licenses are transferable within a federal agency and include secondary use rights. All awarded BPA prices are as low as or lower than the prices each vendor has available on GSA Schedules. The federal government anticipates significant savings through these BPAs. The BPAs were awarded under both the DoD's Enterprise Software Initiative (ESI) and GSA's governmentwide SmartBUY programs, making them available to all U.S. executive agencies, independent establishments, DoD components, NATO, state and local agencies, foreign military sales (FMS) with written authorization and contractors authorized to order in accordance with the FAR Part 51.

Service component chief information officers (CIO) are currently developing component service-specific enterprise strategies. Accordingly, customers should check with their CIO for component-specific policies and strategies before procuring a DAR solution. The Department of the Navy, Army and Air Force will be releasing service-specific DAR guidance for their personnel to follow. Go to the ESI Web site at www.esi.mil for more information.

As of press time, DoD users are not authorized to purchase DAR software because service-specific guidance has not been issued. DON users are not authorized to purchase a DAR solution until the DON CIO has issued an enterprise solution for purchasing DAR software.

Mobile Armor – ***MTM Technologies, Inc.*** (FA8771-07-A-0301)

Safeboot/McAfee – ***Rocky Mountain Ram*** (FA8771-07-A-0302)

Information Security Corp - ***Carahsoft Technology Corp.*** (FA8771-07-A-0303)

Safeboot/McAfee – ***Spectrum Systems*** (FA8771-07-A-0304)

SafeNet, Inc. – ***SafeNet, Inc.*** (FA8771-07-A-0305)

Encryption Solutions, Inc. – ***Hi Tech Services, Inc.*** (FA8771-07-A-0306)

Pointsec/Checkpoint – ***immix Technologies*** (FA8771-07-A-0307)

SPYRUS, Inc. – ***Autonomic Resources, LLC*** (FA8771-07-A-0308)

WinMagic, Inc. – ***Govbuys, Inc.*** (FA8771-07-A-0310)

CREDANT Technologies – ***Intelligent Decisions*** (FA8771-07-A-0311)

GuardianEdge Technologies – ***Merlin International*** (FA8771-07-A-0312)

Ordering Expires: 14 Jun 12 (If extended by option exercise.)

Web Link: http://www.esi.mil

McAfee

McAfee - Provides software and services in the following areas: Anti-Virus; E-Business Server; ePolicy Orchestrator; GroupShield Services; IntruShield; Secure Messaging Gateway and Web Gateway.

Contractor: ***En Pointe*** (GS-35F-0372N)

Ordering Expires: 12 Dec 09

Web Link: http://www.esi.mil

Antivirus Web Links: Antivirus software available at 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: https://www.jtfgno.mil/antivirus/av_info.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Securify

Securify - Provides policy-driven appliances for network security that are designed to validate and enforce intended use of networks and applications; protects against all risks and saves costs on network and security operations. Securify integrates application layer seven traffic analysis with signatures and vulnerability scanning in order to discover network behavior. It provides highly accurate, real-time threat mitigation for both known and unknown threats and offers true compliance tracking.

Contractor: ***Patriot Technologies, Inc.*** (FA8771-06-A-0303)

Ordering Expires: 04 Jan 11 (if extended by option exercise)

Web Link: http://www.esi.mil

Symantec

Symantec - Symantec products can be divided into 10 main categories that fall under the broad definition of Information Assurance. These categories are: virus protection; anti-spam; content filtering; anti-spyware solutions; intrusion protection; firewalls/VPN; integrated security; security management; vulnerability management; and policy compliance. This BPA provides the full line of Symantec Corp. products and services consisting of over 6,000 line items including Ghost and Brightmail. It also includes Symantec Antivirus products such as 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; and support.

Contractor: ***immixGroup*** (FA8771-05-0301)

Ordering Expires: 12 Sep 10

Web Link: http://var.immixgroup.com/contracts/overview.cfm or www.esi.mil

Notice to DoD customers regarding Symantec Antivirus Products:

A fully funded and centrally purchased DoD enterprise-wide antivirus and spyware software license is available for download to all Department of Defense (DoD) users who have a .mil Internet Protocol (IP) address.

Contractor: ***TVAR Solutions, Inc.***

Antivirus Web Links: Antivirus software can be downloaded at no cost by linking to either of the following Web sites:

NIPRNET site: https://www.jtfgno.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: 30 Nov 08 (Call for extension information.)

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

Lean Six Sigma Tools

iGrafx Business Process Analysis Tools

iGrafx - Provides software licenses, maintenance and media for iGrafx Process 2005 and 2006; Six Sigma and iGrafx Flowcharter 2005 and 2006; iGrafx Process for Six Sigma 2007; iGrafx Flowcharter 2007; Enterprise Central; and Enterprise Modeler.

Contractors:

Softchoice (N00104-06-A-ZF40); (416) 588-9002 ext. 2072

Softmart (N00104-06-A-ZF39); (610) 518-4292

Software House International (N00104-06-A-ZF38); (732) 564-8333

Authorized Users: Open for ordering by all Department of Defense (DoD) components, U. S. Coast Guard, NATO, Intelligence Community and authorized DoD contractors.

Ordering Expires: 30 Nov 08 (Please contact project management for extension Information.)

Web Links:

Softchoice
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softchoice/index.shtml
Softmart
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/softmart/index.shtml
Software House International
http://www.it-umbrella.navy.mil/contract/enterprise/iGrafx/shi/index.shtml

Minitab

Minitab - Provides software licenses, media, training, technical services and maintenance for products including Minitab Statistical Software, Quality Companion, and Quality Trainer. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: ***Minitab, Inc.*** (N00104-08-A-ZF30); (800) 448-3555 ext. 311

Authorized Users: This BPA is open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community and authorized DoD Contractors.

Ordering Expires: 07 May 13

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

PowerSteering - NEW!

PowerSteering - Provides software licenses (subscription and perpetual), media, training, technical services, maintenance, hosting and support for PowerSteering products: Software-as-a-Service solutions to apply the proven discipline of project and portfolio management in IT, Lean Six Sigma, Project Management Office or any other project-intensive area and to improve strategy alignment, resource management, executive visibility and team productivity. It is the responsibility of the ordering officer to ensure compliance with all fiscal laws prior to issuing an order under a BPA, and to ensure that the vendor selected represents the best value for the requirement being ordered (see FAR 8.404).

Contractor: ***immixTechnology, Inc.*** (N00104-08-A-ZF31); Small Business; (703) 752-0661

Authorized Users: All DoD components, U.S. Coast Guard, NATO, Intelligence Community, and authorized DoD Contractors.

Ordering Expires: 14 Aug 13

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

Office Systems

Adobe

Adobe Products - Provides software licenses (new and upgrade) and upgrade plans (formerly known as maintenance) for numerous Adobe and formerly branded Macromedia products, including Acrobat (Standard and Professional); Photoshop; Encore; After Effects; Frame Maker; Creative Suites; Illustrator; Flash Professional; Dreamweaver; Cold Fusion and other Adobe products.

Contractors:

ASAP (N00104-08-A-ZF33); Small Business; (800) 248-2727, ext. 5303

CDW-G (N00104-08-A-ZF34); (703) 621-8211

GovConnection, Inc. (N00104-08-A-ZF35); (301) 340-3861

Insight Public Sector, Inc. (N00104-08-A-ZF36); (301) 261-6970

Ordering Expires: 30 Jun 10

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

Four Blanket Purchase Agreements (BPAs) provide both new and upgrade software licenses for Adobe products. These agreements also provide Adobe software upgrade plans, formerly known as maintenance agreements. The BPAs include software licenses formerly known under the Macromedia product brand. Products include: Acrobat (Standard and Professional); Photoshop; Encore; After Effects; Frame Maker; Creative Suites; Illustrator; Flash Professional; Dreamweaver; Cold Fusion; and other Adobe products.

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); (877) 890-1330

Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 37010 or (512) 723-7010

GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI or (703) 502-2959

Hewlett-Packard (N00104-02-A-ZE80); (800) 535-2563 pin 6246

Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638

Softmart (N00104-02-A-ZE84); (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

Ordering Expires: 31 Mar 10

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

Red Hat/Netscape/Firefox

Through negotiations with August Schell Enterprises, DISA has established a DoD-wide enterprise site license whereby DISA can provide ongoing support and maintenance for the Red Hat Security Solution server products that are at the core of the Department of Defense's Public Key Infrastructure (PKI).

The Red Hat Security Solution includes the following products: Red Hat Certificate System and dependencies; Red Hat Directory Server; Enterprise Web Server (previously Netscape Enterprise Server); and Red Hat Fortitude Server (replacing Enterprise Server).

August Schell also provides a download site that, in addition to the Red Hat products, also allows for downloading DISA approved versions of the following browser products: Firefox Browser; Netscape Browser; Netscape Communicator; and Personal Security Manager.

The Red Hat products and services provided through the download site are for exclusive use in the following Licensed Community: (1) All components of the U.S. Department of Defense and supported organizations that utilize the Joint Worldwide Intelligence Communications System, and (2) All non-DOD employees (e.g., ontractors, volunteers, allies) on-site at the U.S. Department of Defense and those not on-site but using equipment furnished by the U.S. Department of Defense (GFE) in support of initiatives which are funded by the U.S. Department of Defense.

Licensed software products available through the August Schell contract are for the commercial versions of the Red Hat software, not the segmented versions of the previous Netscape products 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 Red Hat product 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 August Schell Red Hat 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 August Schell Red Hat download site (or contact the project manager listed below).

GIG or GCCS users: Common Operating Environment Home Page
http://www.disa.mil/gccs-j/index.html
GCSS users: Global Combat Support System
http://www.disa.mil/main/prodsol/gcss.html

Contractor: ***August Schell Enterprises*** (www.augustschell.com)

Download Site: http://redhat.augustschell.com

Ordering Expires: 14 Mar 09 (Contract options expire 15 Mar 11)
All downloads provided at no cost.

Web Link: http://iase.disa.mil/netlic.html

Red Hat Linux

Red Hat Linux - Provides operating system software license subscriptions and services to include installation and consulting support, client-directed engineering and software customization. Red Hat Enterprise Linux is the premier operating system for open source computing. It is sold by annual subscription, runs on seven system architectures and is certified by top enterprise software and hardware vendors.

Contractor: ***DLT Solutions, Inc.*** (HC1013-04-A-5000)

Ordering Expires: 30 Apr 09

Web Link: http://www.dlt.com/

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 Standard, 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.

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

Apple - NEW!

Apple - Provides Apple Desktop and Server Software, maintenance, related services and support as well as Apple Perpetual Software licenses. These licenses include Apple OS X Server v10.5; Xsan 2; Apple Remote Desktop 3.2; Aperture 2; Final Cut Express 4; Final Cut Studio 2; iLife '08; iWork '08; Logic Express 8; Logic Pro 7; Mac OS X v10.5 Leopard; QuickTime 7 Pro Mac; and Shake 4.1 Mac OS X. Software Maintenance, OS X Server Support, AppleCare Support and Technical Service are also available.

Contractor: ***Apple, Inc.*** (HC1047-08-A-1011)

Ordering Expires: 10 Sep 11

Web Link: http://www.esi.mil

Novell

Please go to the DON IT Umbrella Program Web site for more information:

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

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 BPA

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 (N00104-07-A-ZF30); (703) 378-5697; Awarded 01 Dec 2006

Ordering Expires: Effective for term of GSA contract

Authorized Users: All DoD components. For the purpose of this agreement, DoD components include: the Office of the Secretary of Defense; U.S. Military Departments; the Chairman of the Joint Chiefs of Staff; Combatant Commands; the Department of Defense Office of Inspector General; Defense Agencies; DoD Field Activities; the U.S. Coast Guard; NATO; the Intelligence Community and Foreign Military Sales with a letter of authorization. This BPA is also open to DoD contractors authorized in accordance with the FAR Part 51.

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: 31 Aug 10

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.

The DON IT Umbrella Program offers great customer service

Go to the Web sites below to learn more:

www.it-umbrella.navy.mil

www.itec-direct.navy.mil

www.esi.mil

YOU ARE INVITED TO THE

West Coast DON IM/IT Conference

Department of the Navy Information Management/Information Technology Conference

Hosted by the Department of the Navy Chief Information Officer (DON CIO)

February 10 - 13, 2009

SAN DIEGO CONVENTION CENTER, SAN DIEGO, CA

The DON IM/IT Conference provides a venue to share information about the latest DON IM and IT initiatives, policy and guidance. Conference topics include:

- Computer Network Defense
- Data Strategy
- DON IT Workforce
- DON IT Umbrella Program
- Electromagnetic Spectrum
- Enterprise Architecture
- Enterprise Software
- Information Assurance
- Knowledge Management
- Privacy
- Service Oriented Architecture
- Wireless

The DON IM/IT Conference is open to all DON, government, military and support contractor personnel. No conference fee will be assessed, but registration is required.

In the coming months, check the DON CIO website at www.doncio.navy.mil to register for the conference and to see tentative and final agendas.

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

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC ATLANTIC
CHIPS MAGAZINE
USPS 757-910
ISSN 1047-9988