Sharing Information - Technology - Experience

CHIPS

October - December 2005

KNOWLEDGE MANAGEMENT

For the Strike Group - Multinational Task Force - Training - Enterprise Planning

U.S. FLEET FORCES COMMAND
Adm. John C. Harvey Jr.

ARMY CIO/G-6
Lt. Gen. Jeffrey A. Sorenson

CHIPS

October – December 2009 | Volume XXVII 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
Tony Virata
DON IT Umbrella Program

Columnists
Sharon Anderson, Robert J. Carey
Christy Crimmins, Tom Kidd,
Steve Muck, Retired Air Force Maj. Dale Long

Contributors
Eric Carr, DON CIO Graphics
Lynda Pierce, DON CIO Communications
Holly Quick, SSC Atlantic

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 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) 443-1775; DSN 646. E-mail: chips@navy.mil; Web: www.chips.navy.mil.

Disclaimer: The views and opinions contained in CHIPS are not necessarily the official views of the Department of Defense or the Department of the Navy. These views do not constitute endorsement or approval by the DON CIO, DON IT Umbrella Program or SPAWAR Systems Center Atlantic. The facts as presented in each article are verified insofar as possible, but the opinions are strictly those of the individual authors. Reference to commercial products does not imply Department of the Navy endorsement.

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) 443-1775, DSN 646.

SPAWAR

Naval Surface Warfare Center (NSWC) Dahlgren, Va. (Aug. 19, 2004) – Naval reservists, scientists and engineers work in the Integrated Command Environment (ICE) Human Performance Laboratory located at NSWC Dahlgren, Va. The ICE lab focuses on the Navy's evolving human performance and human systems integration (HSI) testing. The lab demonstrates the ability to fight future battles with HSI-engineered hardware, software and features common consoles, displays and knowledge management components that fleet Sailors helped design to enhance human performance and mission accomplishment. ICE is part of the vision of Sea Power 21. NSWC Dahlgren provides research, development, test and evaluation, engineering, and fleet support for: Surface Warfare, Surface Ship Combat Systems, Ordnance, Strategic Systems, Mines, Amphibious Warfare Systems, Mine Countermeasures and Special Warfare Systems. U.S. Navy photo.

Cover

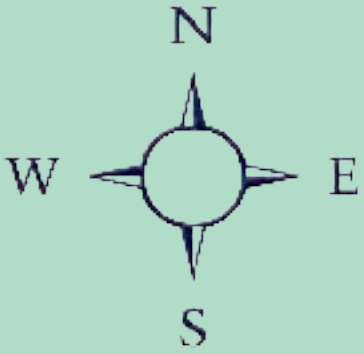
Members of the Department of the Navy knowledge management community of practice present a diverse view of a few of the applications of knowledge management in the department — from strike group training and operations — to designing and building the Navy Enterprise Portal. Articles begin on page 20.

Jim Knox, knowledge management leader for the Department of the Navy, helps commands achieve the DON knowledge management vision. The department's vision for KM/IM is to, "create, capture, share and reuse knowledge to enable effective and agile decision-making, increase the efficiency of task accomplishment, and improve mission effectiveness." Knox leads a KM learning session at each DON Information Management/Information Technology Conference featuring guest speakers who discuss KM successes that organizations can emulate to attain the benefits of implementing KM practices.

Navigation Guide

Features

In Every Issue



From the DON CIO

Knowledge Management

Around the Fleet

Joint Communications

Navy Enterprise

Information Technology

Editor's Notebook

In this issue, we explore a few of the applications of knowledge management in the Department of the Navy. The articles came from the knowledge management community of practice, a hard-charging group of KM leaders from across the department.

The idea for the focus on knowledge management came from the KM session at the West Coast DON Information Management/Information Technology Conference held in February. From the strike group to Multi-National Force - Iraq, a diverse group of KM champions explained how the application of KM principles is improving the speed of decision making and having a direct impact on warfighter effectiveness.

Citing the high operations tempo, the many demands on the department's budget and the need to collaborate jointly, and with coalition and nongovernmental agencies, their compelling argument to further the implementation of KM across the department was so convincing that I asked them to write.

As retired Navy Cmdr. Nancy Jenkins, knowledge management officer for Commander, U.S. Second Fleet, said, "Knowledge management is not new. The only thing that has changed is the impetus to do it better."

In August, the CHIPS staff attended the Army's LandWarNet Conference and had the opportunity to talk with Army leadership, Lt. Gen. Jeffrey Sorenson and Maj. Gen. Susan Lawrence, about technology improvements on tap for battlefront Soldiers. Look for their interviews in this issue.

The CHIPS staff had the pleasure of attending the NATO Supreme Allied Command Transformation change of command ceremony Sept. 9, where French Air Force Gen. Stéphane Abrial took over command from U.S. Marine Corps Gen. James Mattis. The occasion was significant because it marked the first time in NATO's 60-year history that a non-U.S. officer was permanently assigned as one of NATO's two Supreme Allied Commanders. U.S. Navy Adm. James Stavridis serves as Supreme Allied Commander Europe. Gen. Mattis will continue to serve as commander of U.S. Joint Forces Command. Look for an article about the event on the CHIPS Web site.

Sept. 17, at a breakfast hosted by the National Defense Industrial Association (NDIA), Commander, U.S. Fleet Forces Command, Adm. John Harvey, led the audience in a thoughtful discussion about the challenges facing the Navy today. Highlights of the admiral's remarks appear in this issue.

Welcome new subscribers!

Sharon Anderson

Please join us for the next DON IM/IT Conference, to be held Feb. 1-4, 2010, at the San Diego Convention Center. Go to the DON CIO Web site at www.doncio.navy.mil for details and to register.

French Air Force Gen. Stéphane Abrial delivers his first address as Supreme Allied Commander Transformation during a change of command ceremony held Sept. 9 on board USS Dwight D. Eisenhower (CVN 69).

U.S. Marine Corps Gen. James N. Mattis, former Supreme Allied Commander Transformation, French Air Force Gen. Stéphane Abrial, current Supreme Allied Commander Transformation, NATO Secretary General Anders Fogh Rasmussen and Italian Navy Adm. Giampaolo Di Paola, Chairman of NATO's Military Committee, conduct a press conference following the Allied Command Transformation change of command Sept. 9 aboard the aircraft carrier USS Dwight D. Eisenhower (CVN 69) at Naval Station Norfolk.

MESSAGE FROM THE

DON CIO

Mr. Robert J. Carey

In past editions of CHIPS, I've written about information sharing. For this edition, I'd like to discuss knowledge management (KM) as it pertains to the concept of information management (IM). Closely related to sharing information and data strategies, KM is about providing the specific (actionable) information needed to make a decision or complete a task. KM is about not reinventing the wheel or, as the KM team at Tactical Training Group, Pacific puts it, finding what you need from the "sea of information."

Our vision for KM/IM is to, "create, capture, share and reuse knowledge to enable effective and agile decision-making, increase the efficiency of task accomplishment, and improve mission effectiveness." This is a broad task, but once we break it into components, we find that some central themes arise.

Not everyone thinks this vision is needed. In discussing KM with DON audiences, we sometimes hear, "We already do this!" and "We've always done this." Though the term may be only 10 to 15 years old, KM is not new. The term IM is not new either, but it is gaining a lot of traction with the operational community as a way to navigate the plethora of systems and databases to quickly discover information needed to support decision making.

Our vision for KM/IM is to, "create, capture, share and reuse knowledge to enable effective and agile decision-making, increase the efficiency of task accomplishment, and improve mission effectiveness."

Many of us have used and benefited from KM processes such as best practices, lessons learned and post-action reviews. However, for most commands, it is probably fair to say that we only take advantage of KM some of the time.

We have an opportunity to make large, positive impacts on the department through accelerating the tenets of KM/IM. Today's technology offers unprecedented information and knowledge flows, but our focus will be to navigate the most efficient route to the information we need.

We can take advantage of DON knowledge by applying the tenets of KM, often with little or no cost. KM can be implemented at a variety of levels; it doesn't require significant or disruptive changes to a command.

At the grass roots level, there is individual KM. This involves people, who have been educated about KM tools, techniques and processes, applying these tools, as appropriate, to different tasks and challenges. The next level up is command KM. Many DON commands now have KM officers. Their objectives and responsibilities vary, but there is a common denominator for successful KMOs. They did not implement KM for KM's sake; rather, they applied KM processes to command challenges.

One KMO, hired several years ago, looked around the command for a serious pain point and solved it. After a few more victories, his value and KM's worth were validated. Today, he doesn't have to look around; shipmates routinely seek his assistance.

There is real potential benefit to leveraging KM from an enterprise point of view. Across the DON there are similar commands, similar platforms, similar missions and similar processes. In sharing experience and knowledge, we will not only improve performance but also make our professional lives easier.

Neither information management nor knowledge management in the Department of the Navy is a program of record. In our KM strategy document we noted that KM is a centralized vision being executed in a decentralized manner. It is being implemented by commands across the department and around the globe that recognize its value.

We are working on a strategy for maximizing the investments we make in the information management domain so that we can make optimal use of our computing experience and discover, analyze, decide and act on information as we need to.

In the spirit of information sharing about KM, we began hosting DON IM/IT Conferences in 2005. As a part of those conferences, we have KM tracks that are half-day sessions with five to six speakers sharing their KM experiences. More than 20 DON commands as well NASA, the U.S. Army and the Virginia Department of Transportation have presented some of their KM stories.

It is encouraging that the focus of the tracks has shifted over the past few years from KM definitions and fundamentals to command experiences with KM. The next conferences will be held Feb. 1–4, 2010, in San Diego and May 10-13, 2010, in Virginia Beach. The KM track is typically held on the first day of the conference.

Talking with Admiral John C. Harvey Jr. Commander, U.S. Fleet Forces Command

Adm. John C. Harvey Jr.

Adm. John C. Harvey Jr. assumed command of U.S. Fleet Forces Command in July 2009 bringing with him a wealth of knowledge about the inner workings of the functions and missions of the U.S. Navy — from the Nuclear Navy to three tours at the Bureau of Naval Personnel in a variety of billets including surface nuclear officer detailer, CGN/CVN placement officer, surface nuclear program manager in N13, legislative adviser to Chief of Naval Personnel (CNP), executive assistant to CNP and as director, Total Force Programming and Manpower Management Division (OPNAV N12).

He has also served as the senior military assistant to the Under Secretary of Defense (Policy), and on the Navy staff as deputy for Warfare Integration (OPNAV N7F).

Most recently, he served as the 54th CNP/OPNAV N1 and as the director, Navy Staff (OPNAV).

The admiral is interested in extending the intellectual discussion of the Navy's mission and challenges. He hosts a blog (http://fleetforces.dodlive.mil/) and Commander's Thinking Corner (www.cffc.navy.mil/thinking_corner.htm) on the Fleet Forces Web site posted with articles and speeches that he considers valuable for professional development and decision making.

The National Defense Industrial Association (NDIA) Greater Hampton Roads Chapter hosted a breakfast Sept. 17 in Norfolk, Va., where Adm. Harvey spoke about Fleet Forces Command's posture and priorities. Highlights of the discussion included many factors that impact the Navy mission, including the global economic crisis; cybersecurity; maritime security; fleet maintenance; and the current high operations tempo. The admiral called these conditions a "perfect storm" in sustaining Navy operations.

Key points of Adm. Harvey's remarks and his response to questions from the audience follow.

Budget Constraints and the Operational Tempo

We are in 'Class 6' rapids — that is what the next few years are going to be like. There are huge decisions coming [from the Administration] on Afghanistan that will affect Fleet Forces and the Navy and the armed services writ large. Along with that the international fiscal crisis is impacting us today and will continue to do so. The economic factor sets the stage for everything. For the last eight years, we were in an increasing budget environment. That is over. We are now on a downhill slide.

We have been through these build-up and downsizing cycles before. When I came into the Navy in 1973, it was post-Vietnam, the bottom of a cycle. So now we are on what I believe will be the third cycle during my time in the Navy. This is going to be a different experience for everybody in the chain of command, not just the budgeteers, because it is going to drive how we perceive the force, how we operate the force, how we deploy the force, and how we sustain the force into the future.

My job hasn't changed — provide forces ready for tasking. It is clear; it is unambiguous. The challenge is the demand signal from the combatant commanders has gone up every year in every force category. The money has gone up every year [too], and we have been able to generate more force and what we have generated has been consumed.

Now, we are getting less resources to generate those forces, but we have a demand signal that continues on an upward trajectory, whether you are talking about Africa Partnership Station, Southern Partnership Station, Comfort (USNS Comfort) and Mercy (USNS Mercy) humanitarian deployments, from the South Pacific to Southeast Asia, and single deployers for counterterrorism and counter-piracy operations in the Gulf of Aden, requirements continue to rise.

Sixty percent of all close air support in Afghanistan now is coming off the deck of an aircraft carrier. Just think what that does to flight hours. You see that reflected in every part of operations within the force and that demand signal continues to build up while the resources go down.

Today, we have about 48 percent of the Navy underway. We have been sustaining that for a number of years now. Operational tempo drives your maintenance tempo. We are using this force considerably and building up a maintenance bill at the same time we are struggling to procure the future force.

In order to sustain a Navy that is global, that is inherently expeditionary, that is ready and responsive to that commander and to sustain that 313-ship floor, I have to get the existing force out to its service life. Yet, I am using that existing force more than we ever have before in the past on a standard basis.

The good news is that however long you have been out of uniform, when you get the chance, go walk the flight line and the deckplates because the people we get have never been better.

It almost sounds like a cliché, but it is not. If you take a hard-nosed look at the data, where these Sailors come from, their test scores, backgrounds and education, and how they are performing, and what we are doing to advance them, the quality we are bringing into the officer and the enlisted corps, by any measure, we are doing extremely well.

That's what gives me my confidence in the future. Despite being in permanent whitewater, I have the right people in the kayaks to get us through. I told the CNO that the third class petty officers will save the day and figure it all out and make it work for us. I keep that foremost in my thoughts.

The Navy's Core Competency

I think the core competency of the United States Navy, the reason that taxpayers have funded this Navy for 234 years, is so that in a powerful and sustainable way, we can go to a place somebody doesn't want us to be, do things that people don't want us to do, and sustain that activity for as long as we need to. That is our core competency.

Today the Navy is our strategic reserve. Whatever scenario you want to apply that to, I think that means that I have to be able to provide the CNO with four carrier strike groups within 30 days. That is my model for how I look at what we need.

To do that over time, I think I have to start looking at the demand signals and recommending some 'nos.' We did it in '09; there will be more in '10 looking at the Global Force Management process. We need to recognize that if we go beyond what we can do, we are doing real damage to the ability to sustain today's force into the future.

We are very sensitive to saying no; it is not our culture. Now I am saying, 'Here is what I can do with the resources you have given me to answer the bell.'

Discussion with Audience

Q: How do you plan to meet the operational challenge?

A: I did two things right away at FFC that were at the heart of how I view the operational challenge. I took Mark Honecker, who was serving as executive director and chief of staff and lead for the Fleet Readiness Enterprise, and I split his job.

Vice Adm. Pete Daly is now the deputy chief of staff, and Mark Honecker is the executive director and leader of the Fleet Readiness Enterprise. That refocused the FRE. I told Mark I wanted him like a laser on the challenge of readiness in '10. How do I produce forces ready for tasking in '10 when I already know that I will have a lot less resources than I had in '09?

I told him that I was not so much interested in more efficiency, but I am interested in effectiveness, the effectiveness of the force that we send forward and not simply in generating more efficiencies within various enterprises where you add it up to the money saved. When we send people forward, they are going to be trained, there is going to be material in the parts bins, they are going to have weapons in their magazines, and they are going to be ready to do what we expect them to do. That is an effective force. That is what we owe the nation.

Now I have a clear line of accountability. It is important to bring that concept back; it is what all of us grew up with, if you had your time in uniform. It is a fundamental understanding; I am accountable and responsible.

Q: What will be the economic impact on training?

A: You have to balance and sustain your force with maintenance and personnel training and unit training to deliver forces ready for tasking. My goal is that whoever we send out is trained for what we expect them to do. I think that is a moral responsibility that I have to deliver on.

What will change is fleet synthetic training. There is an iron law on a flight deck. You launch and recover aircraft safely, or you do not, there is nothing in between. You must train the carrier, the air wing and the supporting cast to do that to an absolute level of perfection. You can't surrender on it. It is binary.

When I take that ship and that air wing that are now a cohesive unit, do I have to get the ship and the air wing underway for a period of time when I have already achieved a level of competence in their fundamental competency? The answer is no, [we can use] fleet synthetic training.

Q: What are your thoughts about controlling maintenance costs?

A: I have a lot of thoughts about controlling maintenance costs.

Adm. John C. Harvey Jr. Commander, U.S. Fleet Forces Command, addresses the audience at a breakfast hosted by NDIA Sept. 17 in Norfolk, Va. The admiral engaged the audience in a discussion on topics that are at the forefront of issues facing the nation and Navy, including fleet readiness, maintenance and training.

"The good news is that however long you have been out of uniform, when you get the chance, go walk the flight line and the deckplates because the people we get have never been better."

I think we have underfunded for many years the true maintenance costs of a ship. Back in the '90s, we went to continuous maintenance rather than coming back from deployment and taking the deep look.

Continuous maintenance assumes that you have knowledge in the crew to self-assess at a sophisticated level, that you have continuous funding applied to deal with the results of that self-assessment and are doing the right things on a routine basis, and eventually bringing in pros for eight months of a deep overhaul for a cruiser or destroyer.

We shifted our fundamental philosophy. Then we took out all of the supporting repair organizations and the experts on how we sustain these ships. If you look at the numbers today, we have six operational carriers, five in deep maintenance. We have 38 operational submarines and half that number in deep maintenance. We have a strong commitment to deep maintenance on the nuclear side.

If you look at surface ships today, I have 51 destroyers available, and I have four in deep modernization. I have to get 30 or 35 years of life from these ships and figure out a way to do it. Name one destroyer class, post-World War II, which we have taken to the end of its service life? We have never done it.

Now, to get to 313 ships with this global view of operations, we have to get to full service life. That is going to be a big issue for me that takes a lot of love and attention constantly. You can't pretend there is a cheap way to do it.

It is a balance between operations and maintenance, training and procurement, to give us a whole force. That is my take-away. If you were going to bury me and carve something on my forehead, it would be, 'He worked for the whole force, a coherent force that went out there and could do what he said they could do with confidence, and Sailors were confident they could do their jobs.' CHIPS

Interview with Army Director CIO/G-6
Lt. Gen. Jeffrey A. Sorenson

Lt. Gen. Jeffrey A. Sorenson

One of the critical initiatives for the Army CIO/G-6 is transforming LandWarNet (LWN) through the Global Network Enterprise Construct (GNEC) strategy. LWN is the Army's part of the Global Information Grid technology infrastructure that enables Soldiers to "reach back" for data, in the form of high-definition intelligence products, voice, video and data.

GNEC is the focused, time-phased, prioritized, resource-sensitive Army-wide strategy to transition LandWarNet from many loosely-affiliated independent networks into a truly global capability that is designed, deployed and managed as a single integrated enterprise.

As part of GNEC, the Army issued a Request for Information (RFI) Aug. 17 to seek vendor recommendations for commercially managed enterprise messaging and collaboration services. The two chief drivers for the RFI are to provide Soldiers a single e-mail address, along with collaboration functions, that would be accessible from anywhere in the world throughout their career and to reduce operating costs.

The cost savings will come from changing the current paradigm of Army installations hosting and supporting their own e-mail exchanges to an enterprise model of hosting e-mail services at centralized data centers.

Lt. Gen. Sorenson and the Army Signal Corps led a series of discussions and learning sessions about GNEC, LWN and security and cyber initiatives at the LandWarNet Conference in Ft. Lauderdale, Fla., in August. The discussion was so compelling CHIPS asked Lt. Gen. Sorenson to discuss the GNEC strategy and other Army technology efforts.

CHIPS: Army Vice Chief of Staff Gen. Peter W. Chiarelli said in his address to the LandWarNet Conference that Signal staff must work to make systems and networks accessible to warfighters and support staff while at the same time assuring that networks and systems are safe. What is the right balance?

Sorenson: We need to improve operational capabilities and take advantage of many commercial systems and yet, at the same time, we have to provide adequate security to ensure that the systems and data are such that the users can trust them.

In some cases, we have certainly been conservative with respect to security, probably to the point that we have limited, or in many cases hindered, our ability to take advantage of some of the commercial technologies to advance capabilities, specifically, with social networking sites (SNS). These sites clearly provide some operational benefits; yet it is a domain where there is evidence of malicious activity. We must ensure they don't create an operational security violation.

We are trying to improve our enterprise architecture such that we are protecting what we call the 'coins of the realm,' those specific aspects of the network that you do not want to have compromised. Part of our strategy now is setting up area processing centers to reduce the number of points of presence on the network, so that we have a consolidated number of centers where different organizations across the Army can draw services, but leave network management to a number of centers that are highly standardized in terms of their tool sets, as well as function, so they can better manage the security of the network. That's part of the enterprise architecture.

The second thing is that we are trying to consolidate some of our active directory capabilities. As we have proliferated the number of active directories throughout the Army, we have so many that they can't see each other. We have difficulties making sure they are all secure. A lot of consolidation is taking place, both in the area of processing centers and our consolidation of active directory capabilities, to get to an improved security posture across the board.

Going back to what Gen. Chiarelli was talking about, his point was that in many cases there have been policies written about security that do not get challenged adequately as we are trying to bring an operational capability to the forefront. He is absolutely insistent upon having a secure network, but at the same time, we have to be smart about this.

As an example, in COMSEC, communications security, we are right now working on something called Suite B. Suite B COMSEC is leveraging encryption capabilities that are now resident within the financial industry which has an enormous vested interest in security to prevent fraud and financial crimes.

In some cases, the financial industry has built a capable system for encryption that we in the Army could leverage — giving us enough security to satisfy what Soldiers need on the battlefield but not restricting our ability to deliver the network.

We have examples in theater where Soldiers say the information presented in the forefront of the battlefield is cutting edge and very critical information, but within a few minutes, it becomes historical information.

Therefore, why can't we make sure that we get everybody that situational awareness and maybe, in some cases, take a little risk because within a few minutes it is going to become obsolete anyway? Clearly, Soldiers want to get the information that they need without having the security barriers to crawl through all the time.

There is no inconsistency with what Gen. Chiarelli said versus what we hear from the field. It is the management of polarities. What information is required at the edge versus what security classification do you need to have? These discussions are taking place not only for the network; I think you see that in the Intel community as well.

CHIPS: How would you rate technology and systems interoperability with joint and coalition partners?

Sorenson: Working with our partners right now has certainly been challenging. If I had to rate it, I would give us a 'C' at best.

With our coalition partners, as well as nongovernmental organizations that participate in some of our operations, we have [protected] sensitive information on our networks to the point that we can't provide our partners the data they need.

When you get into coalition warfare and are fighting side-by-side with a partner, and you have the intelligence situational awareness, you have the understanding of the enemy and the friendly situation, but because they don't have a particular clearance, you can't share with them. It begins to be somewhat dysfunctional in terms of conducting combined operations.

We are working hard in OEF (Operation Enduring Freedom) to make data more accessible and more visible to our coalition partners, and I think we are making some great progress.

When we get to working with the sister services, from a land component perspective, we are doing a lot with the Marines. They are using some of our capabilities, the Fixed Regional Hub Node (FRHN) — in Camp Arifjan in Kuwait — to extend connectivity and services via their tactical satellite terminals to their deployed units in theater.

Clearly, there is more to do when we get into this world of cyber with our Air Force and Navy brethren service components that we need to fix. Going back to the whole issue of security of the network, we as an Army have globally deployed Theater Network Operations and Security Centers (TNOSC) in each one of the combatant command areas of operations. The difficulty has been that each TNOSC has different methods of how they monitor the network, and they use different tools.

When I returned from visiting the TNOSCs, I spoke to Maj. Gen. Susan Lawrence, the commanding general of the Network Enterprise Technology Command/9th Signal Command, about the disparity I saw with respect to monitoring the network. It is obvious that we needed to standardize our toolsets to get to a better global perspective of what the network looks like. To do that, we had to find additional resources during the budget year, which was somewhat challenging. We are now getting these funds along with the funding to set up the Fixed Regional Hub Nodes in CONUS this year and additional area processing centers.

CHIPS: What is the most difficult challenge in initiating GNEC? There seems to be many similarities with the Navy Marine Corps Intranet such as the establishment of regional network service centers, enterprise services and e-mail. Will you be using a seat management concept? Are you using a similar model to the NMCI or the Information Technology Infrastructure Library (ITIL)?

Sorenson: Funding and technology are the two major GNEC challenges right now. These have been unresourced requirements. We have not put enough money into this over the last few years to address adequately the needed improvements.

Secondly, we have had technical challenges in terms of trying to deploy our enterprise architecture and consolidate a number of active directories into two— one for applications — and one for e-mail. Until we can get to a global perspective, we could be spending a lot of money but not achieving success because of the technical challenges we have.

With respect to NMCI, the difference is that we are not turning everything over to a managed service. There are aspects of this that we would like to get to a managed service, predominantly for e-mail. We are now working with the Defense Information Systems Agency and U.S. Transportation Command to prototype that capability.

"Clearly, Soldiers want to get the information that they need without having the security barriers to crawl through all the time."

CIO/G6 is leading an initiative to bring about an enterprise e-mail strategy for the entire DoD. Currently, a member of the Army cannot access the address for an individual from a separate military branch through the Global Address List, the directory used to locate contact information. The focus is to set this in place for the headquarters of Army Materiel Command (AMC), Army Forces Command (FORSCOM) and TRANSCOM. Once this proves effective, DISA will take the lead in extending this capability to the entire force.

From the standpoint of turning over the entire network to another party to manage, we are not going to go there. NETCOM/9th Signal Command is still going to be the global provider of the network and make sure it is operational, as well as retaining responsibility for defending it.

All of these other capabilities, the area processing centers, the Fixed Regional Hub Nodes, the TNOSCs, they will all work for NETCOM/9th Signal Command. There are certain aspects of NMCI that we want to take advantage of, but in my discussions with my Navy counterparts, as well as the Marines, we are trying to use the lessons learned to determine how we can take the benefits of NMCI but not have a network [that] we don't command and control ourselves.

We are now in the process of combining the globally deployed FRHNs, area processing centers and the TNOSCs on a regional basis to form what we call a Network Service Center. We hope to develop five of these — one for Southwest Asia, one for Europe, two in the CONUS theater and one in the Pacific. Think of them as more regionally based segments of what might compare to an AT&T or Verizon global network, where they have to define certain regions and regional responsibilities for delivery of that network.

We are also interested in ITIL. We have begun to look at those processes in ITIL across the board from the standpoint of security and enterprise architecture. Those processes are well-standardized and certainly have been shown to be of use in the commercial sector. It gives us a way to not only baseline what we are doing, but also to compare ourselves to our counterparts in the military services, as well as industry, to improve the delivery of the network through these process improvements.

CHIPS: I saw an impressive demonstration of WIN-T Increment 2 on the exhibit floor. How does LandWarNet relate to the Army's Warfighter Information Network-Tactical? Will the Network Service Centers support both WIN-T and LandWarNet?

Sorenson: WIN-T is the tactical transport piece that is going to take data and applications from the Fixed Regional Hub Node into the tactical domain to deliver it down to the Soldier at the far edge of the battlefield. The program manager for WIN-T is also responsible for building out the capabilities within the FRHN. He does not only have the ability to ensure that there is a standard configuration of the delivery of this network, but also to enable the improvements in the future.

The PM is building out what is going into the Fixed Regional Hub Node and making sure it conforms to the configuration he has put into the tactical set so we have an end-to-end network — from the Soldier at the far distant edge — all the way back to and throughout the GIG.

Increment 2 of WIN-T begins to give us a little of the on-the-move capability as opposed to what we have today, which essentially is a system on a vehicle that is providing the communications backbone to the warfighter. In many cases today, WIN-T has to be set up during a halt in operations to communicate; WIN-T Increment 2 will deliver the on-the-move capability.

WIN-T Increment 2 also enhances the delivery of the network to much lower organizational aspects of the Army down to, in some cases, the company level with the use of the Capability Sets. It is an improvement in our ability to deliver network capacity down to lower echelons in our formations, as well as to do it in a manner that they can conduct those operations on the move, as opposed to being static.

WIN-T, Warfighter Information Network–Tactical terminals, are much like something the Marines have called SWAN, Support Wide Area Network. They are built by the same company and have almost the same capabilities, but the SWAN is more of a transient-case implementation.

Today, if you use your cell phone, your cell phone communicates back to a tower and those towers are populated all throughout the United States and overseas. WIN-T provides those cell phone towers but does it in a manner that those towers move. That provides the on-the-move capability by constantly resetting the network based upon where people are and what they can see.

CHIPS: How is the Army meeting the technology needs of its expeditionary force? Are security concerns more difficult to manage than technology readiness?

Sorenson: The biggest challenge to adopting and bringing in new technology is interoperability. It goes back to the whole notion of enterprise architecture, providing an architecture by which changes can be made, new equipment can be integrated, and old equipment can be updated. With the size and scale that it is, the Army will never, never have the same systems throughout our Army.

You will always have generation one, generation two, generation three technology because of size, funding, training, integration, deployment and OPTEMPO (operational tempo) — all those facts of life that are never going to allow our Army [forces] to all have the same piece of equipment throughout all units at the same time.

Security is embedded in interoperability. It is always harder trying to make older generation systems function with newer generation systems, and to have the architecture to accommodate newer capabilities without the need to go back and redesign what we have already built.

Like the Vice Chief of Staff said, we have to provide the ability, much like the Apple iPhone, which has 60,000-plus applications because it has a standard platform, to allow different developers to make improvements to increase capability at a rapid pace. We need to do what we can to adopt that same capability to allow newer technology and make it interoperable with other systems that we have.

CHIPS: How do you balance the technology needs of Soldiers so they aren't overwhelmed by the equipment they carry into the fight?

Sorenson: In many cases we have designed capabilities in the lab, only to take it to the field and Soldiers said, 'This is very interesting. This is very neat. This is very sophisticated … but I don't need all this stuff.' We had that example as we deployed the initial Land Warrior capability to Soldiers.

Land Warrior was built as a way to give them up-to-date situational awareness. They had a monitor on their head, they had a radio, and they were getting all this situational awareness information — but it got in the way of them doing their regular job — which is to fight an enemy.

In some cases, we had to scale back the functional capability within that Land Warrior ensemble because the functional capability was so robust that the Soldiers found that there was too much information for them to use. We had to spend considerable time with the maneuver force schools, (Ft. Benning is the maneuver center for Army armor and infantry.), to get at what amount of information is needed and at what echelon, to help scale the network because some of these applications are bandwidth and capacity intensive.

We had to do it a couple of different ways: lay out what the network capacity is and then say, for that network capacity, this is the amount of information I can give you. What part of it do you want and what part don't you want so we can scale the applications to deliver only what the Soldier needs.

CHIPS: What is the most important communications technology to the individual Soldier on the battlefield — a radio?

Sorenson: A Soldier relies on knowing where he is, where his buddies are, and where the enemy is. A certain percentage of the information will only get radio [communication], but that radio, at some point, could be a cell phone type of capability that tells where they are, where their buddies are, and where the enemy is, but they can also get more situational awareness information as they require it.

CHIPS: Can you talk about your priorities since becoming the Army CIO, have they changed?

Sorenson: My priorities have not changed much. At different points in time, some have been more dominating than others. I have four priorities. The first one has been the deployment of the Global Network Enterprise Construct, otherwise known as GNEC, and getting it to the point that we can get the resources and the organization and the technical aspects worked through to deliver the global network for our Army.

The second priority has been working a number of issues related to cyber. With the establishment of CYBERCOM (U.S. Cyber Command), what is the Army Service Component Command going to look like? How is it going to be structured? What authority is it going to have? We are trying to work through all of those particular aspects.

The third one has been the area of knowledge management and data strategy. We have a lot of information in the Army, but in many cases, it is in stovepipes. For example, one functional area might have logistics information [that] they are not sharing with the personnel community. We have been working on a data strategy that makes data visible, accessible and available, and also integrates it into our knowledge management strategy, such that we can get this information out, and our knowledge management warriors can begin to use this data in ways that we have never anticipated.

We see it all the time. We develop a capability and give it to Soldiers for an intended use, but they figure out different uses for it and make modifications to it over time.

The fourth priority that supports all of the rest is the resourcing strategy. What does the resourcing strategy look like for information technology for the Army? How do we prioritize to do what we need to do with, in some cases, limited resources? What do we do first? What do we do second? We can't do it all.

CHIPS: Is the current Army technology infrastructure sufficient to support the Army buildup?

Sorenson: Yes, we are building out the capability to accommodate the additional 22,000 Soldiers. That is the least of my worries right now. Getting this network globally deployed and standardized so that it can continue to accommodate more improvements and changes is really the focus.

We are in a unique period where the advances in technology that we have seen in the commercial sector are coming to the forefront in our Army. We are seeing a lot of activity with respect to the use of robotic technology for unmanned aerial vehicle and unmanned ground vehicle systems.

We are beginning to see a need, as we build out support forces for CYBERCOM, for those who have the knack to conduct operations on the network, to improve their skills, not only to conduct defensive operations on the network, but also to conduct offensive operations.

In the Army, and the other services, cyber operations are now required. These are very exciting times within all the military departments. If you have an interest in technology and want to make a difference to the nation, you clearly have a lot of opportunities here.

We continue to emphasize within the Army that in developing the global network we are not doing this independently, nor do we plan to do so.

We need more work on the joint piece of it, trying to work the interoperability, trying to leverage what we are doing so that the Air Force can take advantage of it, and we can leverage what the Air Force and Navy are doing. CHIPS

What is Global Network Enterprise Construct (GNEC)?

GNEC is an Army-wide strategy that will transform LandWarNet to an enterprise activity. A single integrated enterprise will achieve an information environment with global access, standard infrastructures, unity of command and control across Army cyberspace and common policies/standards that ultimately provide information services from the generating force to the tactical edge.

GNEC Vision:
Operationalize LandWarNet; transforming to deliver a global, standardized, protected and economical network enterprise that is effective, secure and well-managed.

GNEC Mission:
LandWarNet transformation will deliver timely, trusted and shared information and create an environment where innovation and service empowers Army and mission partners through an unsurpassed responsive, collaborative and trusted information enterprise.

GNEC Objectives:
- Operationalize LandWarNet
- Dramatically improve the LandWarNet defense posture
- Realize economies and efficiency while improving effectiveness
- Enable Army Interoperability and collaboration with mission partners

What is LandWarNet?

The Army's portion of the Global Information Grid (GIG), LandWarNet, is a combination of infrastructure and services. It moves information through a seamless network and enables the management of warfighting and business information.

The Army remains committed to providing reliable communications for a global force and LandWarNet is a key enabler for information superiority, decision superiority and ultimately full spectrum dominance.

Interview with Commanding General, Network Enterprise Technology Command/9th Signal Command Maj. Gen. Susan Lawrence

Maj. Gen. Susan Lawrence

U.S. Army NETCOM/9th Signal Command is a Direct Reporting Unit under the Army's Chief Information Officer/G-6 (CIO/G-6). Its core mission is operating and defending the Army LandWarNet (LWN) — the service's portion of the Global Information Grid (GIG), with the primary objective to ensure Army's network enterprise enables the warfighter at all echelons of operation. Additionally, the commanding general is designated as the Deputy for Network Operations for U.S. Army Space and Missile Defense Command/U.S. Army Forces Strategic Command.

With the headquarters at Fort Huachuca, Ariz., the NETCOM/9th Signal Command team has nearly 17,000 Soldiers, Department of the Army civilians and contractors stationed and deployed around the world, providing direct and indirect support to Army, joint and coalition warfighting forces.

NETCOM/9th Signal Command's organization is comprised of theater Signal Commands and brigades in the Pacific, Europe and Southwest Asia. Additionally, a U.S.-based Signal Command, 7th Signal Command (Theater), is scheduled to attain full operational capability by 2010. Nearly all of these organizations work under the operational control of Army and joint commands, and most are geographically dispersed.

It is this network of trained professionals that enables battle command and supports missions at all echelons — from the foxhole — to the White House.

The first woman to command the global organization, Lawrence was formerly the commanding general of the 5th Signal Command (Theater) and held the post of Chief Information Officer and Director, Command, Control, Communications and Computers, J-6, U.S. Central Command. CHIPS asked Maj. Gen. Susan Lawrence to discuss the critical mission of NETCOM.

Maj. Gen. Lawrence enlisted in the Army in 1972. She received a bachelor's degree from Campbell University in North Carolina and was commissioned in 1979. Lawrence has a master's degree in information systems management from the University of Georgia. She has served in a number of assignments — platoon leader, aide-de-camp, executive officer, company commander, battalion commander, brigade commander, as well as serving in a number of staff positions in Washington, D.C.

CHIPS: Can you talk about new technologies on the field that are in response to warfighter demand?

Lawrence: I often tell my team that our No. 1 job is ensuring that the squad in Afghanistan is never out of touch; that the network will always be with them, ensuring that they have the capabilities necessary to fight and win. We have aggressively applied new technologies to make that happen — to guarantee that applications and data are available wherever and whenever the Soldier needs them.

We've also worked to introduce technologies that will decrease the preparation time to access intelligence and operations data and services from distant theaters and deployed joint task forces. As we've done this, we've been mindful of the need for seamless, secure and reliable communications in a joint, coalition and interagency environment and have partnered with other organizations to enhance the interoperability of the systems in the field.

One specific area we're working on involves leveraging advances in the management of virtual environments. Over time, this will allow the Army to develop more applications on virtual machines and enable us to quickly move applications and data between Network Service Centers (NSC) on demand. Similar advances in identity management, security management and configuration management technologies will allow the Army to provide a means of secured access to warfighter and enterprise applications, including information technology resources and data, which remain with them through all deployment phases.

By the time we're done, the Soldier from Fort Bragg will have access to the same information in the field as he or she does at home station or in transit. Finally, we're also using improved security management, system management and network management tools to efficiently provision network enclaves to support collaboration with mission partners.

CHIPS: U.S. Joint Forces Commander Gen. James Mattis has talked about the increased importance of the small unit. Does this change the type of technology that small units will need?

Lawrence: The truth is that we really are living in a world in which tactical decisions can have strategic consequences. Quality communication is the chief way that we can make sure that those decisions are informed. As smaller units assume more responsibility, technology and connectivity must be extended to their level. Recent history has shown us that network resources that once resided at the brigade level often need to be pushed down to the battalion and company levels. We're working a range of initiatives to do just that, including the fielding of Warfighter Information Network - Tactical Increment 2.

CHIPS: Can you talk about WIN-T Increment 2?

Lawrence: We're excited about WIN-T Increment 2. It is an important part of getting the network down to the unit in the field. It enhances warfighter mobility and provides a communication network down to the company level. Tactical communication nodes in Increment 2 are the first step to providing a mobile infrastructure on the battlefield.

Combined with mobile points of presence, vehicle wireless packages and Soldier Network Extensions, Increment 2 enables mobile battle command from division to company in a completely ad hoc, self-forming network.

"Today's world is one [in] which adversaries often only meet electronically, facing off across the borderless expanse of cyberspace."

Commanding General NETCOM/9th Signal Command
Maj. Gen. Susan Lawrence

WIN-T Increment 2 also includes embedding communications gear in the commander's vehicles, bringing SIPR (Secure Internet Protocol Router) to a commander on the go. Commanders and select staff will have the ability to maneuver anywhere on the battlefield and maintain connectivity to the network. Once we're done, WIN-T Increment 2 will deliver an initial, on-the-move, broadband networking capability using satellite and radio links. We conducted development and limited user tests of this build earlier in fiscal year 2009 and plan to field the latest increment later this year. That fielding will focus on mobile formations, specifically Brigade Combat Teams.

CHIPS: The Army is consolidating servers and their applications to Area Processing Centers to provide consistent services in a netcentric environment for geographically dispersed tactical networks. Can you explain how the APCs will improve warfighter effectiveness?

Lawrence: APCs allow the Army to manage IT services and ensure that the right information reaches the right person, at the right time, in a joint netcentric environment. The APCs are just one of the three components of the Network Service Centers. Combined with the other elements — Regional Hub Nodes (RHN) and the Theater Network Operations and Security Centers (TNOSC) — they will dramatically improve responsiveness to warfighter requirements and rapidly changing mission demands. Like our forces, these components are not always collocated. The NSCs provide warfighters with connectivity, network operations (NetOps), data processing, storage, security and applications hosting capabilities.

The connect capability, provided by both standard network connections and the RHN, provides a point of entry into the APC services and the GIG for expeditionary forces. The NetOps capability enables the TNOSC to manage and protect the network to meet the needs of the commander in the field. It also provides the means for units to manage their applications within the units' processing and storage enclave at the APC.

Warfighters will no longer be required to establish their own service delivery and support. Instead, they will derive those capabilities from the NSC and focus on their missions. Additionally, the Army will realize efficiencies by integrating and consolidating network, computing, storage and virtualization resources across applications and services provided by the NSC.

At the end of the day, everyone wins. The warfighter receives improved support while the Army is able to make more effective use of limited resources.

CHIPS: Can you discuss the LandWarNet vision and progress to date? Can you talk about the approaches that are used to defend LandWarNet?

The Network Enterprise Technology Command/9th Signal Command (A) Soldier of the Year, Spc. Daniel Justice, 2nd Signal Brigade, 5th Signal Command, is congratulated with a coin from Lt. Gen. Jeffrey Sorenson, U.S. Army Chief Information Officer/G-6, Aug. 20, 2009, during the LandWarNet Conference in Fort Lauderdale, Fla. Maj. Gen. Susan Lawrence is second from right.

Lawrence: As you know, our nation faces a wide range of threats. They are synchronous, asynchronous and global. What's more, they aren't going away. The Army must be able to seamlessly join the LandWarNet with the larger DoD enterprise, the GIG, while meeting these threats. The Global Network Enterprise Construct (GNEC) is our Army's strategy for aligning and transforming our network assets — our people, equipment and policies — to meet these challenges.

The reason for transforming to the GNEC is clear. We live in a different world than we did in the Cold War. When I joined the Army in the early 1970s, the focus was on the forward deployment of forces. The new reality is that 80 percent of Army forces are CONUS-based. This means that our Soldiers are called to deploy with little to no notice, and the Army's relevance in these conflicts will be judged by its responsiveness and expeditionary capability. The Army must be ready to fight upon arrival. The key to that is ensuring that we can provide reliable network services to our Soldiers anytime, anywhere. The GNEC will allow us to do that by providing a seamless network that is universally available and accessible to the warfighter from the home station, to the area of operations and back again.

We took an important first step toward this earlier in the year when we conducted the NSC operational validation (OPVAL). This operation successfully demonstrated that NSCs can host battle command applications out of Area Processing Centers on behalf of a brigade-level organization. By standardizing network operations, network management, collaborative tools and application hosting, we proved that the NSC and its pillars (Regional Hub Node, APC and the Theater Network Operations and Security Center) provide warfighters unparalleled access to the GIG.

Of course none of this matters if we can't provide the warfighter with a safe, secure network. We've developed a comprehensive strategy to ensure that the SIPRNET, NIPRNET, and all the elements of the enterprise network provide that safe and secure operating environment. Our approach enhances our defensive capabilities, improves the sustainment of programs, and working with industry, develops more effective and rapid detection

and response capabilities. We're partnering with the military intelligence community as well to improve predictive intelligence. This strategy will allow us to dominate and win the Army's cybersecurity fight.

At the center of this fight are our security centers: the Army Global Network Operations Security Center and our Theater Network Operations Security Centers. The A-GNOSC and TNOSCs are the network's guardians. They work on a daily basis to detect, analyze and overcome the threat to theater and global network operations, helping our forces to maintain information dominance.

Additionally, the TNOSCs also provide NetOps and service desk functions — ensuring the seamless delivery of standardized enterprise services — while the A-GNOSC serves as the Army's operational arm into the world of the Joint Task Force-Global Network Operations. Together, they represent the Army's key LandWarNet cyber defense capability.

CHIPS: NETCOM/9th Signal Command executes command and control over a global network of organizations and commands. Among its many other responsibilities, EP&E [Enterprise Programs and Engineering] ensures configuration management and information assurance for the LandWarNet. How do you balance the need for security with the need for Soldier accessibility?

Lawrence: Balancing security with access isn't a new problem. It was with us when messages were written on paper and carried by a courier and remains with us in the current age of social networking sites like Facebook and MySpace. What has changed is the ease with which bad actors can try to disrupt our operations. Notice I said 'try.' Our Soldiers and civilians do a remarkable job in identifying, containing and defeating threats to the network.

But despite our good track record, we can't rest. As I mentioned earlier, a safe, secure network is fundamental to defeating those who would take aim at our nation. 9th Signal Command personnel work 24 hours a day, 365 days a year to ensure information the Soldier receives in the field or garrison is delivered in a manner that ensures the information has not been tampered with or provides information to our adversaries.

We can only do this by ensuring that adequate information assurance controls are in place to ensure timely delivery of trustworthy information to only the audience to which it was intended. Sometimes that means extra work. Sometimes it means less access than some might like. In the end though, it's about saving lives and winning wars; something we can't do unless the Soldiers engaged in those wars have confidence that the network they rely upon is secure.

CHIPS: Can you talk about the U.S.-based signal command scheduled to attain full operational capability by 2010?

Lawrence: I'd love to. That would be 7th Signal Command (Theater). The command stood up earlier this year and is scheduled to achieve full mission capability by Jan. 16, 2010. 7th Signal Command (Theater) is the heart of the continental United States portion of the Army network and will initially command and control 39 separate elements located at posts, camps and stations across the country, as well as two Theater Strategic Signal Brigades: the 93rd at Fort Eustis, Va., and the 106th at Fort Sam Houston, Texas. Once it's fully in place, the command will extend the Army's GNE capabilities to the operating and generating forces located within CONUS, providing integration, security and defense of the network.

NETCOM/9th SC (A) Commanding General Maj. Gen. Susan Lawrence and Command Sgt. Maj. Donald Manley unfurl the new colors of the 7th Signal Command (Theater) during an activation ceremony March 6, 2009, at Fort Gordon, Ga.

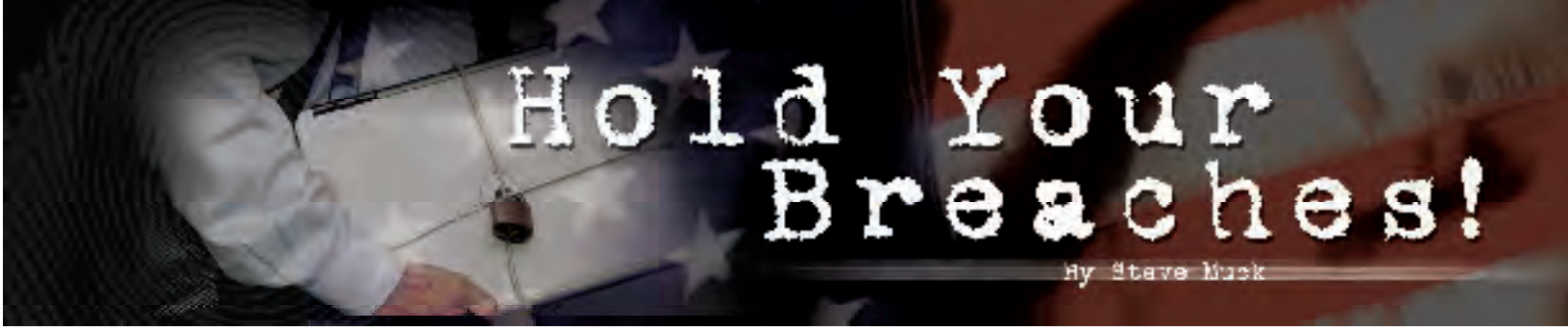
CHIPS: Can you discuss what's going on in each Signal Command and organization under NETCOM/9th SC (A)?

Lawrence: Everyone on the team has been extremely busy as we continue to operationalize the Global Network Enterprise. 5th Signal Command (Theater), together with 7th Signal Command (Theater), played an important role when they led the NSC OPVAL I discussed earlier. This assessment proved that we can seamlessly transition a Brigade Combat Team and its data from CONUS to OCONUS through all phases of operation.

Of course, Iraq, Afghanistan and Kuwait remain the focus of much of our activity. Our units there have been extremely busy, both in supporting ongoing operations and in the build out of the region's communications infrastructure. We achieved a major accomplishment recently with the completion of the Fixed Regional Hub Node at Camp Arifjan, Kuwait. This hub provides up to 48 links of frequency division multiple access and time division multiplex access satellite connectivity, as well as 12 links of mounted battle command on the move and airborne command and control to support warfighter communications in Afghanistan, Kuwait and Iraq.

Meanwhile, in the Pacific, the 311th Signal Command (Theater) has been working closely with the CIO/G-6 Cyber and 9th Signal Command to establish effective security standards for the portion of the LandWarNet falling within their area of operations. You only need to read the newspaper to recognize the importance of information assurance and cybersecurity to operations in this critical part of the world.

Also in the Pacific, the 1st Signal Brigade in Korea is assuming the Joint Command Information Systems Activity (JCISA) mission from U.S. Forces Korea (USFK). Once the transfer is complete in FY10, 1st Signal Brigade will be the primary provider of C2 communications throughout the entire Korean theater. CHIPS



The following is a recently reported compromise of personally identifiable information (PII) involving the theft of storage media containing personal information. Incidents such as this will be reported in each 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 Privacy Office.

The Incident

On July 27, 2009, the DON CIO Privacy Office received a breach report that initially was thought to be one of the DON's largest and most egregious to date. While only sketchy details were received in the first report, the DON CIO alerted the Under Secretary of the Navy, Navy Chief of Information (Public Affairs), Naval Criminal Investigative Service (NCIS) Headquarters and the Defense Privacy Office, then waited for updates to come in. Here is a summary of what was first reported:

> *"A headquarters complex was burglarized over the weekend. Numerous items, including storage media, were stolen from our workspaces. Police and local NCIS have been contacted. At least 10 laptops and 9 external hard drives were stolen. One laptop contained a file with approximately 60 system passwords/usernames/secret words along with the link to the related sites; a file that contained personal financial data including bank accounts, investment accounts, credit cards, salaries for myself and my wife, expenses, gifts and overall balance sheet.*
>
> *The file also contained links to the various financial institutions, as well as passwords/usernames/secret words and phone numbers; my entire contact list which included work and personal cell phone numbers, addresses, and personal notes, such as birthdates for friends and family; a file that recorded my lifetime government pay, bonuses, awards, promotions and salary; 'government only' contract sensitive information; discrimination and hostile work environment correspondence and a host of other privacy or sensitive information."*

This incident was most disturbing because it involved theft and appeared to target storage media that held large amounts of data that were easily transportable.

Follow-up reports provided a much better outlook with regard to potential damage to the DON and to affected personnel.

In the final analysis, only one laptop contained PII that was considered "high risk," affecting eight individuals. Most of the stolen storage media were either brand new (still in the box) or encrypted with the GuardianEdge encryption solution. An investigation is ongoing to identify the perpetrators. CHIPS

Lessons Learned

Insider threats continue to cause the most concern with regard to PII data and the high potential for identity theft.

- Physical security plans must be continually scrutinized and updated.
- As a best practice, never store your PII on a government computer.
- Personnel should never store unencrypted passwords/usernames/secret words and links to URLs on a government computer.
- External hard drives are becoming as vulnerable as thumb drives; a best practice should be to physically secure them at the end of each workday.
- Regardless of who owns the equipment, inventory controls must be in place and tightly enforced.
- Full disc encryption works.

The theft of storage media containing PII with data at rest encryption should be reported to the U.S. Computer Emergency Readiness Team (US-CERT) within one hour even though it is generally not considered a high risk event.

US-CERT
www.us-cert.gov

DoD Privacy Office
www.defenselink.mil/privacy

DON CIO Privacy Office
www.doncio.navy.mil

Additional Privacy information can be found on the DON CIO Web site, www.doncio.navy.mil.

Steve Muck is the DON CIO privacy team lead.

New DON EA v1.0 Supports Investment Decision Making

By Michelle Derus and Victor Ecarma

The Department of the Navy (DON) Chief Information Officer recently released the DON Enterprise Architecture Version 1.0 (DON EA). It provides the management foundation necessary to transform the Navy's systems and Information Technology/ National Security System (IT/NSS) investment decision-making processes to an optimized state. The memorandum may be downloaded from the DON CIO Web site by going to www.doncio.navy.mil and clicking on the Policy and Guidance link.

The DON EA structure, as depicted in Figure 1, is designed to ensure uniformity, standardization, modernization and interoperability of systems across the department and promote efficient and cost-saving investment management, capital planning and control and capabilities-based acquisitions.

The framework identifies operational and mission requirements, determines capability and performance gaps and shortfalls, and supports effective and efficient investment management decisions to enable the DON to meet the current and future needs of the warfighter and warfighter-support operations.

The DON EA documents key IT/NSS attributes related to achieving DON objectives and outcomes. This initial version of the DON EA focuses on establishing a baseline framework of core principles and rules that are tied to underlying policies and guidance. The DON EA is linked to the appropriate laws, regulations, policies and guidance, providing a means for users to navigate through the many applicable legislative mandates, federal regulations, executive orders and IT architecture standards.

The DON EA consists of an integrated set of models and products. The DON EA "Description" describes the manner in which the DON EA will be developed and implemented, and the All View-1 (AV-1) serves as an executive summary and overview of information for all EA products and a central source for definitions. The DON EA framework is comprised of an Abstract Layer, Capstone Layer and a Solution Layer, which are described in the AV-1, providing a comprehensive department-wide architecture view.

The DON CIO began assessing compliance of IT/NSS investments with the DON EA on Oct. 1, 2009. This assessment is conducted using three existing processes: DON Business System Investment Review process; Title 40/Clinger-Cohen Act (Title 40/ CCA) confirmation process; and the Mission Area Chief Engineer (MACE) review process. Currently, the DON Business System Investment Review is applicable to all proposed obligations of development or modernization funding for business systems. Under this process, proposed investments are assessed for their compliance with the Department of Defense Business Enterprise Architecture (DoD BEA).

Starting Oct. 1, 2009, the following changes to this process were implemented:

✓ The DON Business System Investment Review process was renamed the DON Information Management/Information Technology Investment Review.

✓ The review process was expanded to include other mission area investments (e.g., development of a shared data environment or piloting of a business capability) rather than only those associated with a "business system."

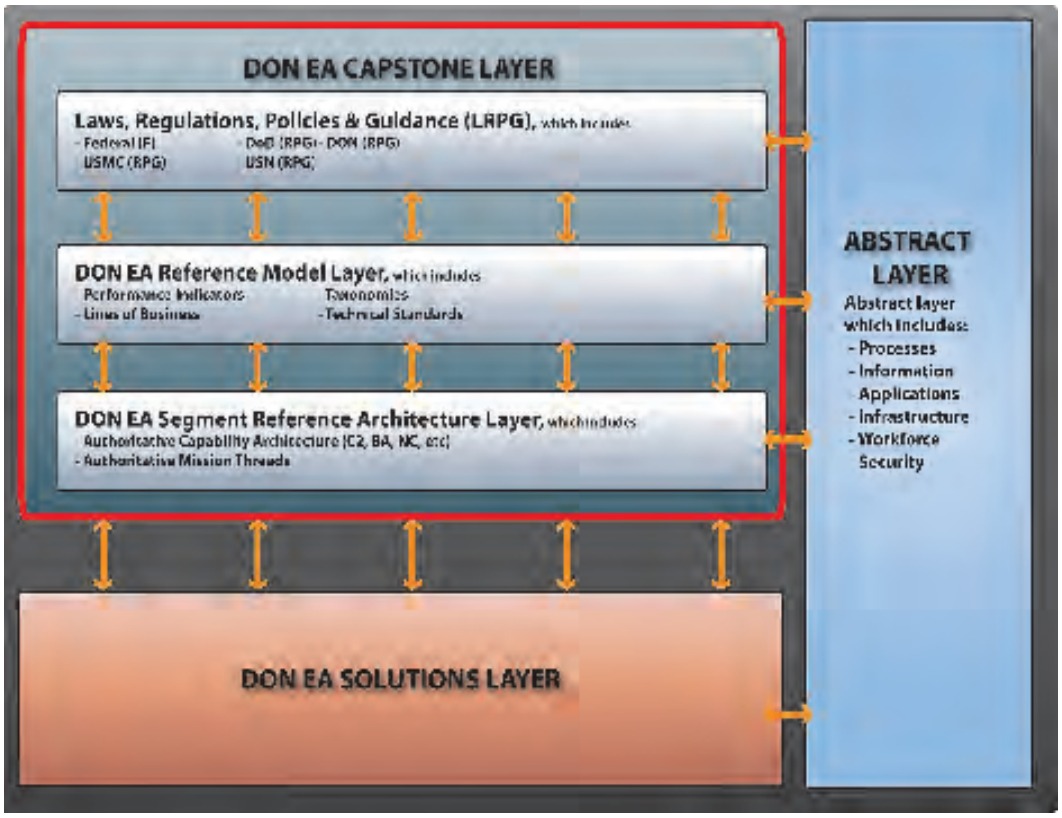


Figure 1. The DON EA structure is designed to ensure uniformity, standardization, modernization and interoperability of systems across the department, and to promote efficient and cost-saving investment management, capital planning and control, and capabilities-based acquisitions. The framework identifies operational and mission requirements, determines capability and performance gaps and shortfalls, and supports effective and efficient investment management decisions to enable the DON to meet the current and future needs of the warfighter and warfighter-support operations.

✓ The review process was expanded to include proposed investments in the Enterprise Information Environment Mission Area of $1 million or more.
✓ All proposed investments will be assessed for compliance with the DoD BEA, the DoD Information Enterprise Architecture and the DON EA.

Updated guidance for implementation of DON EA compliance assessments, as part of the Title 40/CCA and MACE processes, will be forthcoming. In addition to assessing compliance with the DON EA, the DON CIO will work closely with appropriate Navy, Marine Corps and Secretariat level organizations to incorporate DON EA compliance assessment into the Program Objective Memorandum (POM) process and budget phases of the Planning, Programming, Budgeting and Execution process.

In addition, the upcoming DON Architecture Product Guide Version 1.0 will be used in the development of "Solution Architectures" — a description of the end-to-end design responsibility required to address a specific problem or requirement and the dependencies that need to be addressed.

These solution architectures are developed as required to supply information about the various "systems" that will be developed to fulfill a needed "operational" capability. The primary stakeholders for solution architecture are: program managers, system users and developers.

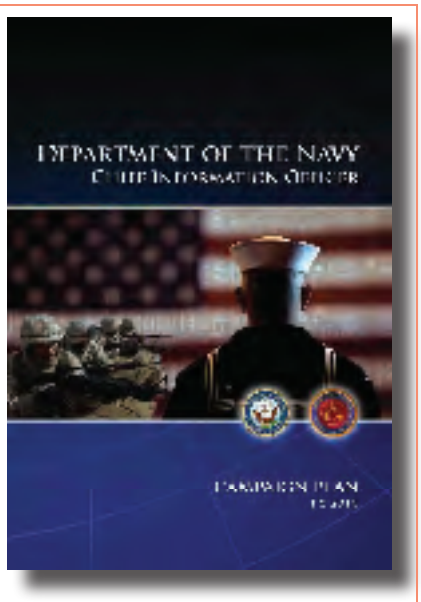
While this initial release represents a strong beginning, the DON EA will always be a work in progress. Future releases of the DON EA will include refined processes and products essential to the warfighter and warfighter support operations and will increasingly guide the department's IT investment decision-making processes. Each DON EA layer will be expanded as more architecture products and views are expanded, enhanced or developed.

Implementation of the DON EA will provide a more robust understanding of the Navy's business architecture and how its investments and systems align with this model. In the near-term, the DON EA will be broken into more granular functions, processes and activities within each business component. Ultimately, the DON EA will define the manner in which all components of the enterprise work seamlessly to ensure business and technology alignment; realize operating efficiencies; identify cost savings and cost avoidance; and provide adaptability for more responsiveness to evolving warfighter requirements.

The DON EA governance structure and associated processes will enable the achievement of that vision through a well-defined and well-orchestrated transformation plan. The DON EA will be updated twice a year. CHIPS

Michelle Derus and Victor Ecarma provide support to Naval Air Systems Command and DON CIO respectively to advance Enterprise Architecture throughout the DON.

Campaign Plan Highlights DON CIO FY 2010 Focus Areas



The Department of the Navy Chief Information Officer has released the DON CIO Campaign Plan for FY 2010, which outlines the major DON information management/information technology (IM/IT) efforts, tactics and deliverables expected during the next fiscal year.

Throughout FY 2010, the DON CIO will concentrate on enabling improved IT for the warfighter through: a secure infrastructure; the future networking environment; effective management and use of the spectrum; improved management of IT investments; improved information sharing and knowledge management; a capable and trained IT workforce; and an aligned governance structure for agile decision making.

The campaign plan supplements the forthcoming DON IM/IT Strategic Plan for FY 2010-2012; it provides an outline of the initiatives the DON CIO considers most important to ensuring that the office has the most impact through FY 2010 and that the needs of the warfighter are met.

Go to the DON CIO Web site to obtain a copy of the Campaign Plan and for other news and policy information. CHIPS

www.doncio.navy.mil

A Breakthrough in Promoting DoD Certification and Accreditation Reciprocity

By Eustace D. King

Defense Department information systems (IS) are routinely deployed across the globe, embedded in host enclaves and connected to naval operational networks. Command and control, logistics, intelligence — regardless of the function, all information systems must be assessed to meet security requirements prior to connection.

Reciprocity is the mutual agreement among participating enterprises to accept each other's security assessments to reuse IS resources and/or accept each other's assessed security posture to share information. Without reciprocity, the receiving activity must conduct a security certification and accreditation process (C&A) from square one.

Air Force Maj. Gen. Michael J. Basla, then Vice Director, Command, Control, Communications and Computer Systems for the Joint Staff, reflected on the negative impact of reciprocity delays on the warfighter, "From the warfighting mission area perspective, we have witnessed the protracted delay of fielding capability to the warfighting community due to lack of comprehensive security review criteria and an executable, repeatable process."

On July 23, 2009, reciprocal acceptance of information systems certification and accreditation documentation within the DoD took a giant leap forward with the issuance of a groundbreaking memorandum.

The memorandum, "DoD Information System Certification and Accreditation Reciprocity," seeks to ensure the rapid and secure fielding of DoD information systems by providing clear communication of the reciprocity policy and implementing guidance to establish a systematic, repeatable process.

The memorandum was endorsed by the four DoD mission area (MA) principal accrediting authorities (PAAs) responsible for resolving accreditation issues within their respective mission areas working with other PAAs to resolve issues among mission areas as needed.

The PAAs and their associated MAs are:

- Assistant Secretary of Defense (Networks and Information Integration)/DoD Chief Information Officer, ASD (NII)/DoD CIO; Enterprise Information Environment MA
- Under Secretary of Defense for Acquisition, Technology and Logistics, USD (AT&L); Business MA
- Chairman of the Joint Chiefs of Staff; Warfighting MA
- Under Secretary of Defense for Intelligence, USD(I); Defense Intelligence MA

In the memorandum, the principal accrediting authorities state that the timely deployment of information systems is critical to attaining the department's strategic vision of netcentricity. They also stress that reciprocity of accreditation decisions and the artifacts contributing to the accreditation decision will advance information sharing; reduce rework and cycle time when establishing combined and joint information systems and networks; and support DoD mission accomplishment.

The memorandum reaffirms that each DoD information system has one, and only one, assigned designated accrediting authority (DAA), who is responsible for issuing an accreditation decision based on achieving an acceptable risk posture, and it requires due diligence in complying with the DoD Information Assurance Certification and Accreditation Process (DIACAP). However, it also recognizes that DoD components receiving and deploying DoD information systems are also stakeholders, and therefore must be provided situational awareness and access to C&A data to make informed connection and net-worthy decisions.

The PAAs recognize

that reciprocity requires a level of trust based on transparency, uniform processes and a common understanding of expected outcomes, and the memo provides for continuous visibility of information assurance C&A packages, deployment milestones and transparency of risk management decisions.

Connection and net-worthy requirements for other than IA can also have an impact on a DoD component's decision to accept deploying information systems. These requirements include interoperability and supportability issues other than security and may have an impact on network operations.

In order to ensure that these requirements are not addressed at the last minute and become limiting factors in information systems deployment, the memorandum facilitates early visibility and active involvement in the net-worthiness and connection approval processes.

The memorandum provides terms and conditions for accomplishing timely reciprocity within DoD for the two types of information systems deployments: enterprise-wide and non-enterprise-wide.

An enterprise-wide deployment occurs when a Defense Department information system is deployed to multiple components across the DoD information enterprise.

A non-enterprise-wide deployment occurs when a Defense Department information system is deployed to two or more DoD components, but is not designed to satisfy a DoD-wide requirement.

Governance responsibilities for the Defense Information Assurance/Security Accreditation Working Group (DSAWG) and the Defense Information System Network/Global Information Grid (DISN/GIG) Flag Panel are identified.

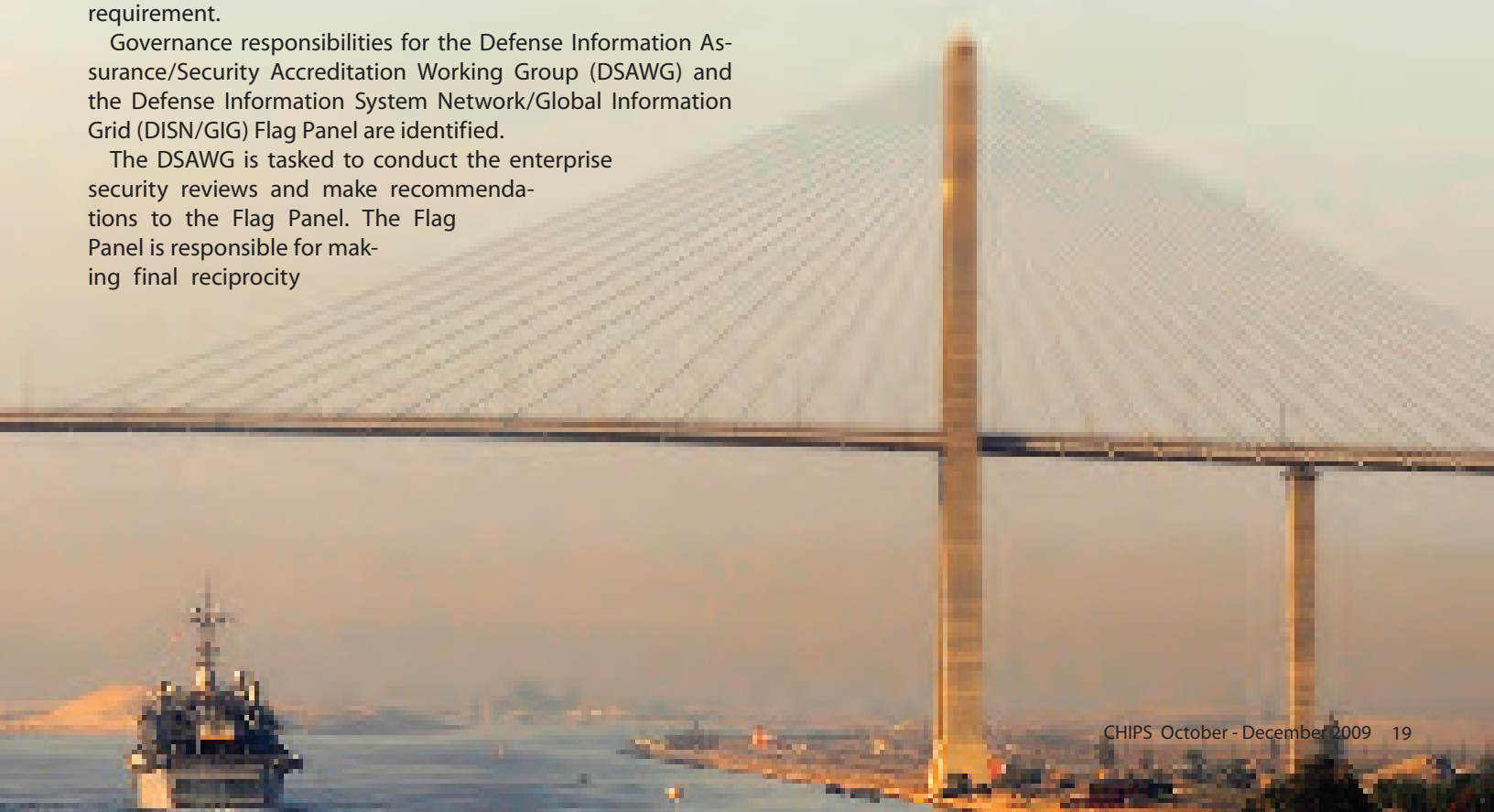
The DSAWG is tasked to conduct the enterprise security reviews and make recommendations to the Flag Panel. The Flag Panel is responsible for making final reciprocity decisions that are binding upon both the deploying and receiving communities.

Reciprocity within DoD has been a tough issue to resolve. The reciprocity memorandum, when fully implemented, will be an important tool in achieving rapid and secure fielding of DoD information systems.

As Maj. Gen. Basla said, "The expectation over time is that the reciprocal acceptance of accreditation decisions will cease to be one of the systemic problems impeding the effective and timely delivery of information systems across all the mission areas."

The DoD Reciprocity Memorandum is available for download from the DON CIO Web site at www.doncio.navy.mil under the Policy and Guidance link. CHIPS

Mr. Eustace King is assigned to the Office of the Deputy Assistant Secretary of Defense for Cyber, Identity and Information Assurance. As the principal authority within DASD/CIIA for ensuring successful implementation of the DIACAP, King provides oversight and community outreach to ensure understanding and adherence to DIACAP policy. He also chairs the DIACAP Technical Advisory Group with responsibility for DIACAP configuration management.



KM IN A STRIKE GROUP

The 7 Minute Drill

By Capt. Danelle Barrett

The strike group knowledge manager faces many challenges to ensure seamless information flow between warfare commanders, strike group units and other organizations critical to operations.

The knowledge manager's role is critical to identifying and ensuring a shared awareness of the Commander's Critical Information Requirements (CCIRs) and decision cycle, the battle rhythm supporting that cycle, and the means for effective information exchange among players.

Several processes and tools can assist, including establishing a Knowledge Management Working Group; assessments such as the "7 Minute Drill" for battle rhythm analysis; developing an information management matrix; and codifying business rules in operational tasking orders (OPTASKs) for standardization.

KM ACROSS THE STRIKE GROUP

The KM Working Group provides a forum for the knowledge manager to coordinate KM and information management initiatives and ensures a common shared awareness of issues and solutions. The KM Working Group operates under a charter that provides a framework for the scope of the group's efforts to improve information exchange of the information resources within the strike group.

Specific KM Working Group activities should include sharing best practices for wider strike group implementation; prioritizing KM and IM initiatives; identifying potential resource shortfalls for successful implementation; recommending changes to improve IM policies and procedures; suggesting standardized processes to capture and codify lessons learned within the strike group; sharing with other Navy and joint organizations; implementing IM/KM training for personnel; standardizing Collaboration at Sea (CAS) Web pages and document management; identifying metrics for baselining and gauging success of KM initiatives; and identifying additional tools required to accomplish KM/IM objectives.

Because KM is essential in all warfare areas and across staff functional areas, I suggest that the group include permanent representation from each of the warfare commanders, every unit in the strike group and special assistants to the commander. Other key stakeholders or change agents can be invited as ad hoc members or to support specific initiatives.

It is important to engage the KM Working Group early in the work-up cycle prior to the first group sail to ensure that participants understand their KM roles and responsibilities and become active proponents of change. Whenever possible, core membership should remain constant throughout workups and the deployment.

Due to the dispersed location of participants, a low bandwidth chat tool is the recommended means to conduct KM Working Group meetings. CAS is recommended for document sharing to improve collaboration between bandwidth disadvantaged platforms.

Personnel selected to represent a warfare area or unit should have a solid understanding of the strike group mission, operational tasking and their area's existing decision-making processes. Members of the Working Group will be instrumental in conducting KM assessments and implementing process changes; they need to be both comfortable and aggressive in eliciting information and proactive in pushing solutions.

KM ASSESSMENTS

Understanding and prioritizing the focus of KM efforts can be a daunting task given the complexity of the strike group decision-making environment. The knowledge manager can help frame the problem by identifying the processes needed to support effective decision making and information exchange by conducting a KM assessment.

KM assessments can identify gaps that require corrective action and are valuable in discovering what assessment respondents consider successful processes that should be continued or replicated in other operations.

PORTSMOUTH, England (April 5, 2009) The aircraft carrier USS Theodore Roosevelt (CVN 71) is anchored in the English Channel as a ferry prepares to transport Sailors to Portsmouth Harbor. Theodore Roosevelt and Carrier Air Wing 8 Sailors are on a port visit to Portsmouth on their way home from a seven-month deployment supporting Operation Enduring Freedom. U.S. Navy photo by Mass Communication Specialist 3rd Class Christopher Hall.

The KM assessment can take many forms such as an automated survey tool or personal interview. Interviews often provide the most comprehensive feedback and are recommended over automated tools because they provide more detail and immediate feedback. Regardless of the means for collecting information, when conducting the KM assessment it is important to target those personnel who understand the strike group mission and its context within the larger operational environment to get the most relevant feedback.

The initial KM assessment is the first step in a larger KM continuum that should include reassessments of strike group information sharing and decision-making processes. It will also provide a starting point for the focus of effort and a baseline to gauge the success of subsequent KM efforts to improve the decision cycle and information exchange processes.

The knowledge manager should identify trigger events or a specific periodicity for conducting reassessments. Metrics should be developed and maintained to quantify degrees of improvement whenever feasible.

Some key items to cover in the KM assessment include:

- Processes and process owners, how the process contributes to the mission and identification of key supporting players;
- Process inputs and outputs, when they are due, format and information exchange mechanisms that support the process;
- Known overlaps between processes;

• Cultural issues that may adversely impact process success; and
• Information technology tools used in support of this process, such as collaborative tools like CAS, portals, chat, blogs and any other tools that might enhance process effectiveness.

An important byproduct of the KM assessment is the IM Matrix, a document the knowledge manager develops to codify critical information flows supporting the battle rhythm and other key decision processes.

The IM Matrix lists what the information is; its relative importance (high, medium, low); the drafter or information owner; key collaborators; who the information is provided to and how it is provided, for example, orally in person, via video teleconference, posted to a Web site or network drive; and any other relevant information. It also includes technical attributes of the information, such as format type, means of delivery, and nontechnical attributes, such as classification, releasability and perishability.

The IM Matrix easily identifies information dependencies that must be considered to ensure the right information is available to decision makers at the right time and in the correct format.

Information gaps that could cause a process or decision breakdown should be quickly identified and corrected. For example, the input for an Air Tasking Order is needed by 1200, but the targeting working group is scheduled to meet at 1300 so input will not be provided on time. The IM Matrix should be updated as command and control structures, roles, missions and their corresponding information exchange requirements evolve.

Another key assessment is the battle rhythm analysis. The battle rhythm is the heartbeat of operations on a strike group staff and consists of a series of recurring decision points and events throughout the day that must be properly aligned to support operations.

The battle rhythm includes meetings by boards, centers, cells or working groups, and events such as the release of the "Commander's Daily Intentions Message." These must be carefully orchestrated and synchronized to ensure information flows properly to enable timely and accurate decision making.

The battle rhythm analysis must not only take into account the staff's decision points and events but those of higher authorities, subordinate organizations and other ancillary partners (i.e., another supporting joint task force, group or unit).

While the initial analysis is a snapshot in time, like the IM Matrix, the battle rhythm must be periodically revised as operations evolve and tasks change. As changes occur, the battle rhythm analysis should be repeated to identify any necessary recalibration or realignment of specific battle rhythm events.

A tool commonly used by knowledge managers to conduct the battle rhythm analysis is the 7 Minute Drill, a concept

7 Minute Drill Example

Main Planning Group (MPG)

Purpose: Allow Warfare Commanders, USS Theodore Roosevelt (TR) Operations Officer and Assistant Chiefs of Staff (ACOS) to coordinate and synchronize medium range Strike Group Schedule of Events (SOE) (24 to 96 hours) and events for CTF 50 and USS Theodore Roosevelt Carrier Strike Group (TRCSG) with higher level guidance.

Product/Output: Shared situational awareness of requirements, capabilities, limitations and operational plans across all warfare areas. Inputs into the Commander's Daily Intentions Message, Strike Group SOE, CTF 150 SOE and Air Plan.

Procedure/Techniques:
When: 10:15 Mon, Wed, Sat
Where: TRCSG War Room
Inputs: CTF 50 daily slides, SOE, Material Status, Intel Brief, Air Plan, higher level guidance from Daily Brief and Warfare Commander's Council Board.
Key Tasks:
• Identify and resolve SOE issues and conflicts
• Ensure SOE are aligned with higher level tasking
Membership: TR OPS, N2, N3, N4, Deputy Information Warfare Commander, DESRON Chief of Staff, Strike Ops Officer, TR Air Ops, N3 Planner, N3 Senior Watch Officer, Air Defense Coordinator Liaison Officer, Meteorological Officer, TRCSG Communications Officer, Judge Advocate General and Center for Naval Analyses representative.
IM/KM Tools: Collaboration at Sea, PowerPoint briefing slides and War Room video display.

GULFOFOMAN(March4,2009)AshooterlaunchesanEA-6BProwlerassignedtothe"Shadowhawks"of ElectronicAttackSquadron(VAQ)141fromtheaircraftcarrierUSSTheodoreRoosevelt(CVN71)during routineflightoperations.TheodoreRooseveltandCarrierAirWing8areoperatingintheU.S.5thFleet areaofresponsibility.U.S.NavyPhotobyMassCommunicationSpecialist3rdClassJonathanSnyder.

Information gaps that could cause a process or decision breakdown should be quickly identified and corrected.

originally discussed by retired four-star Army Gen. Gary Luck in his paper, "Insights on Joint Operations: The Art and Science, Best Practices, The Move toward Coherently Integrated Joint, Interagency, and Multinational Operations" of September 2006.

The concept behind the 7 Minute Drill is that each event in the battle rhythm should be scrutinized to determine how it contributes to the decision cycle. The 7 Minute Drill documents the event and purpose and the IM/KM tools needed to accomplish the event, the product or output, and the procedures and techniques used (where and when it is conducted, the inputs, key tasks and membership).

As with the IM Matrix, the battle rhythm analysis can identify key information linkages and the continuity that must exist to provide the correct information to decision makers.

Examples of 7 Minute Drills on the Theodore Roosevelt Carrier Strike Group battle rhythm, include the Commander's Daily Brief and the Main Planning Group. The box on the previous page shows the Main Planning Group 7 Minute Drill.

Once the 7 Minute Drills are completed, the knowledge manager, warfare commanders and other staff personnel align the events, ensuring proper synchronization for effective information flow that will shorten the decision cycle.

When analyzing the battle rhythm, the 7 Minute Drills will help with strike group controlled events, but other external factors must also be considered, such as the numbered fleet or joint commander's battle rhythm; potential changes to the command and control structure or mission assignments; and the enemy's battle rhythm, for example, the enemy only conducts operations during daylight hours.

Additionally, analysis of information exchanges necessary to support the battle rhythm between the strike group and coalition and interagency partners or nongovernmental organizations must be identified early to ensure sufficient time is built into the battle rhythm to account for information releasability requirements.

GULF OF OMAN (Feb. 9, 2009) An HH-60H Sea Hawk helicopter assigned to the "Tridents" of Helicopter Anti-Submarine Squadron (HS) 3 embarked aboard the aircraft carrier USS Theodore Roosevelt (CVN 71) hovers into position during cast and recovery operations with demolition materials. Theodore Roosevelt and embarked Carrier Air Wing 8 are operating in the U.S. 5th Fleet area of responsibility. U.S. Navy photo by Mass Communication Specialist 3rd Class Jonathan Snyder.

CODIFYING THE RULES

The strike group knowledge manager promulgates documents that codify processes and business rules. Two primary documents are the OPTASK IM and OPTASK Chat. These are normally coalition, joint task force or strike group specific and should be released early in the work-up cycle to ensure units are trained and familiar with the processes prior to the start of combat operations. The documents will need to be revised as strike group units transition to other theaters of operations and are assigned new missions.

When a strike group is assigned as the lead for more than one task force, it will normally produce a separate OPTASK IM and OPTASK Chat for each task force. This is especially important because different processes may be used for various missions and task force compositions, which may include coalition partners or other non-Defense Department organizations.

Many task forces today are dynamic and subject to frequent changes in participants. For example, the members of Coalition Task Force 152 (maritime security operations in the central and southern Persian Gulf) and Coalition Task Force 151 (counter-piracy operations) in the 5th Fleet often change on a daily basis, so careful attention must be paid to those fluctuations and shifts in roles and responsibilities.

A fine balance must be achieved in the promulgation of KM guidance. If guidance is too specific, it will require constant modification; if it is too generic, it will be useless. The KM should work with key stakeholders and higher authority to ensure that processes articulated in the OPTASK IM and OPTASK Chat are relevant, executable and meet mission requirements. Proper execution of guidance and adherence to policies must be a priority for the warfare commanders and all other members of the strike group and task force.

The knowledge manager plays a critical role and has many tools available to enable decision superiority within a strike group. These tools are part of an iterative process that requires constant tuning and commitment throughout the strike group to ensure mission success. CHIPS

Capt. Barrett is an Information Professional Officer and the assistant chief of staff for C4 for Commander, Carrier Strike Group 2.

Radio Frequency Congestion

We are all familiar with overcrowding and traffic congestion. Most people in the United States experience long work commutes, jammed shopping malls, as well as long lines at restaurants, train stations and other locations where people frequently congregate.

However, congestion in these occurrences usually has peaks and valleys, and many times, people can arrange their schedules to avoid peak times. Some people living in rural areas have never experienced overcrowding.

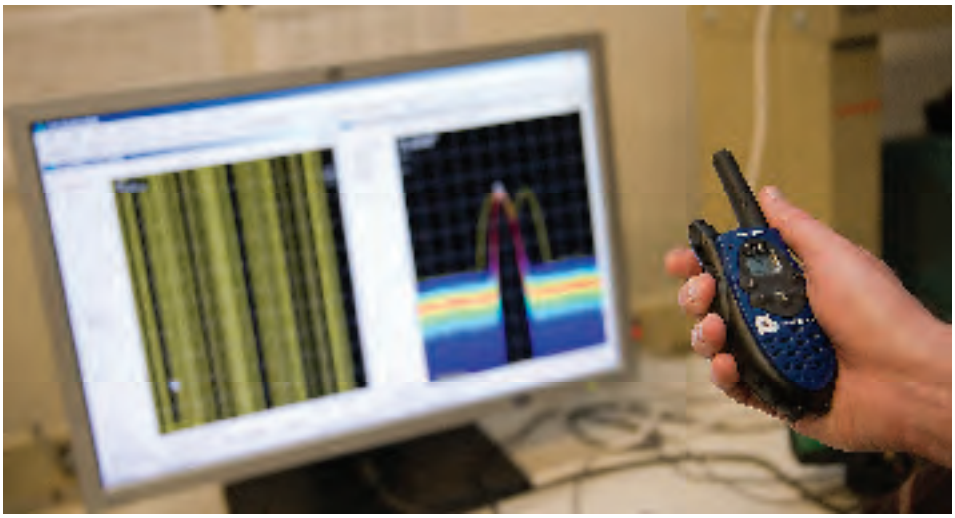
The use and congestion of radio frequencies (RF) parallels that of roads, shopping malls and restaurants. While radio frequencies may be congested in some geographical areas, many geographical areas of the world and of the United States rarely, if ever, experience frequency congestion.

Natural resources such as oil, coal and precious metals are limited or finite and are in high demand; similarly, radio frequencies from the electromagnetic spectrum are also in high demand.

However, radio frequencies have one significant difference when compared to those other resources. Radio frequencies are instantaneously recyclable; the use of a frequency to communicate between radio devices does not deteriorate or consume that frequency.

Because of this radio frequency characteristic, radio frequencies can be shared and reused worldwide. Consequently, due to the ability to reuse and renew radio frequencies, congestion is generally limited to geographical areas where population density is high. This means that the preponderance of RF congestion is experienced at specific, geographical locations and predictable times that directly correlate to the typical use of wireless capabilities and devices.

For example, radio frequency use surges in the morning as people commute to work, during the commute home and into the early evening.



INDIAN HEAD, Md. (March 6, 2009) Personnel at the Navy Explosive Ordnance Disposal (EOD) Technical Division, Indian Head, Md., demonstrate how radios and walkie-talkies send out frequencies that could detonate improvised explosive devices. U.S. Navy photo by Mass Communication Specialist 2nd Class Jhi L. Scott.

But not all spectrum usage is predictable. For the Navy and Marine Corps, unanticipated congestion within certain frequency bands is increasing. The requirement for 24/7 operations places unique demands on the use of radio frequencies, and new requirements for sensor and unmanned aerial system capabilities now strain available RF resources.

This RF congestion has reached the point where some strategic and tactical operations, such as use of unmanned aerial systems, must be scheduled to avoid frequency fratricide with other UAVs and other RF equipment operating within the same geographical area.

RF congestion is not going to diminish anytime soon. The use of RF-enabled capabilities continues to increase. However, there are actions that can be taken by warfighters and acquisition officials to minimize RF congestion.

Warfighters should always make their RF requirements known to responsible spectrum planning and operations personnel and always use only radio frequencies that have been provided by such personnel.

Acquisition officials should always consider radio frequency use from the warfighter's perspective when developing or acquiring systems and equipment.

Spectrum is a resource in high demand throughout the world. Use of the spectrum fuels the economy and enables a plethora of Navy and Marine Corps capabilities. While radio frequency congestion is a reality for Sailors and Marines, employing spectrum-dependent equipment in a congested environment can be managed if warfighters and acquisition officials recognize the risks and challenges associated with its use. CHIPS

Tom Kidd is the Director of Strategic Spectrum and Wireless Policy for the Department of the Navy. In addition to "Full Spectrum," he also authors (or sponsors) the recurring CHIPS series "Going Mobile" which focuses on enterprise mobility and the DON Wireless Working Group. Please send questions to donwirelessteam.fct@navy.mil.

GOING MOBILE

Putting Text to the Test

By Mike Hernon and Bob Turner

Delivering a robust enterprise mobility capability to the Department of the Navy workforce requires leveraging various wireless tools at our disposal. One such tool, Short Message Service (SMS), or text messaging, is often overlooked but can provide significant benefits when used appropriately.

Industry statistics, compiled by CTIA–The Wireless Association, show a definitive trend for individuals to let their "fingers do the talking." More people are using their phones for text messages and less to actually talk. In 1987, the average mobile call length was 2.33 minutes.

In the following years, the number of mobile calls continued to grow until peaking in 2003 with an average call length of 3.07 minutes. By 2008, average call length was down almost a third to 2.27 minutes — less than what it was in 1987.

On the other hand, the number of text messages has increased dramatically from 14.4 million messages per month in 2000 to more than 110.4 billion per month in 2008.

Likewise, an analysis of DON usage shows a similar increase in text messaging. It is clear that people, including DON personnel, are changing the way they communicate.

Is it Safe?

There is a perception in many quarters that since text messaging is not secure, it cannot be used within the Defense Department or DON. Indeed, many believe that there is a department-wide prohibition on its use — which is not the case.

Generally, SMS and Multimedia Messaging Service (MMS) may be used if only unclassified, public releasable (i.e., not "For Official Use Only" (FOUO), sensitive or classified) information will be sent or received.

Additionally, an Executive Order, issued Oct. 1, 2009, prohibits all government employees from texting while driving a government vehicle or privately-owned vehicle while on official business.

There are many aspects of texting that engender concerns regarding information assurance. Short Message Service was not designed to provide a secure, reliable or robust messaging capability. Text messages are not encrypted end-to-end and could potentially be read by people other than the intended recipient.

Further, as texting has grown in popularity it has increasingly attracted the same scam artists and hackers that attack the wired environment.

Techniques such as spamming, phishing and spoofing now use text messages to target mobile phone users and may be more of a threat in this environment because Short Message Service does not provide authentication of either the sender or the content.

Viruses customized for mobile devices can use text messages as an entry point to control or disable a device (in addition to user-initiated downloads and e-mail). The assignment of phone exchanges to mobile operators makes the job easier for attackers because they can better direct their automatic dialers to cellular devices.

So, is it safe? Well, not 100 percent!

"R U OK?"

One of the most appealing aspects of text messages is that experience has shown that during regional or national calamities when cellular networks are bogged down with callers, text messages often get through without any trouble.

This is due to the fact that Short Message Service works on a control channel in the provider's network, not the traffic channel where voice and data services are provided.

This was evident during the Sept. 11 terrorist attacks when network demand seriously obstructed cellular voice traffic in New York City and Washington, D.C., but text messages got through. Thus, there may be circumstances where SMS is the only viable means of communication.

When it comes to cellular devices, most people "Don't leave home without them." As a result, Short Message Service provides an efficient platform for applications beyond standard phone-to-phone messages between two individuals.

There are a number of applications where users can sign up to receive text messages to alert them to pre-defined conditions or circumstances. The National Weather Service provides an alert service for adverse weather conditions in user-defined areas at http://inws.wrh.noaa.gov/.

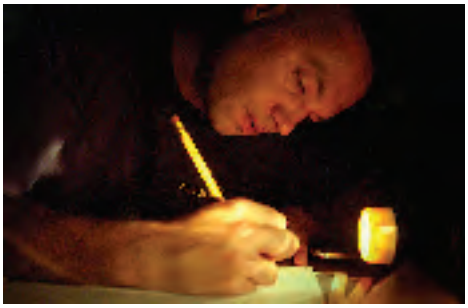
After the devastating hurricanes in 2006, New Orleans launched NOLAReady, a notification system for first responders, as well as the public, at www.nolaready.info. Other applications offer stock market reports, sports scores, e-mail notification and many other alert options.

A number of public safety departments use SMS to track vehicle locations to enhance crew safety as well as to assist in dispatching first responders. A text message has more than sufficient space to transmit GPS coordinates and other data, such as speed and direction, to support this capability. Using SMS also frees up bandwidth for voice or more data-intensive applications.

To protect against viruses and other malware, one popular SMS-based application is not available to DoD and DON users. Downloading any sort of code, such as ring tones or MP3 files, to a mobile device is prohibited under DoD Directive 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG) of April 23, 2007.

Always Practice Safe Texting

None of the mobile technology tools we use are 100 percent secure. Like every



Mobile, Ala. (Aug. 29, 2005) – Coast Guard Petty Officer 2nd Class Justin R. Feussner writes down the locations of stranded individuals in need of assistance in the wake of Hurricane Katrina at Coast Guard Aviation Training Center in Mobile, Ala. With electrical power out, Feussner communicates with the Alabama Emergency Operations Center on his cell phone to coordinate search and rescue operations. U.S. Coast Guard photo by Petty Officer 2nd Class NyxoLyno Cangemi.

other technology we use on a daily basis, the risks and benefits of Short Message Service must be analyzed to determine how to implement this capability. The Navy and Marine Corps Designated Approval Authorities (DAA) conduct such analyses on a daily basis.

The DAAs consider texting to be safe as long as content is limited to only unclassified, publicly releasable data and no applications are downloaded.

Within these constraints, Short Message Service may be used in any manner that might contribute to your productivity or efficiency. Keep in mind that Short Message Service is not a guaranteed delivery system; Marine Corps personnel using text messages during Hurricane Katrina found that while many messages got through, others were delayed by several hours until they were delivered.

In the final analysis, Short Message Service can play a key role in enhancing enterprise mobility across the DON when used appropriately. CHIPS

Mike Hernon is the former chief information officer for the City of Boston and currently serves as an independent consultant to the DON CIO on a variety of telecommunications-related topics.

Bob Turner supports the Naval Network Warfare Command office of the Designated Approval Authority.

Navy ERP Program Receives Positive Operational Test Agency Follow-on Evaluation Reports

By Bob Coble

The Navy's Enterprise Resource Planning (ERP) Program reached another successful milestone with the completion of the evaluation of the Follow-on Operational Test Agency Evaluation Report.

The purpose of this report was to assess the operational effectiveness and operational suitability of Navy ERP System Release 1.0 to provide a fielding recommendation.

"Navy ERP System Release 1.0 is operationally effective and operationally suitable, and I recommend full fielding in accordance with the current schedule," said Rear Adm. David Dunaway, Commander, Operational Test and Evaluation Force.

The Department of Defense Operational Test and Evaluation office concurred with the COMOPTEVFOR finding in a subsequent memorandum to the Under Secretary of Defense for Business Transformation.

The Navy ERP system standardizes and modernizes the Navy's business practices. It provides commanders significantly enhanced visibility into financial, program, workforce and material management information across their areas of responsibility. The Navy ERP system is currently being used by more than 35,000 individuals in three major Navy systems commands.

The Naval Air Systems Command and the Naval Supply Systems Command are currently operating their business activities using Navy ERP as their financial system of record.

The Space and Naval Warfare Systems Command is using the system for training and preparation for an Oct. 1 "Go-Live."

The current Navy program of record calls for the SPAWAR implementation to begin October 2009, and the Naval Sea Systems Command implementation to begin October 2010.

Dr. Jennifer Carter, Navy ERP program manager, said, "This evaluation is a major step forward for the program and the Navy. What has been a promise in development for several years is now an operating, functioning management system that is saving money and providing better information right now to Navy commanders so they can efficiently provide the support Navy warfighters must have. These benefits will continue to increase as we implement the system in more Navy commands."

When the current deployment schedule is completed, the Navy ERP system will support more than 64,000 users and be used to manage more than 53 percent of the Navy's total obligation authority, the money it is authorized to spend.

The Navy directed the implementation of an ERP system as part of efforts to transform its business affairs to more efficiently support warfighter readiness, part of the Navy's maritime strategy.

ERP systems integrate management functions enabling all aspects of a business operation to use the same information, aligning activities and speeding information availability.

The Navy ERP program is part of the portfolio of the Program Executive Office for Enterprise Information Systems. CHIPS

Bob Coble is the Navy ERP public affairs officer.

Lisa Widner, a consultant who assists with Navy ERP classroom training at SPAWAR Headquarters, helps Jim Churchill, program manager, International C4I Integration Program Office, navigate through a Web-based training module Aug. 17. SPAWAR employees are preparing for the command's Oct. 1 Navy ERP "Go Live" implementation date. Photo by Steven A. Davis.

SSC Pacific's Far East C4ISR Division — Sharpening the Tip of the Spear

By Ann Dakis

As the forward deployed arm of Team SPAWAR, Space and Naval Warfare Systems Center Pacific's Far East command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) division in Japan ensures that ship and shore commands in the region remain operationally ready with superior warfighting capabilities.

Led by Officer in Charge Cmdr. Andy Gibbons and division manager Tom Mills, engineering and installation support is provided to U.S. Seventh Fleet and joint and coalition commands.

As well as being OIC, Gibbons is the Naval Sea Systems Command (NAVSEA) strike force interoperability officer. He ensures combat systems are strike group ready and surge capable. Gibbons makes certain that C4ISR systems are integrated and interoperable within the USS George Washington Carrier Strike Group and other ships based in Japan.

Installations of enhanced capabilities are closely monitored, and when issues are identified, Gibbons works with NAVSEA to determine the best resolution.

During a recent visit, SSC Pacific Commanding Officer Capt. Mark Kohlheim complimented the staff, "You're on the tip of the spear — but even more important — you're out here sharpening it … My hat is off to you."

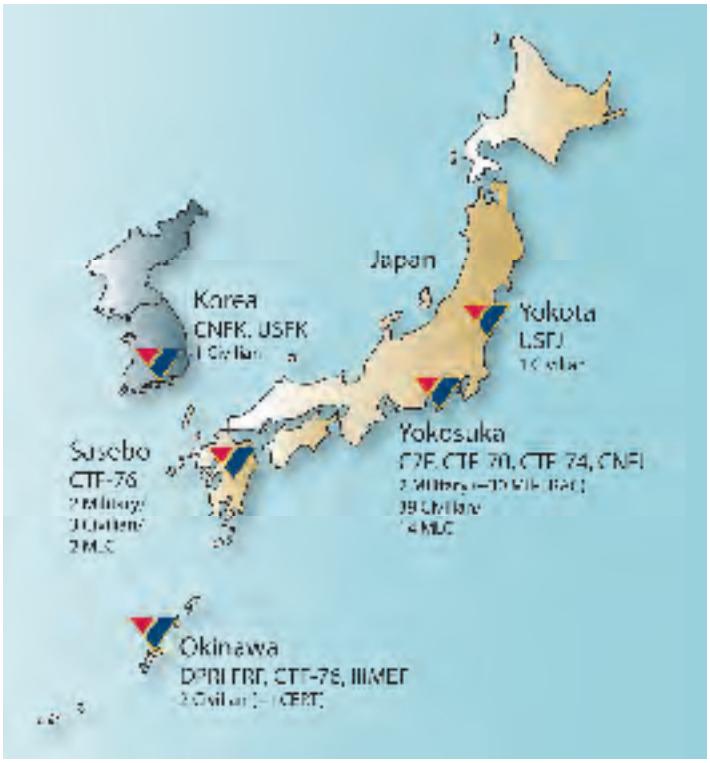
Although there are only about 60 employees at the facility, it has a large area of responsibility including: Combined U.S. Naval Forces Korea and U.S. Forces Korea; Commander Task Force (CTF) 76 in Sasebo; Seventh Fleet, CTF 70 and 74 and U.S. Naval Forces in Yokosuka; U.S. Forces Japan in Yokota; and Defense Policy Review Initiative Futenma Replacement Facility, CTF 76 and III Marine Expeditionary Force (III MEF) in Okinawa.

SSC Pacific's footprint extends to Thailand, Vietnam — even China. SSC Pacific personnel are permanently assigned to 7th Fleet and U.S. Forces Japan and Korea major concentration areas. Mission success is achieved through the teaming of military, civilian and Japanese foreign national employees. There is a status of forces agreement in place which allows Japanese citizens, paid for by the Japanese government, to work alongside their U.S. counterparts in professional roles.

Employees in the fleet engineering and shore engineering branches work together as Team SPAWAR's face to the fleet, interacting daily with operational commanders and their staffs with an aim "to be the world's best provider of integrated C4ISR capability to the warfighter."

The fleet engineering branch, led by Fred Buckley III, focuses primarily on installation of shipboard systems developed by SPAWAR, Program Executive Office (PEO) C4I, PEO for Enterprise Information Systems (PEO EIS) and NAVSEA. The branch also stands ready to provide fleet tech assists and casualty responses. The branch fields installations to naval forces in the Far East that include 11 ships in Yokosuka, members of the USS George Washington (CVN 73) Carrier Strike Group and six units in Sasebo which are part of the USS Essex (LHD 2) Expeditionary Strike Group.

Perhaps the greatest challenge is the compressed timeframe to complete installations. Ships are only available for installations



during their ship's restricted availability (SRA) periods. During SRA periods, the ship's port time is split between modernization (continuous maintenance and Chief of Naval Operations-approved scheduled availabilities), training and inspections.

Buckley explained that a shore project may involve a year's worth of work to install electronics inside a building, but branch personnel have mere weeks to complete a series of complex ship installations.

"We generally have nine weeks to put the products on the ships. We usually do between 13 and 25 installations in that period, and all of them have to be integrated. Every installation I'm doing is a project, requiring all the same elements of project management."

While ships that receive upgrades stateside may remain in the local area for operations and are available for any follow-on work, upgraded ships in Japan immediately get underway following an SRA, which means newly installed upgrades are often put to use the day after delivery.

Occasionally, ships may be required to deploy on short notice in the middle of an SRA so branch personnel must be able to return the ship to an operationally ready state if required.

The fleet support team takes these limitations in stride.

"We say here in FDNF (forward deployed naval forces), we're not special, we're different. Our timelines are just compressed," Buckley said.

Jay Barlis, who is the ship superintendent to the USS Blue Ridge (LCC 19), was recently recognized with a SPAWAR Lightning Bolt award for his participation in fielding a rapid prototype for the Republic of Korea – U.S. Allied Enclave to the Global Broadcast System (GBS) for the USS Blue Ridge. The installation

was the first allied security enclave in the AN/USR-10 GBS Afloat Receive Suite and greatly enhanced the capabilities for Seventh Fleet.

The branch also received several "Bravo Zulus" for performing upgrades to the USS Mustin's (DDG 89) Integrated Shipboard Network System which helped improve the ship's NIPRNET and SIPRNET services. The installations were performed with minimal interruption to the Mustin's daily operations and were accepted as operational without any discrepancies.

The division's shore engineering branch, led by Donnie Camp, focuses primarily on the installation of systems developed by SPAWAR, PEO C4I and PEO EIS. The branch also installs products sponsored or funded by other commands.

"If the project comes from the PEO via the installation management office (IMO) at SSC Pacific as a program of record, we provide a cost estimate, they provide funding, and we do the install," Camp said. "For other command-funded projects, we start from scratch, do a site survey, develop a proposal, gain customer and Fleet Readiness Certification Board (FRCB) approval, procure the material and perform the installation."

Shore facilities are critical to Navy communications. Camp explained, "To a large extent, Navy ships communicate via shore installations so many of our installs involve equipment for communications between ship and shore. Two ships, even if they're sitting right beside each other, cannot communicate without some type of shore facility in the middle. Not always, but in many cases." (This concept is illustrated in Figure 1.)

One of the projects of which Camp is proudest involved the homeporting of USS George Washington to Yokosuka in 2008. Constructing an ashore command center was a requirement to prepare for the carrier's arrival.

"We installed projectors and large screen displays and all types of communication equipment in a room on top of the headquarters of Submarine Group Seven," Camp said. Director, Naval Nuclear Propulsion Adm. Kirkland H. Donald inspected the facility and said it was "the best, the nicest they had, anywhere."

Camp's branch installs Combined Enterprise Regional Information Exchange System (CENTRIXS) local area networks for rapid communications between ship and shore facilities without a large supporting infrastructure, using low bandwidth. These networks allow computer-to-computer communication, chat and file sharing.

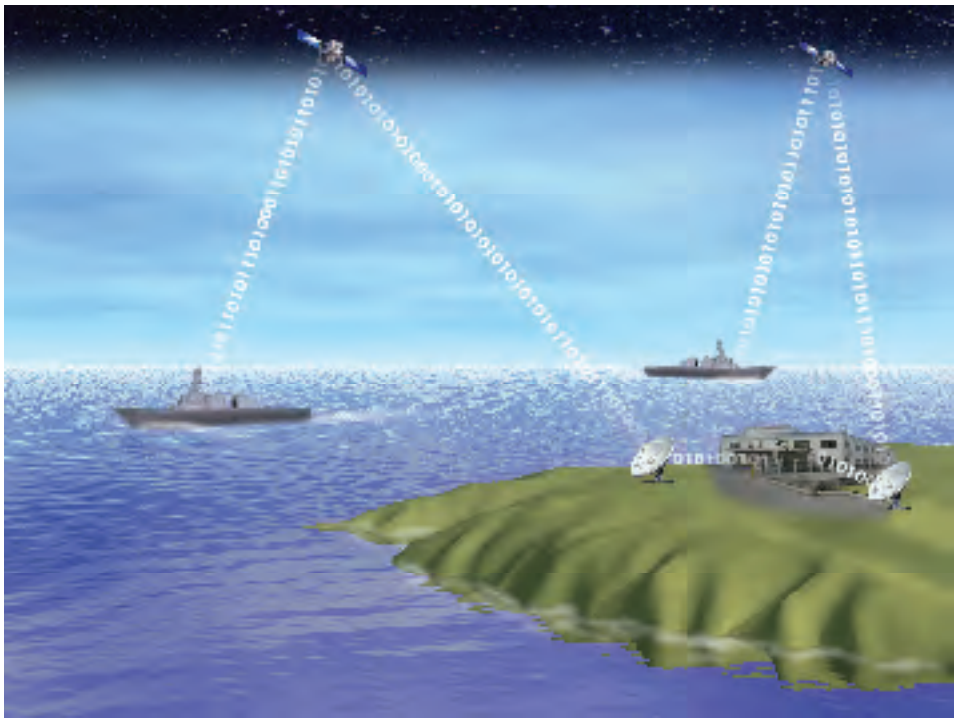


Figure 1.

Several years ago, Camp's branch transitioned 18,000 users from the Global Command and Control System-Korea to CENTRIXS-Korea with Voice over IP capabilities.

A key branch project involves C4I planning, engineering and relocation assistance for approximately 3,500 Marines on Okinawa from Marine Corps Air Station Futenma to Camp Schwab located in northeastern Okinawa. This includes construction of a runway, airfield and approximately 125 host nation facilities.

This effort requires close coordination with Marine Corps Bases Japan, Defense Policy Review Initiative (DPRI), as it affects Okinawa, and the Joint Guam Program Office. A draft master communications plan is nearly complete for the Futenma Replacement Facility. Actual installation of the C4I infrastructure will occur once the building construction is finished at Camp Schwab.

The completion of the Futenma Replacement Facility is the major trigger that will enable the transition of 8,000 Marines from the III MEF located in Okinawa to Guam under the DPRI. Additionally, in support of PEO EIS and Naval Network Warfare Command, branch personnel are migrating more than 200 buildings to the OCONUS Navy Enterprise Network (ONE-Net) and providing the required infrastructure.

ONE-Net provides centralized control authority for Navy and Marine Corps shore installation users from Europe to the Far East. This effort supports the theater network operations and security center in Yokosuka and nine local network service centers across the region.

The numbers are impressive; since project commencement, almost 13,000 seats (96 percent of those required) have been migrated.

SSC Pacific Technical Director Carmela Keeney emphasized the importance of SSC Pacific's on-site presence and ability to meet immediate fleet needs. "We know the Far East fleet and shore commands consistently rely on your support — because of your outstanding efforts and collocation with the fleet — this is often where the real work gets done."

The division's mission is a constant reminder of the critical importance of the team's work — ensuring that our partners in the Pacific Far East maintain C4ISR dominance over all possible threats. CHIPS

Ann Dakis is a staff writer for the SSC Pacific public affairs office.

KM and the Navy Enterprise Portal

Consolidating portals across the Navy under one enterprise roof

By Darlene Shaw

Navy Enterprise Portal KM Working Group
Department of the Navy Chief Information Officer
Office of the Chief of Naval Operations
Center for Security Forces
Commander, Naval Air Forces
U.S. Pacific Fleet
U.S. Second Fleet
U.S. Third Fleet
Commander, Submarine Force U.S. Pacific Fleet
Naval Air Systems Command
U.S. Navy Reserve
Naval Sea Systems Command
Navy Supply Information Systems Activity
Naval Facilities Engineering Command
Naval Computer and Telecommunications Area Master Station
Naval Education and Training Professional Development and Technology Center
Naval Network Warfare Command
Naval Education and Training Security Assistance Field Activity International Training Center
U.S. Pacific Command
Program Executive Office for Command, Control, Communications, Computers and Intelligence
PEO for Enterprise Information Systems
Space and Naval Warfare Systems Command

The Navy Enterprise Portal (NEP) initiative presents a rare opportunity for knowledge managers across the Navy to work together to seek out and integrate user requirements during the design and build out of the enterprise portal.

The knowledge managers' contribution will result in a cohesive, user-friendly interface that integrates the knowledge sharing power of a portal with the necessary knowledge technologies to meet Navy collaboration and content management needs well into the future.

As anticipated, Navy knowledge managers are excited to participate in this effort, and weekly teleconferences boast regular attendance of 20 or more participants.

For those unfamiliar with the Navy Enterprise Portal, it will serve the entire Navy, similar to the services the popular Army Knowledge Online portal provides for Army personnel. This effort is an outcome of the Chief of Naval Operations-mandated portal consolidation and integration process, as well as recognition that the existing ad hoc approach to Navy portals would jeopardize, if not preclude, achieving the goals of the Defense Department netcentric strategy.

Director, Navy Networks, Deputy Chief of Naval Operations, Communication Networks (N6) Rear Adm. David Simpson, in July 2009, cited these major capability gaps as to why the Navy needs an enterprise portal strategy:

- ❑ Existing portals are organization-focused and not designed for information sharing among Navy mission partners;
- ❑ Hosted information in these separate systems is not visible or accessible outside each portal;
- ❑ Navy portals are inefficient with suboptimal capabilities;
- ❑ Multiple designs and acquisition of services across commands;
- ❑ Very little netcentric access to information, no inter-portal interoperability;
- ❑ Inconsistent system performance, reliability, functionality and security; and
- ❑ Cost management inefficiency: no leveraging of licenses, consolidation of servers and administration or reuse of solutions.

The NEP design addresses these gaps and will include a public face, an internal face for common access card (CAC) users, and also private sites for individual organizations and teams. The tool suite includes SharePoint, Oracle WebCenter Interaction and Autonomy functionalities, to name just a few of the capabilities to be incorporated into the portal. When all is said and done, the portal will have CAC single sign-on between all components creating maximum efficiency for users. Figure 1 illustrates the NEP configuration.

Needless to say, Navy knowledge managers have their work cut out for them. However, the depth and breadth of the Navy Enterprise Portal KM Working Group's knowledge and experience will serve them well in meeting this challenge.

To ensure that the diverse needs of all users across the Navy are met, participants hail from a cross section of Navy communities (shown above). While the majority of participants are knowledge managers, there are some members from other disciplines and all are welcome.

With Space and Naval Warfare Systems Command's KM team facilitating, Navy knowledge managers are engaged in many areas of NEP planning. These areas include content, information architecture, governance, and the "look and feel" of the portal in respect to the graphical user interface and aspects of its design, including elements such as colors, shapes, layout and typefaces (the "look"), as well as the behavior of dynamic elements such as buttons, boxes and menus (the "feel").

Look and feel in user interfaces serve two general purposes. An appealing design is important, first to ensure that the best and most useful applications are hosted on the NEP, and second, to enhance ease of use and provide a productive user experience.

Portal elements under review are:

Content
- Media guidelines, i.e., file types and maximum size allowed, data tagging
- Best practice and case studies
- Training
- Content migration strategies
- Search enhancement strategy
- Quality control methodology

Information Architecture
- Meta tag schemes
- Naming conventions
- Full exploitation of software functionality, including Web 2.0 capabilities
- Integration strategies for electronic Navy records – Total Records and Information Management (TRIM)

U.S. Navy photos – www.navy.mil

• Defense Enterprise Computing Center (DECC)-based Web Servers or public SharePoint Portal.
• Intent is to manage content once and ensure available where needed and authorized to the extent possible.
– Content used on private/restricted portals will be identified for one-way push/replication to the public SharePoint portal.
– Data is tagged and managed on the private/restricted portal.
– No content management is performed on the public portal.

Initial operational capability (IOC) is estimated for Oct. 15 to support Naval Air Systems Command migration activities and Dec. 1 to support a subset of Navy users.

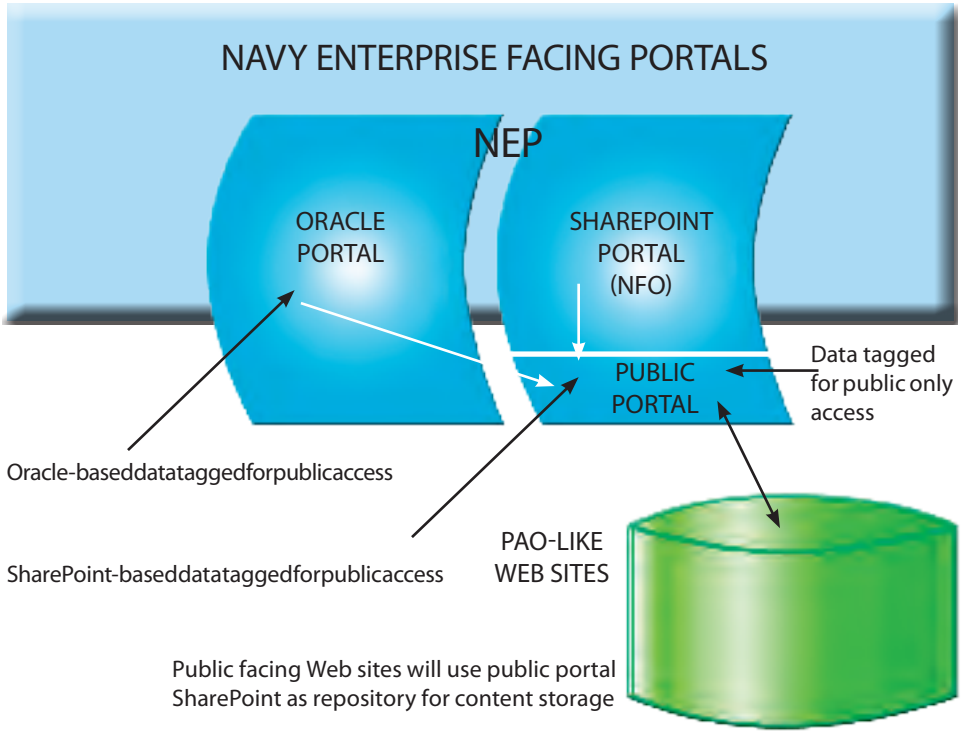


Figure 1.

Look and Feel
- Style Guide
- Branding guidelines
- User interface standards
- Standardized templates for various types of pages
- User interface testing and results
- Section 508 compliance

Governance
- Governance for ongoing maintenance and configuration control
- Process for enhancement approvals
- Business rules for joint content management

Metrics
- Portal role identification and standardization of names and functions

The art and science of knowledge management enable appropriate guidance for the design elements to be integrated into the requirements of the project, and as you can see, they are very important to the success of the Navy Enterprise Portal.

Navy knowledge managers plan to divide and conquer the tasks. To do this, we are currently identifying subgroups to work on particular tasks in parallel. This strategy allows us to leverage the variety of the knowledge managers' skill sets and interests to develop quality deliverables on time.

Initial operational capability (IOC) is estimated for Oct. 15 to support Naval Air Systems Command (NAVAIR) migration activities and Dec. 1 to support a subset of Navy users.

The work is voluminous, but the satisfaction for knowledge managers for a job well-done is priceless. We invite any and all to join our efforts to make the Navy Enterprise Portal an amazing success for the Navy!

For future project notifications, please send your e-mail address to darlene.shaw@navy.mil.

For more information about Navy enterprise planning, go to the Department of the Navy Chief Information Officer Web site at www.doncio.navy.mil. CHIPS

Darlene Shaw is the chief knowledge officer for Space and Naval Warfare Systems Command.

JPEO JTRS teams with UCSD to develop Project 25 Waveform porting guidelines

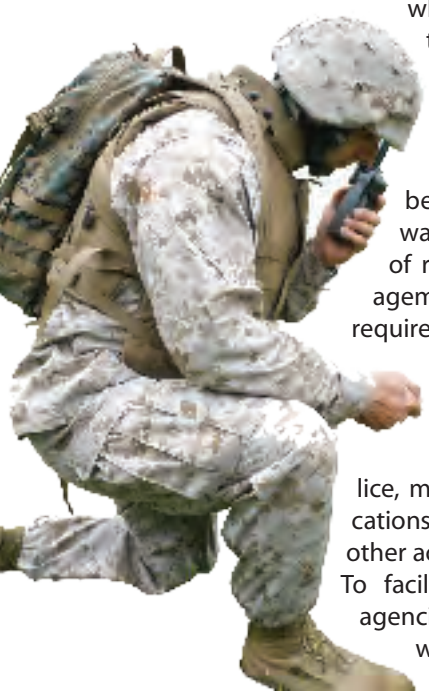
Project marks a crucial step for JTRS radio compatibility with state/local first responders

The Joint Program Executive Office, Joint Tactical Radio System (JPEO JTRS) is working on the Project 25 (P25) waveform porting project in conjunction with the University of California, San Diego (UCSD) California Institute for Telecommunications and Information Technology (Calit2) facility. The effort is phase one of a three-phased approach by the JPEO JTRS designed to allow interoperable capability between military radios and emergency and first responder agencies.

During phase one, the UCSD engineers will use the Software Communications Architecture (SCA) and JTRS Application Program Interfaces to initially implement P25 in a software simulation. Next, they will port the waveform to a COTS development platform, which will then lead to a demonstration of radio frequency end-to-end functionality. Finally, the team will demonstrate interoperability with commercial P25 radios, simulating military interoperability with commercial off-the-shelf first responder radios running the P25 waveform.

Formerly called APCO-25, P25 is now a joint effort between the Association of Public-Safety Communications Officials - International, the Telecommunications Industry Association (TIA), the National Association of State Telecommunications Directors (NASTD), and various agencies of the federal government. P25 encompasses the development of standards for digital telecommunications technology, including an objective to determine consensus standards for digital radio equipment embracing elements of interoperability, spectrum efficiency and cost.

"This is a crucial step toward making JTRS radios interoperable with first responders," said Dr. Richard North, the technical director for JPEO JTRS. "Phase two will be to port the UCSD-developed P25 waveform onto a JTRS radio with additional modes which may include encryption, trunking and analog FM. Both phase one and two are risk mitigation efforts before moving to the third and final phase."



Phase three of the project will be the incorporation of the P25 waveform into the JTRS program of record, which provides the management and funding mechanism required to deliver the radio to military end users.

Interoperability for a first responder participant requires public safety agencies (fire, police, medical) to have direct communications when they operate with one another across disciplines and jurisdictions. To facilitate this communication goal, agencies are looking at non-military waveform standards such as P25.

Using a standardized suite of waveform standards allows radio sets, manufactured by different vendors, to communicate. Ultimately, porting the P25 waveform to JTRS radios will allow military organizations to interoperate with state and local agencies in times of an emergency such as a disaster relief scenario.

"The JTRS radios will host the ported P25 waveform as well as JTRS networking and current force military waveforms such as SINCGARS (Single Channel Ground and Airborne Radio System), EPLRS (Enhanced Position Location Reporting System), HF, Link 16, or UHF SATCOM (Ultra High Frequency Satellite Communications)," Dr. North said. "With all these waveforms on the same radio we can provide direct communications to P25-equipped first responders, as well as routing and retransmitting messages from the P25 net to current force radios. This provides a tremendous capability for unit commanders equipped with JTRS radios." CHIPS

About Calit2 UCSD

The University of California San Diego division of the California Institute for Telecommunications and Information Technology (Calit2), together with Calit2's division at University of California, Irvine, houses more than 1,000 researchers across the two campuses, organized around more than 50 projects. With a focus on discovery and innovation at the intersection of science, engineering and the arts, Calit2 constitutes one of the largest multidisciplinary research centers in the nation.

Research is conducted on the future of telecommunications and information technology and using these advancing technologies to transform a range of applications. For more information, please visit www.calit2.net.

About Calit2/JTRS project

The Calit2/JTRS Software Defined Radio (SDR) Project is a collaborative research effort supported by JPEO JTRS involving Software Communications Architecture SDR platforms for development and porting of SDR waveforms, creating a high performance amplifier (HPA) test-bed, and hosting the JTRS Open Information Repository (IR). For more information, please visit http://jtrs.calit2.net.

Enterprise Domain Demonstrates Wideband Networking Waveform

The Wideband Networking Waveform (WNW), a critical capability of the Joint Tactical Radio System, successfully demonstrated its validated design and tactical utility June 3 and 4 during a multi-node demonstration with senior service and Department of Defense officials at the Space and Naval Warfare Systems Center Atlantic, Charleston, S.C. Thirty ground mobile radios were used in the largest demonstration of the capability to date.

"The Wideband Networking Waveform overcomes many mobile networking challenges," said Navy Capt. Jeffery Hoyle, program manager for the JTRS Network Enterprise Domain. "We've now demonstrated [that] this capability successfully scales to tactically useful numbers of nodes in an operationally relevant environment and is on track to meet joint warfighter require-

ments to provide a flexible and pervasive networking capability to address the challenges of modern battlefields."

The event demonstrated how the WNW, operating on JTRS ground mobile radios, can effectively network 30 mobile and static nodes, sharing data and video across multiple sub-networks in a challenging, heavily forested suburban environment with significant multi-path propagation effects.

"During this field demonstration testing, WNW performed as expected, and we were able to validate laboratory performance improvements from recent waveform algorithm enhancements in the field," Hoyle said. "The ability to integrate waveform enhancements rapidly while testing in the field (three times in as many weeks) thoroughly demonstrated a significant advantage that JTRS provides — the ability to upgrade warfighter communications and networking capability while deployed through software only updates in fielded radios. This is an important accomplishment, and this capability that has now been successfully demonstrated in a field environment can be leveraged continuously throughout the WNW product life cycle."

The WNW is a networking waveform that enables connections between vehicles, aircraft and ships using mobile networking technologies. WNW offers the ability to transit more information with greater security and provide new capabilities to seamlessly route and retransmit information. Performance results measured during this demonstration indicate a significant new networking capability that will continue to improve as the data collected are thoroughly analyzed to enable additional waveform software upgrades, as well as through processor and power amplifier improvements inherent with the improved Ground Mobile Radio Engineering Development Model hardware being delivered now, and the Airborne/Maritime/Fixed Station hardware in the future.

The WNW is a high data rate networking waveform application that provides a tactical Internet backbone to connect tactical forces across the battlespace. It features the following signals-in-space under the initial increment: Orthogonal Frequency Division Multiplexing and anti-jam. WNW provides high throughput, dynamically adaptable connectivity for the exchange of IP-based voice, data and video traffic, and will support network nodes on mobile, airborne and maritime platforms.

WNW includes networking services, security, High Assurance IP Encryptor capabilities, red-black switching and internal routing of other WNW signals. Increment 1 (first quarter) is scheduled later this year on a Ground Mobile Radio Engineering Development Model. CHIPS

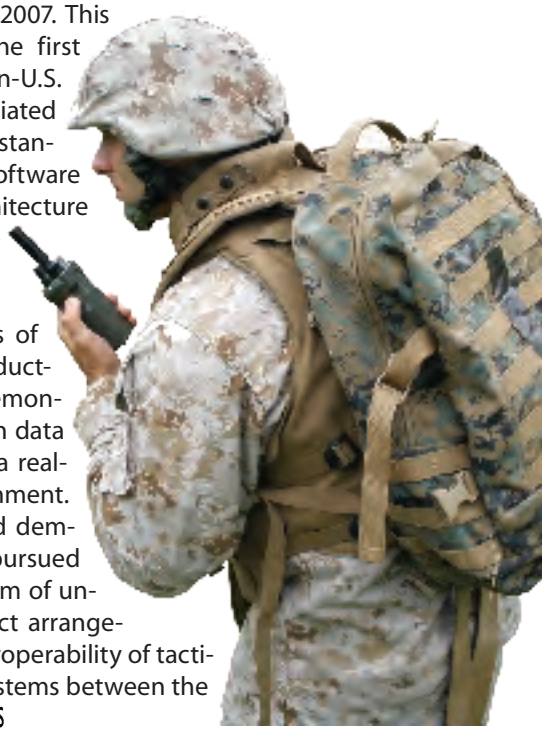
JPEO JTRS and PEO Integration team with UK Defense Agencies

The JPEO JTRS International Programs Directorate and the PEO Integration, formerly known as the Future Combat Systems Joint Interagency Multi-National Interoperability (JIMI) team, completed a demonstration of communications interoperability that will greatly enhance and benefit coalition warfighting capabilities. JPEO JTRS and PEO Integration partnered with the U.K. Defense Science and Technology Laboratory and Defense Equipment and Support agency to participate in the Multinational Experiment 3.0 at Fort Monmouth, N.J., April 29. MNE 3.0 successfully demonstrated interoperability between the U.S. ITT-developed Soldier Radio and the U.K. Advanced Digital Radio+ using the JTRS Bowman Waveform (JBW).

MNE 3.0 included many first-time achievements that offer tremendous opportunity for improved battlefield interoperability with coalition partners — porting and demonstrating operation of JBW in a handheld software defined radio; successful interoperability through exchange of secure voice and data between the two nations' communications systems; and use of a foreign nations' cryptographic keying material in a U.S. secure network. The demonstration was performed in a closed (non-radiating) lab environment where the team successfully exchanged data using voice messaging, and demonstrated the ability to pass crucial situational awareness and fire control data on a shared U.S. and U.K. communications network.

Working closely with the National Security Agency and its U.K. counterpart, Communications Electronics Security Group, the United States imported and used non-U.S. mission data and keying material for the experiment. This unprecedented use of foreign crypto was critical to the successful interoperability between the two nations' radios and will support development of processes for future exchange of tactical keying material for coalition usage.

The JBW project between the United States and United Kingdom began in September 2003 under a Cooperative Research Development Memorandum and two separate Tactical Communications Project Arrangements (PA). The initial PA is a cooperative agreement established to develop the JBW in an effort to promote increased interoperability capabilities between the two countries. Under the second PA, the JBW was ported to a JTRS representative radio for the purposes of demonstration in a test, training or operational environment. The waveform was tested for interoperability with the ADR+ using a JTRS developmental test bed in June 2007. It was delivered to the JTRS Information Repository in October 2007. This activity represented the first development of a non-U.S. waveform, with associated crypto, in a software instantiation, targeted to a software communications architecture compliant software defined radio.



Future plans include expanding the success of this experiment by conducting live (radiating) demonstrations where mission data will be transmitted in a real-time battlefield environment.

These objectives and demonstrations are being pursued under the memorandum of understanding and project arrangements concerning interoperability of tactical communications systems between the two governments. CHIPS

Has the Use of E-Mail Peaked?

By Brian Burns

Historically, each generation expands the use of the communication inventions from the previous generation. Communication has evolved from cave drawings and carvings, to smoke signals and music (such as drumbeats, chants and yodeling); to written inscriptions; to letters distributed by foot, horseback, ships and railroad. Morse code revolutionized communication through the telegraph and line-of-sight light flashes.

The traditionalist generation, those born prior to the early 1950s, experienced the transition from paper correspondence to radios, telephones and television. Baby boomers ushered in the use of computer networks, fax machines, e-mail, listservs, bulletin boards, chat and the Internet. Millennials are extending the use of the Internet to provide global communication in the form of text, instant and simple messaging, wikis, blogs and other social media.

Until the late 1980s, office workers were accustomed to using official letters and memoranda typed on typewriters and stored in file cabinets; using handwritten notes often thumbtacked to a board or paper-clipped to papers; using the phone for informal communication; and congregating by the water cooler for office gossip. Mimeograph machines and photocopiers duplicated documents. Transparencies and light projectors were used to present information. A blackberry was a fruit, a tweet was a sound a bird made, a tweeter was a high-pitched speaker for a hi-fi stereo and a palm device was a pen or pencil.

Beginning in the 1980s, personal computers began to replace typewriters, "stickies" replaced thumbtacks and paper clips, and photocopiers and printers replaced mimeograph machines. Shared file systems began to replace file cabinets, and many secretaries and office assistants were displaced by office automation assistants and office automation tools. Voice mail and electronic mail were introduced and blurred the line between official and unofficial correspondence and documents. E-mail became the easy, ad hoc way to communicate, store and distribute information.

The positive aspects of automation are that employees could send, receive and respond to information requests and direction at any time without having to be physically located with the sender. Telecommuting and alternative work schedules became feasible. As wireless solutions improved, pagers emerged, which were replaced by cell phones, which converged with e-mail, calendar functions, the Internet and other services available on personal digital assistants or palmtops.

On the negative side, the blur between official and unofficial correspondence, a lack of enterprise document management, and the ease of attaching big files and distributing them to many e-mail addresses, made records management and electronic discovery far more difficult. E-mail trails became long and a business's ability to control how many copies were sent and received, where the copies ended up, and how much storage was required was limited.

With 2010 on the horizon, Web 2.0 tools and cloud computing will become embedded in the business environment. Does this mean that e-mail is dead? No, but it does mean that the use of e-mail has peaked and that the use of Web 2.0 tools will gradually become predominant. This is no different than the rise and fall of other evolutionary tools such as Morse code, the telephone, typewriter, newspaper and live television broadcasts. These technologies are still used today, but not as the primary tool or to the degree that they were used in the past.

E-mail cannot be considered by itself. It is one tool in the evolving e-messaging environment which includes standard mailbox tools such as e-mail, calendars, contact lists, task lists and notes. It also includes voice mail, Voice over Internet Protocol (VoIP), instant/text/simple messaging, fax integration and file/document sharing. Added to e-messaging are new Web 2.0 tools such as wikis, blogs, Really Simple Syndication feeds and social media sites.

Why has e-mail peaked? Approximately 80 million Millennials now exceed the approximate 75 million baby boomers. For Millennials, it is easier to post information on a social media site for their friends and colleagues to see, or send a text message, than it is to open up an e-mail, select a list of users, type and attach information, send the e-mail and wait for a reply.

Baby boomers are accustomed to using e-mail for official and unofficial correspondence. It was easier for them to use e-mail than to use a typewriter or dictate a letter and then proofread it.

Social media sites are organized to socialize information. For example, wikis allow authorized users to edit the information in one location. When e-mail is used to edit documents, version control and aggregation of multiple comments are time consuming and cumbersome. E-mail stores and forwards information to specific users who can reply or forward the same or updated information to others.

Wikis and blogs open up a dialogue in a single location where authorized users can contribute to the conversation and content and compare each edited version and comments. This method results in a more democratic approach to editing information, allowing more subject matter experts to participate, more informed opinions and facts to be presented and a larger consensus to be reached.

Consequently, the playing field is leveled. Autocratic media is replaced with democratic dialogue, making information more transparent to the community of interest. CHIPS

Brian Burns is on a detail assignment from the Department of Education as the DON Deputy CIO for Emerging Technologies.

A Pragmatic Approach to Implementing Knowledge Management at the Operational Level of War

By Nancy Jenkins

Historically, U.S. military forces conducted operations in a joint operational area that was divided between the services in terms of time, latitude and longitude. Within the services, operational forces typically trained and deployed together.

Maritime battle groups were composed of the same number and types of ships. Any one ship of a particular class was fitted out with basically the same operational capabilities as all ships of that class.

The enemy we trained to oppose in the Cold War was the same enemy we trained to oppose for decades. The most likely geographic areas in which we would see combat were familiar to our commanders. But today, the services fight as integrated joint forces which tend to be made up of multiple ad hoc service units that have neither trained nor worked together to any great extent before deployment.

This integrated force is involved in opposing adversaries we are only now beginning to understand. Our new adversaries engage in combat within geographical areas unfamiliar to commanders who are executing command and control over dispersed units while trying to make informed, effective decisions within extremely compressed time cycles.

In this regard, using knowledge management methodologies can be invaluable to fighting in the current threat environment. Traditional KM implementation approaches seek to transform hierarchical, stovepiped organizations into "learning" organizations. While that goal may be desirable, the process of achieving that goal requires consistent leadership and unwavering commitment over an extended period of time.

At the operational level of war (OLW), senior leadership turns over in 12 to 18-month cycles on average. The operational environment is extremely fast-paced and results-oriented. Consequently, the requisite time period for the implementation of organizational approaches to KM simply does not exist. If KM is to be successfully implemented at the OLW, it must be focused, achievable (in terms of weeks), and have a benefit that is directly linked to enhanced operational performance.

Although command of a learning organization may be an ideal situation, most operational commanders would settle for a common understanding of the commander's intent; shared situational awareness; and well-informed decisions made in a timely fashion.

The following discussion seeks to articulate the operational value gained from implementation of KM methodologies in direct support of command, control and decision making. Although this discussion focuses on the OLW, carrier and expeditionary strike groups can also benefit from these practices.

What does KM look like?

In the most basic of terms, KM is simply an organization's approach to managing mission critical knowledge and information. The enhanced capabilities that effective KM can lead to are impressive.

Using the scenario of a large number of augmentees reporting to a numbered fleet or joint task force to support an exercise or crisis operation, an ideal command

Knowledge management is NOT new. The only thing that has changed is the impetus to do it better.

HELMAND PROVINCE, Afghanistan (Sept. 9, 2009) U.S. Navy Hospital Corpsman 3rd Class Ryan Tucker, assigned to 2nd Battalion, 8th Marine Regiment Police Mentoring Team, walks through a field during a patrol to an abandoned bazaar with Afghan national border police in Little Jugroom, Garmsir District. Afghan Border Police and the Police Mentoring Teams are looking for possible enemy activity after reports of the Taliban using the bazaar as a meeting place. U.S. Marine Corps photo by Sgt. Pete Thibodeau.

environment would be one in which all reporting personnel had a direct, expeditious means of understanding:

- the operational environment;
- the commander's guidance, mission objectives and decision cycle;
- their role in the operation and the organization as a whole;
- who their chief contacts are apt to be;
- what meetings they need to attend and what they are expected to provide at those meetings;
- how they discern the current status of the operations, plans and progress;
- what information sources are available;
- how to get questions answered; and
- how to find answers to questions asked of them.

Often, due to the high operations tempo, newly reporting personnel are hurriedly brought on board with minimal time for orientation. The remainder of that individual's education is provided via on-the-job training. But implementation of KM practices could greatly mitigate the burden of training new personnel and dramatically reduce the time they need to "ramp-up" in a new job.

All of the information required to train new personnel already exists somewhere in the command. The trick is to organize it in a digestible manner. Once that is done, the process can be socialized to ensure the process is sustained and improved through the turnover of personnel.

Strike groups, on average, operate as a team for one deployment cycle due to crew and staff turnover; the challenge is always attaining and maintaining sufficient cohesion to enable rapid integration of units in joining and re-joining the group. Training and readiness are paramount and KM can facilitate a smoother cycle time in this regard.

Enhanced Command and Control

At the OLW, KM practices can be applied to enhanced command and control and support improved decision making. Improvements in the way in which participants establish and maintain operational understanding can be done through deliberate management of the knowledge and information exchanges involved in assessing situations, developing a plan, executing operations, and maintaining an accurate understanding of what is happening.

The example of an operations order (OPORD) may illustrate the point. OPORDs are made up of a base order and related annexes (many of which have multiple appendices). The base order describes the situation, mission, operational execution, concept of operations, coordinating instructions, and high-level information about administration, logistics, command and signal.

The real details of the OPORD are contained in a number of annexes that can run the lettering system of Annex A to AA and beyond. Individual annexes are usually drafted by various departments within a command. For example, Annex B (Intelligence) is usually drafted by N2, Annex C (Operations) by N3/5, Annex D (Logistics) by N4.

In extensive operations, the sheer volume of information provided in the base order and all related annexes make reading the entire document a daunting task. Normally, participants will read the base order and only those annexes that apply to their specific role. To expedite understanding, culling the key points and posting them to either an internal shared drive or a Web site will promote further review and enhance understanding.

Briefs that cover the operations, task organization and major plans should also be posted to a central area along with the listing of the main points of contact for staff functions.

A reports matrix that delineates what reports are required and by whom and on what basis is a great tool for informing others about what information is required, and when, how and where it can be found.

Often, the Reports Annex (Annex R) is written by the N3 or N5 staff and does not contain all the reporting requirements delineated in each annex. Creating easy access to information and updates promotes users' ability (and willingness) to review the information frequently to maintain awareness of what is planned, what is occurring, and what progress toward mission completion has been made.

In this context, the answer to the question: "What does KM look like?" would be a central, accessible area that made the following information resources available to all concerned:

- Significant Event Logs
- Commander's Critical Information Requirements (CCIRs)
- Well-understood/managed requests for information (RFIs)
- Consolidated operational information
- Commander's Guidance
- Orders
- Situation Reports
- Briefs
- Rules of Engagement (ROE)
- Battle Rhythm
- Report Matrix
- Planning Matrix
- Common Operating Picture (COP) Management
- List of chat rooms and directions for joining
- Functional/Staff Points of Contact

None of the suggestions and examples contained in this article are novel. Commands are already employing KM methodologies to facilitate understanding and awareness. But, deliberate management does not just happen automatically; it requires a focused effort and at least one "shepherd" to foster the process.

The Not Invented Here Syndrome

There are a number of reasons why KM is not practiced more widely and consistently. Two of the primary reasons are time and credibility.

Just the volume of information pouring into and out of organizations can be overwhelming. Being able to sift through all the chaff to find those kernels of needed knowledge and information is challenging. Message traffic, e-mails, orders, briefs and the seemingly endless litany of additional information referenced in these items can create a "bridge too far" for even experienced staff members.

Most staff personnel are so weighed down with tasking and deadlines that they simply have no time to stay informed about anything that does not directly relate to what they are doing. In other words, people are too busy doing their jobs to figure out how to do their jobs better! It is a classic "Catch-22" example.

Credibility is an earned attribute. If something is credible, it has the power to elicit belief and value. One of the most frequent causes for not leveraging the insights gained by others is referred to as the "not invented here syndrome. "

The not invented here syndrome is manifested as an unwillingness to adopt

an idea, approach, tactic or product because it originated from an event, individual or group outside the potential adopting organization.

It is interesting to see the extent to which people will try to justify their situation as "too unique" rather than recognizing similarities and the merit of hard-won experience and insight.

How KM Fits in an Organization

Up to this point, very little has been mentioned about information technology. Effective management of mission critical knowledge and information has much more to do with people and processes than technology.

Enabling technology can advance KM processes more conveniently. However, the vast majority of KM practices can be implemented with the IT infrastructure currently available at most commands. And yet, the tendency is to make the knowledge manager someone in the IT department and to assign the KM functionality to the webmaster. KMs treated as technical support will tend to focus on technical issues rather than looking at the bigger picture of command knowledge and information flow challenges.

Who should the knowledge manager be? If an N3 or N5 were asked, "Who is the one person you cannot afford to lose?"; the person they name would probably make the best KM for the command. But the odds of getting that person to be the knowledge manager are extremely slim.

Whoever is selected as the KM, he or she must understand the organization's mission and processes. Operational experience will only increase the knowledge manager's value.

Designating the KM position as a collateral assignment may have its merits in a command that already practices KM methodologies. At the starting point, however, a collateral duty knowledge manager will never be empowered with enough time and resources to make a difference.

Ideally, the KM should report directly to the commander or chief of staff. It is important that knowledge managers have either sufficient rank or sufficient support high enough in the command to avoid having their efforts re-directed to tasks of a more department-specific nature. If, for management purposes, the individual remains within a department, it is preferred that the individual be empowered with direct lines of communication to both the commander and the chief of staff so he or she can be most effective.

Most commands have some form of information management. At the OLW, the term, Information Management Plan (IMP), or Knowledge and Information Management Plan (KIMP), is often used to document processes. Within naval commands, the term, OPTASK IM, may be used. These documents, however, tend to be written by communicators for communicators. If an organization is trying to manage its operational knowledge and information, something written by and for communicators is not apt to be reviewed in earnest by those assessing, planning and executing operations.

A suggested alternative to traditional modes of documentation is to create a separate annex to an OPORD, or a reference within an OPORD, or a command instruction that specifically cites command procedures for information exchange and sharing.

Before You Start

A quick way to undermine a KM effort is to allow individuals to NOT comply. Compliance to established KM methodologies should be required because it adds to the body of knowledge and experience an organization possesses.

An example of effective enforcement occurred during a JTF headquarters operational exercise. Inputs to the Commander's Daily Update were to be posted to a Web site using a prescribed template by a specified time. Inevitably, subordinate commanders wanted to create their own slides without conforming to the template and without heed to the submission deadline. Had the JTF commander allowed his subordinates to disregard the preferred process, it would have made coordination more difficult.

Instead, the commander ordered that input not received in the correct format by the established time would not be accepted and a place holder slide would be inserted in the brief that said "XYZ's input was not received by 0715 (or) XYZ's input was not submitted in the proper format."

As a consequence, noncompliance issues were corrected immediately. Enforcement must be something the commander is willing to do if the processes are to produce the desired results.

A quick way to undermine a KM effort is to allow individuals to NOT comply.

In an operational environment, the KM methodologies a command chooses to implement need to be carefully selected. A brainstorming session involving experienced members from all departments will produce a list of potential projects. Those projects should be prioritized based on the following criteria:

- alignment with the commander's priorities/focus areas;
- level of effort and time required to develop and implement;
- level of benefit gained; and
- scope of beneficial effect.

Most commanders would agree that mission completion is a high priority. Therefore, efforts should be weighed based on contribution to mission completion or enhancing mission performance. Initial KM efforts should be achievable within a few weeks to establish momentum. The best efforts to start with are those that will reap benefits as soon as they are implemented so that the value will be immediately obvious to a large portion of the staff. Lastly, avoid starting too many efforts simultaneously; staff members can only juggle so much change within a given timeframe.

The Bottom Line

One might say, "We've been doing this stuff!" True, the Navy has long practiced various KM methodologies such as wardroom discussions, chiefs' messes, surface warfare luncheons, message/read boards, planning boards for training and the plan of the day. These are all examples of getting the word out and promoting a common understanding of what needs to be done and the plan to do it. Knowledge management is NOT new. The only thing that has changed is the impetus to do it better. CHIPS

Nancy Jenkins is a retired U.S. Navy commander and the knowledge management officer at U.S. Second Fleet.

Center for Surface Combat Systems Shares Knowledge Through Communities of Practice

By Kimberly M. Lansdale

As the Navy increases in capabilities to support the joint force to meet the national security needs of the nation, one of the biggest challenges is to provide warfighting Sailors with more skill and experience as expeditiously as possible. The mission of the Center for Surface Combat Systems (CSCS) is to train and prepare officers and Sailors to maintain, operate and, if necessary, fight in a combat environment.

To achieve this mission, CSCS has been utilizing knowledge management (KM) methodologies to help deliver those warfighting skills to Sailors where they live and work, in their homeports, ships and schoolhouses.

Communities of practice (CoPs) are a key KM method to promote the sharing of information and knowledge. CSCS considers CoPs foundational to systems and warfare training effectiveness at almost every level.

"In order to educate and train both Sailors and officers, we must have a virtual environment where students, instructors and staff can connect," said CSCS Commanding Officer Capt. Stephen Hampton. "An environment where the fleet Sailors can reach out worldwide and be mentored in their specialties that will help Sailors grow both professionally and personally in less time."

The CSCS CoP is hosted on Navy Knowledge Online (NKO) and includes the individual rate/job communities that are taught by CSCS. Sailors use their specific community to ask subject matter experts questions, share information, learn from one another and immerse themselves in their technical rate's social framework. They benefit by sustaining relationships and sharing ways of doing things together. The rapid flow of information between Sailors allows innovative ideas to be quickly implemented.

A Sailor working aboard ship can ask an instructor a question regarding a technique or procedure that he or she is not familiar with. The instructor can then provide assistance to the Sailor, as well as others within the community, who may have the same question.

The CSCS CoP provides more than just easy access and flow of information. It's also a storehouse of training material that Sailors can use to prepare for required training, advancement exams or specific job qualifications which directly benefit Sailors and their workcenter.

The resources available range from open forums to additional study aids in the form of quizzes, games, videos and graphics. As Sailors connect with each other, they are able to share knowledge and learn from each other.

"Our CoP provides our students, as well as boatswain's mates (BM) fleetwide, with updated BM news and an open forum where anyone can ask rate-related questions," said Boatswain's Mate 1st Class (SW/AW) Adriane Christian, an instructor at Boatswain's Mate "A" School in Great Lakes, Ill. "We provide information vital to studying for exams and training videos that apply to our curriculum, as well as questions of the week, where I select random questions out of our training curriculum, and I post the correct answers the following week."

"I believe that the reason we are so successful in fostering the use of our CoP is because it lends itself to our community," said Fire Controlman "A" School Leading Chief Petty Officer, Fire Controlman Chief (SW) Miguel Guzman.

"One of the key ingredients of each CoP is the ability for the user to post questions and get an answer in a timely fashion. Users feel more at ease posting questions in a nonconfrontational arena."

Early in the development of the Navy's Littoral Combat Ship (LCS) program, Reinhard Williams, training simulation manager for the CSCS technical support department, recognized communities of practice as the perfect communication tool. He made sure that an LCS CoP was developed and implemented aboard the Navy's newest ships that would take them into the 21st century.

"Communities of practice were ideal to establish a repository to share information about LCS," Williams said. "People working on this new ship program were dispersed throughout the United States. The LCS CoP became an essential communication tool. CSCS's CoP helped define the training requirements for the crew of the new LCS."

CoPs aren't just for apprentices. Journeyman and master Sailors in each rate use them for refresher training, technical information and learning tools. They are able to access online courses and content to assist in developing junior Sailors.

The Littoral Combat Ship community of practice brought together subject matter experts, who were geographically dispersed throughout the United States, to a repository of critical information on Navy Knowledge Online. The CSCS CoP helped define the training requirements for the LCS crew.

The Communities of Practice touch each level of the CSCS Value Stream which provides continuous learning

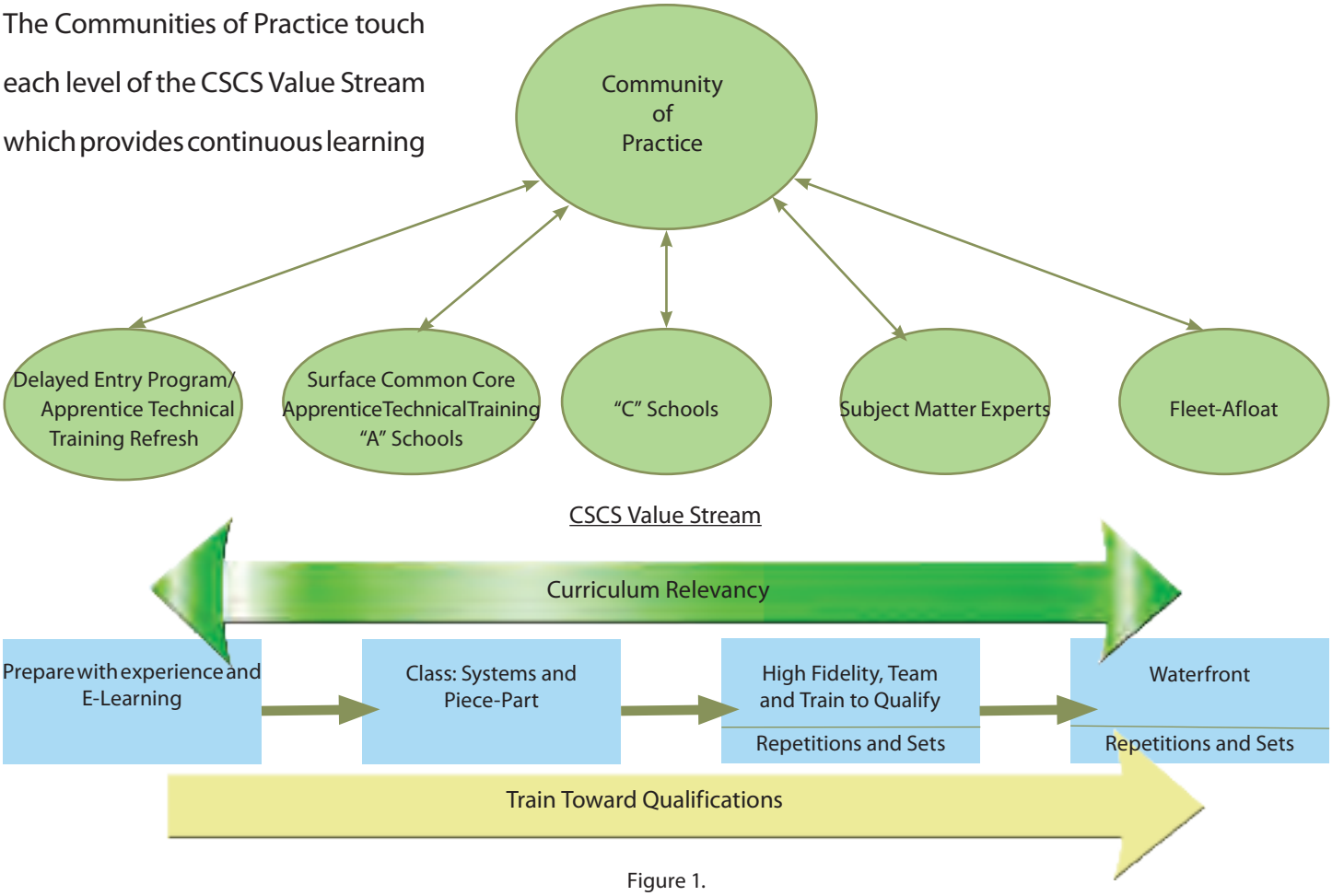


Figure 1.

"For a CoP to be successful, members need to see the benefits to providing and sharing information," Williams added. "Most importantly, we need to generate enthusiasm within the community. Enthusiasm creates an environment where Sailors can gain and share knowledge and see the rewards."

For tomorrow, the Center for Surface Combat Systems envisions a collaborative Web-based environment where instructors can post course requirements, curriculum and data from course activity logs and then map them to enabling objectives and training objectives.

By having a well-based record of content for each course, students, instructors and fleet operators would reap the benefits. Instructors could manage their course content with little or no time delay. Fleet users could view information and provide feedback from a basis of understanding the core content requirement source, which, in turn, would improve training.

"The future of communities of practice is to continue providing relevant information to the right person, at the right time," said CSCS acting chief information officer Robert Stewart. "The bottom line is it should add value to your organization."

Figure 1 above shows how CoPs contribute to the CSCS Value Stream to advance continuous learning.

Today, there are CoPs for most of the courses or operations taught by CSCS. Apprentice-level CoPs available on NKO include: Electronics Technician (ET), Fire Controlman (FC), Gunner's Mate (GM), Interior Communications Electrician (IC), Mineman (MN), Operations Specialist/ Quartermaster (OS/QM), Seaman/Apprenticeship Training Division (SN/ATD), Boatswain's Mate (BM) and Sonar Technician-Surface (STG).

To view the Center for Surface Combat Systems CoP visit https://wwwa.nko.navy.mil/portal/home/. For more information about CSCS visit https://www.netc.navy.mil/centers/cscs/. CHIPS

Kimberly Lansdale is a training support specialist for the Center for Surface Combat Systems, Dahlgren, Va.

To view the Center for Surface CombatSystemsCoP,visithttps://wwwa.nko.navy.mil/portal/home/.

Gaeta, Italy (Apr. 28, 2004) – U.S. Sixth Fleet Command Master Chief James P. Russell helps a junior Sailor understand the Navy Knowledge Online Web site aboard USS La Salle (AGF 3). CMC Russell knows that the strength of tomorrow's Navy lies in the hands of today's junior Sailors. U.S. Navy photo by Photographer's Mate 1st Class Paul Phelps.

Knowledge Management in Navy Strike Groups–So What?

TACTRAGRUPAC trains, mentors and assesses fleet efforts

By Tim Snyder

As knowledge management initiatives become more prevalent in the fleet, every carrier strike group (CSG) and amphibious ready group (ARG) commander should ask "How will knowledge management help me and my organization?" Tactical Training Group, Pacific (TTGP) has been working to help CSG and ARG knowledge management officers (KMOs) and primary staff officers answer this question since 2004.

TTGP's success in spreading KM training and initiatives throughout the Pacific Fleet has resulted in measurable improvement in strike group operations. To implement and inculcate KM into the CSG and ARG ethos, TTGP executes a three-phase approach: training, mentoring and assessment.

Training

With initial direction from the Naval Network Warfare Command (NNWC) in 2004, TTGP began supporting Navy strike group KM efforts through the development and execution of an Afloat Knowledge Managers Course (AKMC). This four-day course trains Information Professional (IP) Officers that are scheduled for assignment to carrier and expeditionary strike groups as the staff KMO.

The course is given twice per year with one scheduled on each coast. To date, more than 230 individuals have attended the course, providing an ever expanding group of individuals who are schooled in KM techniques and are able to articulate the "so what" of KM to Navy organizations. The course includes a day of information management (IM) training that provides an overview and best practices for use of common afloat IM and collaborative systems, such as the Collaboration at Sea tool set, Combined Enterprise Regional Information Exchange System (CENTRIXS), chat tools and Battle Force Email, and three days of KM training.

The AKMC includes guest speakers from industry, government and military organizations providing a balanced view of KM and a diversity of perspectives and ideas for implementation of KM techniques.

The course has also been given, in a modified format, to U.S. 7th Fleet, the Royal Australian Navy and at the Naval War College.

For CSGs and ARGs in the Pacific Fleet at the beginning of their Fleet Response Training Plan (FRTP), TTGP provides a one-day course called the Network Centric Warfare Commanders Course. The NCWCC, which is comprised of classroom instruction and student participation, provides an understanding of NCW concepts, origins, principles and architectures.

Training in the construction of a netcentric culture, as well as improving information and knowledge sharing, management and flow, is discussed in detail.

The NCWCC provides CSG and ARG leadership with recommendations on how to effectively share knowledge throughout their organizations by leveraging their people, and using well thought-out processes and available technology tools.

The NCWCC covers shipboard and aircraft command, control, communications, computers and intelligence (C4I) architecture and systems; collaborative tools; coalition networks; IM and KM techniques and best practices; and reviews processes available to effectively use specific CSG or ARG netcentric tools.

The NCWCC focuses on information flow into, out of and within the CSG and ARG command and control (C2) architecture and concludes with a practical information mapping exercise to highlight and understand the information needs and battle rhythm of warfare commanders and commanding officers.

The primary attendees for this day of training include CSG and ARG commanders, their warfare commanders, ships' commanding officers and key planning officers.

Mentoring

As a part of the FRTP, TTGP knowledge management mentors are involved in each CSG or ARG supported event, providing mentoring to staff personnel, watchstanders, senior planners and commanders within the group. This phase includes two one-week schoolhouse training events (with war games), as well as three one-week shipboard fleet synthetic training (FST) events.

Tactical Training Group, Pacific mentors are placed within the major C2 hubs of the CSG and ARG and provide mentor-

ATLANTIC OCEAN (Sept. 21, 2009) The aircraft carrier USS Harry S. Truman (CVN 75) and ships from participating nations take part in a NATO mine countermeasures exercise upon the completion of Joint Task Force Exercise (JTFX). JTFX is a scenario-driven tactical exercise supporting major combat operations for the Harry S. Truman Strike Group. The exercise provides training for the strike group to proceed into a Fleet Synthetic Training - Joint (FST-J) exercise for final deployment certification. U.S. Navy photo by Mass Communication Specialist 3rd Class David Danals.

ing and advice in the execution of internal and external IM and KM processes.

Assessing

Tactical Training Group, Pacific, in collaboration with Commander, Strike Force Training Atlantic (CSFTL), using the guidance contained in the Universal Joint Task List (UJTL) Manual (CJCS 3500.04C), developed knowledge management and information management measures — the Navy Mission Essential Task Lists (NMETLs) that are used to assess the effectiveness of KM efforts within CSGs and ARGs.

Beginning in fall 2006, TTGP began using draft versions of these measures to evaluate Pacific Fleet CSGs and ARGs, and upon approval of these measures in spring 2008, both CSFTL and TTGP have been using the measures for each and every deploying CSG and ARG and forward deployed groups.

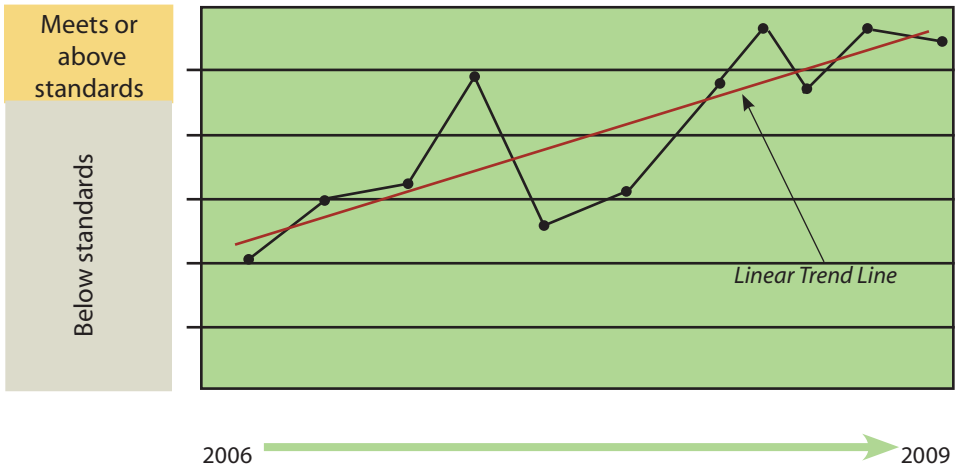
There are 23 separate measures that assess the effectiveness of people (training), processes and tools. Since the original measures were drafted in 2006, TTGP has seen a steady improvement in CSG and ARG KM effectiveness and a significant improvement in those CSGs and ARGs that have participated in the Pacific Fleet Response Training Plan more than once since this three-phased KM approach was implemented in 2006.

Figure 1 shows the steady improvement demonstrated by Pacific Fleet strike groups. Tactical Training Group, Pacific maintains that this demonstrated improvement is directly related to the continued exposure of CSGs and ARGs to the training, mentorship and assessment provided by the KM team.

Knowledge management techniques are generating direct and visible improvements in the way that Navy strike groups plan and execute complex operations. The three-phased approach that TTGP executes with each CSG and ARG ensures that KM principles are highlighted as a key enabler to mission accomplishment. By embracing KM principles when developing and exercising C2 processes in its FRTP cycle, the fleet is better able to plan and execute assigned missions. CHIPS

Tim Snyder is the chief knowledge manager for the TACTRAGRUPAC NCW Syndicate. For more information about TACTRAGRUPAC and course information, go to www.ttgp.navy.mil/.

Figure 1. Pacific Fleet IM/KM Assessment Results 2006-2009.



Knowledge management techniques are generating direct and visible improvements in the way that Navy strike groups plan and execute complex operations.

ATLANTIC OCEAN (Sept. 21, 2009) The aircraft carrier USS Harry S. Truman (CVN 75) and ships from participating nations take part in a NATO mine countermeasures exercise upon the completion of Joint Task Force Exercise (JTFX). JTFX is a scenario-driven tactical exercise supporting major combat operations for the Harry S. Truman Strike Group. The exercise provides training for the strike group to proceed into a Fleet Synthetic Training - Joint (FST-J) exercise for final deployment certification. U.S. Navy photo by Mass Communication Specialist 3rd Class David Danals.

Federal CIO Council Releases Guidelines for Secure Use of Social Media

By Christy Crimmins

The use of social media has become a popular topic within the Department of the Navy, Defense Department and across the federal government. As agencies begin to venture into this media, whether it is creating an agency Facebook page or updating constituents via Twitter, precautions must be taken and risks should be assessed. While these tools open up many avenues for broader communication and collaboration, they also come with threats to network security.

On Sept. 17, 2009, the Federal Chief Information Officers Council released a paper titled, "Guidelines for Secure Use of Social Media by Federal Departments and Agencies." This paper, issued by the Federal CIO Council's Information Security and Identity Management Committee, provides guidance for federal agencies that use social media to collaborate, communicate and share information both internally and externally.

Today's Threats

While the threats to social media users are numerous and ever-changing, the Federal CIO Council's paper narrows focus to the top three potential threats to federal employees, infrastructure and information. They are: spear phishing, social engineering and Web application attacks.

Spear phishing, a targeted approach to traditional phishing scams, uses information unique to the users to trick them into divulging valuable information. This is accomplished by masking communications as internal documents or using personal information to make the communication appear as though it is coming from a legitimate source. These attacks rely on the perpetrator obtaining specific information about the target. When users post personal information to their social networking sites, they are providing attackers with the tools they need to carry out these scams.

Like spear phishing, social engineering relies on the attacker's ability to gather personal information about a target. The paper's primary author, Earl Crane, outlined the threat. "The first step in any social engineering attack is to collect information about the attacker's target. Social networking Web sites can reveal a large amount of personal information, including resumes, home addresses, phone numbers, employment information, work locations, family members, education, photos and private information. Social media Web sites may share more personal information than users expect or need to keep in touch."

As more government employees join social networking sites, they are likely to identify themselves as government employees. When aggregated, this information can provide an Internet footprint valuable to our enemies. According to Crane, an attacker may learn personal information about an individual and build a trust relationship by expressing interest in similar topics.

Attackers use social media to build relationships with a single user, gaining trust and exploiting the relationship by collecting personal information and using their association to extend their reach throughout the user's network of friends and colleagues.

The third threat outlined in the paper is Web application attacks. Web applications are dynamic Web pages that use scripting to provide additional functionality. However, additional functionalities come with additional opportunities to exploit the Web application. Social media Web sites are advanced Web applications; their use requires a high level of interaction and capabilities. This opens up social media Web sites to a wide range of vulnerabilities exploitable by attackers.

For example, Web applications written by third parties are routinely deployed on social networking sites and often require users to grant them access to their profiles as a condition for accessing or running the application. Granting full access to these third party applications can result in the compromise of user accounts and/or the installation of malware on the users' computer.

Mitigating the Threat

In addition to outlining the threats, the Federal CIO Council's paper provides suggestions for mitigating threats. These include a detailed outline of five recommendations: Policy Controls, Acquisition Controls, Training, Network Controls and Host Controls. Users are generally the weakest link when attempting to secure social media networks. While network, host and acquisition controls can go a long way toward monitoring and preventing intrusions, the onus is on users to keep their personal information private.

To this end, federal agencies are advised to update current information sharing and security policies to include emerging Web 2.0 and social media technologies. Additionally, agencies should include awareness of Web 2.0 policy, guidance and best practices as part of employee annual security training.

Agencies across the federal government are using social media tools to both engage with the public and perform their day-to-day operations. While they provide an opportunity for the government to achieve its mission collaboratively and efficiently, they also present significant risks to network security. Agencies must be aware of the threats and mitigating factors to successfully and effectively use Web 2.0 tools.

The full document, Guidelines for Secure Use of Social Media by Federal Departments and Agencies, is located on the DON CIO Web site at: www.doncio.navy.mil under the Policy and Guidance link. Search on "social media." CHIPS

Christy Crimmins provides communications support to the DON CIO.

Tools to Dispel Myths about Your IT System's Power Quality

By Steven Krumm and Mary Hoffken

IF you have worked in the electronics or information technology fields for any length of time, you have probably blamed power fluctuations for causing problems to your systems. Most of us have heard the urban legend about the computer that crashed around the same time every evening and the clever technician-hero who discovered that it occurred at the same time the janitor plugged in a vacuum cleaner on the other side of the wall.

Poor electrical power quality is easy to blame for problems you are experiencing with your organization's IT systems because most people don't know much about it and aren't responsible for its generation, distribution, or the natural or human events that cause disruptions.

But once power quality is cited as the culprit, the IT professional often has to take action. To help you get started, this article will provide some basic information about electrical power quality.

Getting Started

To conduct a power quality study, you need a power quality analyzer for testing the integrity of electrical power distribution systems and for locating faults.

The analyzer will give you the ability to validate power quality coming from your supplier; detect problems external and internal to your room or building; help categorize and diagnose problems; uncover hidden or intermittent issues; verify electrical system capacity; and measure energy usage.

The Fluke 430 Series Power Quality Analyzer, AEMC 3945 Power Quality Analyzer and the Dranetz-BMI Power Quality Analyzer offer the features for a comprehensive power quality study and cost under $10,000.

Surface Combat Systems Center (SCSC) in Wallops Island, Va., uses the Dranetz-BMI PowerVisa 440D with Dran-View 6 software (DADMS ID #49679).

But a word of caution: Power analyzers and other electrical test equipment should be connected by a certified electrician.

Resolving the Problem

There are four steps to satisfactorily resolve your power quality problems: planning, monitoring, evaluating and mitigating. Don't bypass the first three steps because they are as important to successfully mitigating power quality problems as properly preparing a surface is to a satisfactory paint job.

If you suspect a power quality problem, carefully plan where to connect the analyzer. SCSC has two analyzers which are often used in pairs. One is located at the electrical panel closest to the equipment experiencing the problem, and the other is located closest to the source of power for the building. You may be surprised to learn there are more power quality problems generated inside your building than coming from the source of electricity.

After connection, install the memory card and set up the instrument configuration. The monitor we use provides automatic, wizard, upload or manual setup options. Use the automatic setup option and then check the analyzer phasor diagram to make sure the electrician connected each probe to the corresponding A-B-C neutral leg.

To capture intermittent events and collect enough data for analysis, we recommend 60 days for power quality studies.

During the collection period, the tech-

April 2007

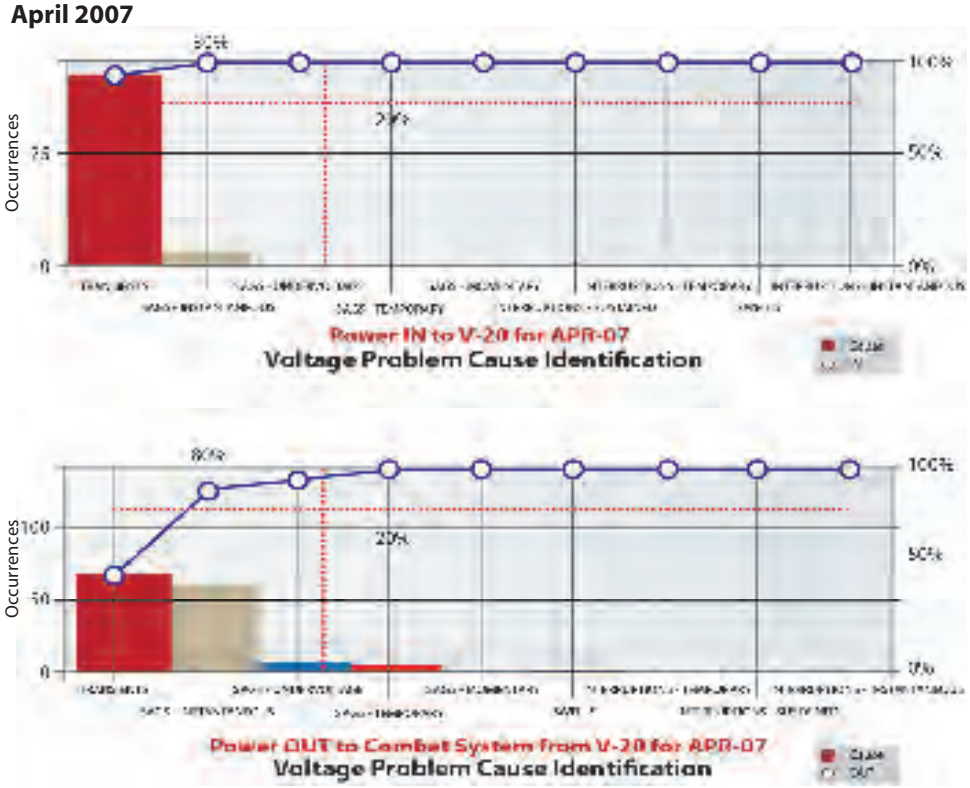


Figure 1.

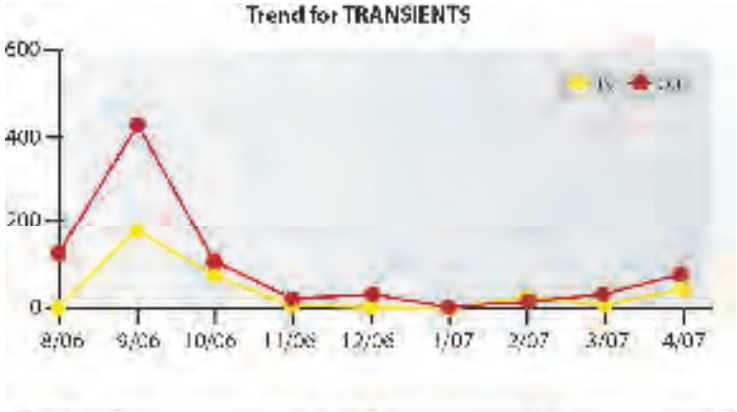
nicians need to keep a log with the date, time and description of equipment problems. This will help focus the data analysis effort. Data are recorded on a compact flash card. A 256 megabit compact flash card will hold approximately 30 days of data. If the card fills up in a day or so, you probably have installed the unit incorrectly.

Once you have collected enough power quality data, it is time to analyze it. The analyzer software allows you to view the information as event lists, graphs, or you can create custom reports.

We initially run a report that summarizes all disturbances by category and magnitude. If we find measurements outside industry standards or customized limits, we compare notes and any other available information, including anecdotal, about the circumstances of the power quality event and the effects on the equipment.

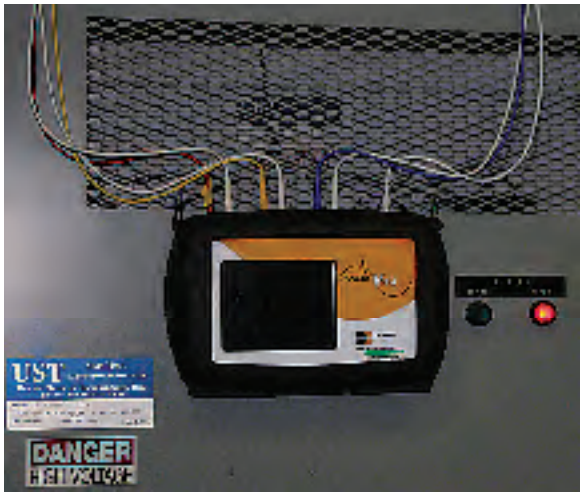
We also copy the event list into Microsoft Excel to feed into our command metrics dashboard. A Pareto chart (Figure 1) and a line chart (Figure 2) are used to visually communicate complex information to managers in a simple, concise manner.

The Pareto chart clearly shows the categories of the top 20 percent of the power quality issues, and the line chart shows the trend for those top issues.



DATE	CAUSE	IN	OUT
8/06	Transients	0	126
9/06	Transients	177	427
10/06	Transients	73	104
11/06	Transients	2	11
12/06	Transients	0	26
1/07	Transients	0	0
2/07	Transients	23	17
3/07	Transients	6	27
4/07	Transients	42	68

Figure 2.



At right, a power analyzer in use at the Surface Combat Systems Center. Always seek the assistance of a certified electrician when using electrical power test equipment. Remember that the electrical wiring in older buildings is often not well-documented. Additions and modifications to the electrical wiring over the years, by certified electricians or a handyman or technician, add another level of uncertainty about the wiring. The difficulty is that these changes over time may eventually lead to a fire hazard, a shock hazard, unexpected failures and costly repairs, or perhaps all of these problems.

Power Quality Problems

There are five major categories of power quality problems: interruptions, sags, surges, transients and harmonics.

✓ Interruptions occur when the line voltage is reduced to zero. Interruptions can be momentary (less than two seconds) or sustained.

✓ Sags are a short duration (less than two seconds) decrease in the line voltage.

✓ Surges are short duration increases in line voltage.

✓ Transients are very short duration but significant deviations in line voltage (usually high voltage spikes).

✓ Harmonics are distortions in the shape of the alternating current (AC) waveform.

Depending on the intensity and duration of the power quality problem, unprotected IT equipment may be damaged.

Since discussing the causes of power quality problems are beyond the scope of this article; we will, instead, focus on the tools for determining if you have a power quality problem and in what ways your power is nonconforming to your equipment's power requirements.

Determining Power Quality

Probably, no organization has "perfect" electrical power quality, so you need to determine if your electrical power quality is "good enough" to effectively operate your IT system. It is important to know what the threshold is between acceptable or unacceptable power quality; otherwise, your solution may either not fully resolve the problem or may exceed your actual requirements and thus be too complex or costly.

There are two straightforward ways to determine what constitutes an adequate power supply. You can use the Information Technology Industry Council (ITI) CBEMA Curve or the manufacturer's equipment specifications. The ITI (CBEMA) Curve was published by Technical Committee 3 (TC3) of the ITI (formerly known as the Computer and Business Equipment Manufacturer's Association).

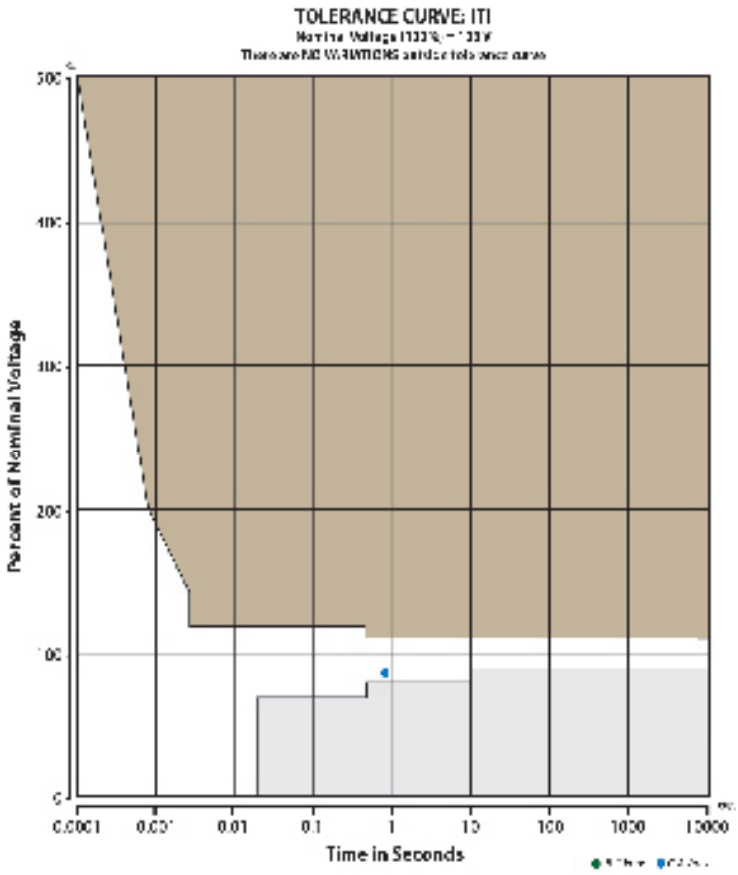


Figure 3.

The manufacturer's equipment specification may not be detailed enough for all characteristics of electrical power. For example, the electrical specifications for a popular router include: input voltage of 180 to 264 volt alternating current (VAC); input line frequency of 47 to 63 hertz; and a source service requirement of 20 amps.

While you should determine if your power meets these requirements, these requirements lack the time element of momentary disturbances that could still cause problems with your IT equipment.

Another standard way to determine acceptable power quality is to use the ITI CBEMA Curve (see Figure 3). While there are many factors that contribute to power deviations, to simplify matters, the CBEMA Curve only measures the voltage deviation from the norm; it is the only factor taken into account.

The CBEMA Curve effectively encompasses all the factors involved with voltage deviations, from long term through to high-speed distortions of the waveform. The CBEMA Curve takes into account that equipment fitted with a power filter, or surge protection device, can protect against electrical noise interference and damaging power transients; and therefore, should be able to withstand greater deviations the shorter the timing of the deviation.

In the CBEMA Curve, the X-axis measures duration (time) and the Y-axis measures magnitude (voltage) of the power event. The chart has three areas: the prohibited region, the no interruption in function region, and the no-damage region.

Satisfactory power quality occurs when there are no power events outside the no interruption in function region. This chart, which can be generated by the analyzer software, provides a very simple and powerful method of determining if your power quality is sufficient to support your equipment.

Case in Point

Now let's put it all together with an example.

The Common Scenario Control Environment (CSCE) is a Versa Module Eurocard (VME) chassis-based simulator that connects to the Ship Self Defense System to drive a common scenario for combat system development testing.

Basic Definitions
amps – a unit of electric current.
hertz – is a unit of frequency. It is defined as the number of complete cycles per second.
The volt is defined as the value of the voltage across a conductor when a current of one ampere dissipates one watt of power in the conductor.
The watt (symbol: W) is a derived unit of power in the International System of Units (SI). It measures rate of energy conversion. One watt is equivalent to 1 joule (J) of energy per second.

The Warfare System Interoperability and Integration Testing (WSIIT) customer reported that the CSCE rebooted at irregular intervals and interrupted certification test events. The customer believed that the problem was caused by electrical power deviations, so we had an electrician connect one of the Dranetz analyzers to the electrical power panel that supplied power to the equipment rack. After a few weeks of monitoring, the customer reported a problem, along with the date and time it occurred.

After analyzing the data captured on the flash card it was determined that there were no power quality events during the time the problem occurred. The power quality events that did occur at other times were within the *no interruption in function* region of the CBEMA Curve.

Technicians then began to troubleshoot the equipment rack and determined that a power filter was faulty. The problem was corrected and no further reboots occurred.

Electrical power quality problems can adversely affect your IT equipment. There are different types of power quality problems, and they can originate externally or internally within your building. You should tailor your remediation efforts to the value of the data or the cost associated with the loss of service. A power quality analyzer, installed by a certified electrician, and analysis software will provide the tools to dispel any power quality myths in your organization. CHIPS

Steve Krumm is the Surface Combat Systems Center, Combat Systems Technology division head.

Ms. Mary Hoffken is a senior systems analyst with Lockheed Martin Information Systems and Global Services.

Navy Career Tool System Puts Sailors in the Driver's Seat for Job Applications

Self-service option is the latest in a series of enhancements to CMS/ID

By Deborah Gonzales

The newest update to the Career Management System/Interactive Detailing (CMS/ID) gives Sailors a self-service option to help manage their professional career path and negotiate orders for their next job assignment.

Technical support, provided by the New Orleans Office of Space and Naval Warfare Systems Center (SSC) Atlantic, for the development and deployment of the "Sailor Apply" capability in July 2009 has enabled active duty Sailors to submit their own Permanent Change of Station (PCS) job applications in CMS/ID via the Internet, similar to applying for a job online in the private sector.

The new functionality, which mirrors the process already used successfully by drilling Reservists to submit assignment requests, complements the detailing process, augments traditional application methods and provides a total force capability for the Navy.

To submit applications to Navy detailers, Sailors must meet Perform to Serve (PTS) requirements and be within their orders negotiation window.

CMS/ID is the centerpiece of a total force Web-based Navy Career Tools suite that empowers active duty, full-time support and Selected Reserve (SELRES) Sailors to manage their careers. The system enables enlisted Sailors to research jobs; update their duty preferences; identify the skills and other requirements needed to make informed decisions to achieve their career objectives; and apply for future jobs. Automatic alerts in the system keep Sailors informed about assignment opportunities and key career milestones. Approximately 15,000 billets (jobs) are listed in CMS/ID monthly.

Until July, the only way active duty Sailors could apply for assignments was through their command career counselors. The new self-service function now gives all Sailors the option of driving the application process themselves.

Sailors research and apply for potential assignments during each month's two-week application window, though the job search process begins nine months prior to a Sailor's projected rotation date (PRD).

A series of color-coded indicator lights pop up on screen in CMS/ID as the system matches the Sailor's personal information with job requirements. Gates prevent applicants from selecting jobs in the wrong paygrade or Navy Enlisted Classification (NEC) and regulate which jobs are available to the Sailor.

Flags warn of factors that could affect whether a detailer approves the application. These capabilities were put in place in an earlier CMS/ID release so that career counselors could begin preparing Sailors to submit their own applications.

Reliance on CMS/ID for career management continues on the increase as demonstrated by 1,878,427 logins since January and 106,352 job applications processed, said Capt. Michael Murphy, program manager for the Sea Warrior program (PMW 240), which manages the CMS/ID application for the Chief of Naval Personnel (CNP)/Deputy Chief of Naval Operations (DCNO) Total Force.

"Deployment of the Sailor Apply capability to the full active and Selected Reserve Navy team via CMS/ID is a huge milestone for us," Murphy said. "Success represents completion of one of the CNP's strategic initiatives for FY09, as well as one of our PMW 240 strategic objectives."

The single information technology acquisition agent for the Navy's manpower, personnel, training and education (MPTE) enterprise, the Sea Warrior program is a component of the Navy's Program Executive Office for Enterprise Information Systems (PEO EIS), which develops, acquires and deploys seamless enterprise-wide IT systems with full life-cycle support for the warfighter and business enterprises.

The Sea Warrior program comprises a portfolio of more than 40 business applications and is focused on enterprise IT management practices, processes and execution to address time-critical business capability gaps ashore and afloat and to migrate or sustain current legacy systems supporting manpower, distribution, pay and personnel management, and medical reporting.

The PMW 240 team is committed to advancing the Navy's total force vision by transitioning to integrated solutions backed by rigorous, enterprise-level IT portfolio management for ashore, afloat and expeditionary units.

To support this mission, SSC Atlantic's New Orleans Office is the technical services provider to PMW 240 and PEO EIS, per-

Personnel Specialist 3rd Class Joanna Rimando of Personnel Support Detachment New Orleans was among the many Sailors who used the new self-service capability in CMS/ID in July to apply for her next duty assignment. Photo by Mass Communication Specialist 2nd Class John P. Curtis, Public Affairs Office, Naval Air Station Joint Reserve Base New Orleans.

forming project management; software engineering; software development, deployment and sustainment; requirements management; configuration management; testing; production support; and quality assurance.

The New Orleans fleet and customer support team provides customer support center and help desk services. The networks engineering and the information assurance applications and systems teams provide program hosting support for CMS/ID in the New Orleans Office Navy Data Center.

In keeping with PMW 240's disciplined performance requirements, the New Orleans Office CMS/ID development team provided technical support for the new self-serve job application function during a five-month assessment and operational test at 15 shore and sea commands and squadrons.

"There have been many early indications that this capability would be extremely well-received," said Kathryn Bailey, long-time CMS/ID project manager at the New Orleans Office. "Application numbers are higher this cycle than they have ever been. I'm very proud of the CMS/ID project lead, Darren Darby, and [the] development team for producing such an important and useful tool for the Sailor and the Navy."

Career counselors will retain the option to review and modify requests, submit applications and perform a vital mentoring role in helping guide good career choices, with Sailors serving as active partners in the orders negotiation process.

Many career counselors report that the new capability is particularly beneficial to Sailors who are familiar with the detailing process thus giving them extra time to work with more junior Sailors in selecting their next assignments.

CMS/ID enables commands to view the service records of Sailors applying for jobs in their commands, rate their qualifications and provide their rankings to detailers.

The system assists detailers and placement coordinators at the Navy Personnel Command (NPC) in Millington, Tenn., with the distribution and placement of naval personnel, identifying the best job for the Sailor and best Sailor for the command.

While the detailer makes the final decision on who gets the job, CMS/ID provides a voice for input into that choice. Interaction between the command, command career counselor, detailer and Sailor remains the most important aspect of career management.

Command leadership will continue to steer the detailing process, ensuring career choices strike the proper balance in meeting the needs of Sailors, their families and the Navy.

Providing this self-service option is the latest in a series of continuing enhancements to CMS/ID. In November 2008, the New Orleans development team enabled the display of a separate category for jobs supporting the global war on terrorism, making it much easier for Sailors to view and apply for these career-enhancing and rewarding positions.

In addition, new capabilities afforded to SELRES Sailors in the November release provided parity with their active duty counterparts, displaying more professional data, increased billet information and qualifying indicators to show appropriate fit to position/billet. This release also linked the NEC code displayed in CMS/ID to the Navy Training Management and Planning System (NTMPS), which displays NEC details, course convening dates and prerequisites for awarding the NEC.

Common access card (CAC) login was implemented in the April 2008 release, per Defense Department mandate, as well as the capability for Reserve detailers (assignment coordinators) to screen applicants for proper fit into a billet.

CMS/ID has its origins in a legacy system known as the Job Advertising and Selection System (JASS). In October 2004, the JASS development team, under Bailey's project leadership at the former SSC New Orleans, finalized a redesign of the system as the first phase of working toward NPC's requirements to have the Navy's MPTE programs work together to enhance warfighting effectiveness, empower Sailors to manage their careers, and ensure the right Sailor with the right skills is assigned to the right position.

NPC's launch of this redesigned system, known as JASS Career Management System (JCMS), provided the acquisition baseline to begin delivering a Web-based distribution environment and introduced the concepts of Job Family/Job Code and Job Title.

Sailors had immediate access to their enlisted master file — a reference page containing personal career and contact data — and could make more educated career decisions by selecting open requisitions and comparing career growth opportunities. Commands owning the billets had access to view, rank and comment on potential applications.

In August 2006, JCMS was renamed CMS/ID. With the name change came the indicator lights, gates and flags that provide Sailors a fast, easy way to check if they are eligible for jobs listed in CMS/ID.

Each new release has matured CMS/ID into a valuable tool in the distribution process. Sailors access CMS/ID either directly through the CMS/ID Internet Web site or through the Navy Knowledge Online (NKO) portal on the NPC Web site.

In the NAVADMIN 200/09 announcement of Sailors' ability to submit their own job applications, Chief of Naval Personnel and Deputy Chief of Naval Operations (Total Force) Vice Adm. Mark Ferguson said the added functionality reflects the continued commitment to place more career management tools in the hands of Sailors as a core initiative in the Navy's total force strategy.

Future CMS/ID enhancements will continue to improve Sailor career management and Navy business operations.

CMS/ID is one of the Navy Military Personnel Distribution Systems (NMPDS), a collection of mission-essential systems supporting Navy personnel distribution, mobilization and fleet readiness that assists Navy planners in maintaining a flexible readiness posture. The New Orleans Office provides technical services for all systems under the NMPDS umbrella for the PMW 240 Sea Warrior program.

"Enabling this new Sailor Apply capability is another milestone in our long history of delivering products and services supporting Navy manpower and personnel business requirements, and [it] reflects the dedication, long hours and hard work from our New Orleans team," said Deputy Technical Director for SSC Atlantic Jacqueline Goff. CHIPS

Deborah Gonzales provides support to the SSC Atlantic New Orleans Office.

Q & A with Capt. Michael S. Murphy
Sea Warrior (PMW 240) Program Manager

Q. The Career Management System/Interactive Detailing application is Web-based, can you talk about the technology used?

A: CMS/ID is hosted in the SPAWAR Atlantic New Orleans Office Shared Services environment using Unix-Sun Solaris and Windows 2000 operating systems in a virtual machine operating environment. It was developed using HTML, Dyno Script, Visual Basic, JAVA, Jboss, EJBs (Enterprise JavaBeans — a database query language) and Apache Web Server. The database is Oracle 10.2 ashore and SQL/Server afloat.

Q: Can deployed Sailors access CMS/ID?

A: Yes. Sailors on ships who have Internet connectivity, either pierside or while at sea, have access to CMS/ID. In addition, CMS/ID in a disconnected mode is deployed on nine ships to evaluate the viability of non-Internet access. They are the USS Pinckney (DDG 91), USS Gary (FFG 51), USS Donald Cook (DDG 75), USS John Paul Jones (DDG 53), USS Nimitz (CVN 68), USS Ponce (LPD 15), USS Jarrett (FFG 33), USS Antietam (CG 54) and USS Laboon (DDG 58).

On these ships, Sailors have connectivity to an afloat version of CMS/ID, essentially mirroring the ashore version, where they can review all the same data they would see on the Internet version. They can make applications and update duty preferences, just as on the Web version. Once Sailors update applications and personal information, the data replicates to the CMS/ID system ashore via Distance Support servers hosted at the Naval Surface Warfare Center in Crane, Indiana.

Q: Is CMS/ID easy to use?

A: CMS/ID is relatively easy to use. Command counselors can demonstrate how to use CMS/ID, plus there are CMS/ID QuickStart guides and job performance aids available to help familiarize users. Also, if users have questions, they can always ask their career counselor or contact the CMS/ID help desk toll free at (800) 537-4617 or DSN 647-7070.

Q: Is training available?

A: Yes. Many Sailors learn how to use CMS/ID through training at their local commands. In addition, CMS/ID is part of the command career counselor school curriculum that equips counselors to train their people.

CMS/ID training is also conducted at other schools and symposiums. Online, the CMS/ID page on the Navy Personnel Command Web site has links to training aids such as the CMS/ID QuickStarts, User Guides and Fact Sheets.

The CMS/ID page under the Career Management tab on Navy Knowledge Online, on both the Internet and afloat versions, also provides a full range of training links and tutorials.

Q: Is there help desk support?

A: Sailors can get support by contacting the Navy Personnel Command Customer Support Center in Millington, Tennessee, toll-free at (866) U-ASK-NPC or (866) 827-5672, Monday through Friday, 0700 to 1900 Central Standard Time, or by e-mailing CSCMAILBOX@NAVY.MIL.

The NPC Customer Service Center is a leading-edge contact center providing support to Sailors and their families around the world. In addition, Sailors can contact the Global Distance Support Center (GDSC) — the fleet's single point of entry for assistance that provides guaranteed resolution for any question, any time. Contact the GDSC toll-free at (877) 418-6824 or e-mail help@anchordesk.navy.mil. The GDSC Web site, called Anchor Desk, provides useful information and is posted at www.anchordesk.navy.mil/.

Q: Do the Navy Military Personnel Distribution Systems (NMPDS) applications supported by the PMW 240 Sea Warrior program have a similar look and feel?

A: The applications are Internet-based and have a common Web application look and feel. This said, we have a significant amount of work ahead of us to give all the Sea Warrior program applications a similar look and feel. This is due to the fact that until the Sea Warrior program was established, at the direction of ASN RDA [Assistant Secretary of the Navy for Research, Development and Acquisition], these systems were managed by different functional and technical organizations with separate funding lines and design and development processes.

Schaumburg, Ill. (June 16, 2009) Capt. Michael S. Murphy, Sea Warrior program manager, (PEO EIS/PMW 240), delivers a Navy Career Tools progress report to the Navy Counselors Association 21st Annual Symposium. U.S. Navy photo MC1 Terence K. Ferguson.

[The] Sea Warrior program will, over time, and at logical points in system life cycles, bring these systems to a point where their use is essentially seamless from an access and look and feel perspective. Make no mistake that we understand the 'ease of use' issue and are doing everything we can to make it easy for Sailors to manage their careers and jobs on Sea Warrior program-maintained systems.

Q: When do career counselors get involved?

A: CMS/ID and other career management systems are tools that help commands and Sailors manage their careers and do their jobs. From the perspective of a career counselor, nothing changed relative as to when they should get involved. Their engagement should begin the moment a Sailor checks on board.

What has changed, with 'Sailor Apply' in CMS/ID, is that CCCs no longer have to submit applications on behalf of their shipmate — though they are still able to do so, as are detailers. CCCs should still be engaged on doing what they do best — counseling Sailors on career choices. CHIPS

USS Kauffman Participates in Multiple Multinational Maritime Exercises

Kauffman crew reassures friends and allies of the U.S. commitment to peace and security in the Western Hemisphere — and plays baseball

By Sharon Anderson

The guided-missile frigate USS Kauffman (FFG 59) pulled in to its homeport the first week of August amid a flurry of ships returning to Norfolk Naval Station. While fleet deployments and homecomings are almost a weekly occurrence in this major fleet port, the Kauffman's hard-working crew had an especially prolific tour of duty, according to Kauffman's Commanding Officer Cmdr. Dale W. Maxey.

"We deployed in April, we participated in the UNITAS Gold exercise, and then we went through the Panama Canal and participated in Team Work South 2009, the other big Chilean-led exercise.

"The Kauffman executed interoperability training with other militaries from both the east and west coasts of South America and Central America, and in port, we would do similar, but much smaller-scale missions, to what the [hospital ship] Comfort does," Maxey said.

Every port visit included military-to-military subject matter expert exchanges (SMEE) and community relations (COMREL) projects, as well as deliveries of Project Handclasp items. Project Handclasp consists of a collection of donated items, such as medical and hygiene supplies, delivered around the world by the U.S. military.

One day before the Kauffman returned on Aug. 5, Maxey, speaking from the ship to local media via telephone, cited the Chief of Naval Operations commitment to strengthening interoperability with international colleagues as part of the national maritime strategy.

"That is exactly what we were working on. We worked with the Mexican navy, with Chileans, Peruvians, Colombians, Brazilians, and we had some of our European allies operating in the Caribbean as well — the French, Germans and British," Maxey said.

In total, the Kauffman operated with military forces from Argentina, Brazil, Canada, Chile, Colombia, Dominican Republic, Ecuador, France, Germany, Mexico, Peru, United Kingdom and Uruguay.

This year's UNITAS Gold marked its 50th anniversary as the longest-running multinational maritime training exercise in the world. The annual U.S. Southern Command-sponsored naval exercise took place off the coast of Jacksonville, Fla., April 20 – May 7.

The exercise was designed to maximize interoperability between the participating multinational forces by taking them through a variety of likely maritime scenarios.

UNITAS, Latin for unity, included 25 ships, four submarines, more than 50 aircraft, 650 Marines and 6,500 Sailors. Training featured live-fire exercises, undersea warfare, shipboard operations, maritime interdiction operations, air defense and surface warfare, amphibious operations, electronic warfare and special warfare.

Maxey said the antisubmarine warfare training was especially valuable because the U.S. Navy employs nuclear-powered submarines, and there is an emerging threat with the worldwide proliferation of conventional, or diesel-powered, submarines.

"There are two big areas that the Kauffman was able to exchange [with the South American navies] on equal terms. One is ASW, antisubmarine warfare, which is one of our mission areas. Several of the South American countries have diesel submarines with competent crews and capabilities. We rarely get extensive exercise time tracking and operating against real-world diesel submarines. They hosted the exercise, but we received some valuable skills out of it.

"The second one is a shared challenge," Maxey said. "Everybody has maritime security concerns for their own country. They have a slightly different flavor depending on whether you are Colombia, Chile or the United States."

Maritime Domain Awareness is a top training objective, Maxey emphasized. In the MDA effort, multinational partners acquire and share maritime information with a broad array of global partners to reduce their vulnerability to attack and improve cooperation toward maritime security and safety. By investing in this

PACIFIC OCEAN (July 19, 2009) Colombian Navy Lt. Alberto Cordoba Garcia, center, explains the safest navigation route to Cmdr. Dale W. Maxey, right, commanding officer of the guided-missile frigate USS Kauffman (FFG 59), and Lt. j.g. Curtis Sanders, while pulling into Bahia Malaga, Colombia. Kauffman is on a deployment to the U.S. 4th Fleet area of responsibility supporting the U.S. Southern Command exercise Southern Seas 2009. U.S. Navy photo by Mass Communication Specialist 2nd Class Brandon Shelander.

concept, the United States and its international partners achieve their common maritime security goals.

"At the tactical level, all of these navies come with the ability to track down a suspect vessel and conduct a boarding operation on that ship. Several of the nations we have worked with have competent boarding teams. We call it NEO (noncombatant evacuation operation); they call it something else, but it is all about establishing maritime security capabilities.

"We learned a lot from those teams because everybody does things slightly differently. ASW and our boarding operations really got a good boost in our training. At the end of this event, particularly in those two mission areas, we were better than we were when we started," Maxey said.

After UNITAS Gold, Kauffman sailed on to Colombia where ships from Brazil, Chile, Colombia, Peru and the United States participated in "Operacion Multinacional Alianza," a naval exercise hosted by Colombia.

Kauffman then participated in a bilateral exercise with Peru. For several days, the units conducted integrated ASW exercises off the coast of Lima, Peru.

During the two-week exercise, Team Work South 2009, hosted by the Chilean Navy, Kauffman again engaged in rigorous training involving ASW exercises, coordinating defense against littoral threats and participating in surface gunnery exercises, among other training events, to develop at-sea proficiency and the ability to operate in a multinational task force. Participants said the training schedule was relentless and challenging.

During SOUTHCOM's Southern Seas 2009, Kauffman operated throughout South America, Central America and the Caribbean. Southern Seas, which stretches from April to October, is part of SOUTHCOM's Partnership of the Americas Strategy; it serves to underline interoperability and cooperation between the United States and partner nations.

If it seems like these exercises have a common theme of enhancing interoperability and cooperation, it is because they do. But that does not mean they are merely routine, according to Maxey.

"It was an ordinary mission set, but it was an extraordinary experience. Our mission was to build on partnerships and improve our interoperability and work to smooth communications and relationships for everybody to share maritime security concerns.

"With many of the nations we worked with, we were on a peer capability; we did not roll in above their capabilities. Their boarding teams were excellent. They have real-world diesel submarines with capable crews so they gave us a good run for our money in antisubmarine warfare. We came away stronger than when we started," Maxey said.

But relationship building extends beyond military partners to local civil and medical authorities and citizens, according to Maxey, who said that strong bonds are formed during the exercises.

Southern Seas involves face-to-face experiences between U.S. Sailors and thousands of host nation citizens and military personnel that can create lasting friendships and promote cultural understanding. The Kauffman crew also found time to put a new spin on the old anthem "Take Me Out to the Ballgame."

"A year ago, the Kauffman, while deployed, stopped in the northern Chilean city of Arica and established a good relationship with the folks there. They challenged some local sports folks to a baseball game. That sporting event received

ATLANTICOCEAN(April23,2009)Theguided-missilefrigateUSSKauffman(FFG59)isunderwaywith,fromleft,theU.S.CoastGuardcutterThetis(WMEC910),theChileanNavyfrigateAlmiranteBlancoEncalada(FF-15),andtheBrazilianNavyfrigateBNSConstituicao(F42)duringUNITASGold,the50thiterationofthelongest-runningmultinationalmaritimeexerciseintheworld.NavalunitsfromtheU.S.areparticipatinginseveralrealistictacticaltrainingscenarioswithmaritimeforcesfromBrazil,Canada,Chile,Colombia,Ecuador,Germany,Mexico,PeruandUruguayofftheCoastofFloridaApril20-May5.U.S.NavyphotobyMassCommunicationSpecialist2nd Class Ron Kuzlik.

SOUTHERN SEAS '09

Southern Seas 2009 is a six-month (April – October) naval deployment to the Caribbean and Central and South America. A task group of three ships — USS Kauffman (FFG 59), USS Doyle (FFG 39) and USS Ford (FFG 54) — conducted a variety of exercises and multinational exchanges to enhance interoperability, increase regional stability, and build and maintain regional relationships with countries in the region. Formally known as the Partnership of the Americas deployment, Southern Seas gives a distinct name to one of U.S. Southern Command's marquee deployments.

national coverage in their media. It generated so much news locally that they have stood up an entire Little League organization in the northern third of their country, a country that had not previously played baseball at all. They now have a Little League organization that includes six cities," Maxey said.

Maxey said the crew was thrilled with the Chilean response to baseball, and he said their eager interest in the sport goes much deeper than their love of the game.

"When we went back this time, a year later, and played against them with the same team, we could not 'take' them. The great benefit is that they are looking to the United States as a place they can interact with; in this case, they just wanted to be a part of the Little League organization [headquartered in Williamsport, Pa.].

"But it wasn't just sports, we engaged with a couple of the schools. We did some maintenance and talked to the students. I found this time, 18 months later, that several of those schools have developed an English curriculum and have brought in an English-speaking teacher and started to teach their students to speak English.

"They have asked that if the United States returns, that instead of doing school maintenance, they want our Sailors to come in to help teach the class, so the students will have the opportunity to interact with Americans. At our country's level, that is fantastic goodwill with people that may never have an opportunity to meet Americans any other way," Maxey said.

According to Maxey, command and control for the exercises went well.

"Almost exclusively all of our coordination for the exercises and our command and control during the exercises was executed by e-mail and on chat. When we went down on satellite, it was a significant blow. Even with the other partner nations we were working with, a lot of our exercise coordination was on unclassified e-mail, passing the different pre-exes (pre-exercises) information.

"During the Chilean exercise, Team Work South, one additional system that they put on was very similar to our own chat capabilities. The Chilean-developed system provided exercise feedback as far as positions of units and, at the same time, provided a direct communications capability. We had liaison communicators from the Chilean Navy that provided the interface between the Kauffman and the Chilean flagship and headquarters.

"Some of the nations we were working with have an active acquisition process; the ones I saw were with European nations. They are buying newer ships from European countries. We operated with the British and the Chileans during Team Work South, and the Chileans had newer ships purchased from Britain, the British contingent that participated in the exercise. They were also purchasing new technology that is available to the Europeans. I found technological parity with the groups I was working with rather than somebody being significantly ahead," Maxey said.

After the exotic port calls and tough training schedule, the Kauffman's 215 Sailors are happy to be home, said Maxey. But not for long, the Kauffman crew is already gearing up to deploy in early 2010.

"The team is excited to be back, and for me as the CO, I could not have asked for a better bunch of Sailors to take to sea. They have entered every mission well, and they have done it through a diverse set of requirements for their skills. They have been fantastic. I am honored to command them, and I am glad to bring them back home safely." CHIPS

ARICA, Chile (July 9, 2009) Sailors aboard the guided-missile frigate USS Kauffman (FFG 59) man the rails while entering port in Arica, Chile. Kauffman is on a four-month deployment to Latin America and the Caribbean as part of Southern Seas 2009 supporting the U.S. Southern Command Partnership of the Americas. Southern Seas focuses on training exercises, military-to-military engagements, and theater security cooperation engagements to enhance relationships with partner nations in the region. U.S. Navy photo by Mass Communication Specialist 2nd Class Brandon Shelander.

Training Information Systems Technicians to Protect Navy Networks

By Mary Purdy

Today's environment presents enormous challenges and unprecedented opportunities, not only to the Department of the Navy (DON) information assurance (IA) workforce charged with defending our cybersecurity interests, but also to the traditional training regimes that prepare Sailors and Marines to meet their operational commitments.

There are approximately 14,000 full-time and 6,000 part-time military and civilian personnel in the DON cybersecurity (CS)/IA workforce. CS/IA functions primarily focus on the development, operation, management and enforcement of security capabilities for systems and networks. Significant portions of the CS/IA workforce are technical individuals with privileged access who perform network operations and system administration tasks. A smaller portion of the CS/IA workforce is made up of IA management personnel, computer network defense service providers, certification and accreditation team members, red and blue team members, and information assurance system architects and engineers (IASAE).

Cybersecurity/information assurance competencies and work functions are mapped to training requirements. Personnel who perform CS/IA technical functions are trained in baseline skills through a multidimensional program that includes in-residence courses, distributed learning, blended training, exercises and certification testing. All members of the CS/IA workforce are required to obtain the appropriate commercial certification through testing to qualify as part of a standardized workforce; moreover, they are required to sustain and improve their knowledge level with continuing professional education.

Both the Department of Defense (DoD) and DON support free virtual/e-learning courses that prepare the total force to obtain commercial certifications. These commercial courses continue to integrate leading-edge data and information into the courses.

At the same time, cybersecurity training curricula in the traditional Navy and Marine Corps schoolhouses must be thoroughly examined. Once the training standards are validated, the schools must revise the training roadmap so that as Sailors and Marines matriculate in these schoolhouses, they acquire the requisite commercial certification to signify they meet DoD standards.

Plans for the Navy's information systems technician rating, called "IT of the Future," reveal that the rating is being revamped to be an advanced technical field (ATF). The ATF allows the Navy to recruit Sailors to both four-year and six-year obligations. Sixty-five percent of the new recruits will be recruited with a four-year obligation, get their basic training in "A" School, and then go to their first permanent change of station (PCS). Thirty-five percent will be recruited with a six-year obligation and receive advanced training in a "C" School before transferring to their first PCS.

Information Systems Technician "A" School will change from an 11-week course to a 19-week course with the pilot course beginning in July 2010 and formal training to start January 2011. Sailors enrolled in "A" School will graduate with CompTIA's A+ and Microsoft Certified Professional XP (MCP 70-270) certifications.

Thirty-five percent of the new Sailors will go right into "C" School and receive the new system administration (SYSADMIN) Navy Enlisted Classification (NEC). This training path includes additional certifications for Security+ and MCPs 70-290 and 70-291 (for servers).

The new "C" School training will pilot in January 2011. Fleet IT Sailors will have the opportunity to gain these new NECs with additional training that will be announced once the new training is fully in place. The information systems administrator, NEC 2735, will be phased out as a valid NEC. Sailors will be required to hold the new SYSADMIN NEC before being allowed to enroll in more advanced NEC training (i.e., NECs 2780, 2781, 2779).

All Sailors who hold privileged access to servers, routers and switches are required to have appropriate IA and operating system certifications in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. Therefore, current fleet and shore IT Sailors must attain commercial certifications as part of their daily training regimen.

The Sailors can complete the required courses via Navy e-Learning on Navy Knowledge Online; Carnegie Mellon University's virtual training environment at https://www.vte.cert.org/VTEWEB/; or via classroom courses sponsored by Naval Network Warfare Command (NETWARCOM) in fleet concentration areas. Certification for all IT Sailors will be paid for by Navy Credentialing Opportunity On-Line (COOL). Go to https://www.cool.navy.mil for more information. Under no circumstances should an individual in the IT rating pay for required certifications.

The DON's approach to cybersecurity/IA workforce training must remain flexible as the definition of the domain continues to mature and cyberspace capabilities evolve. Since the IT rating is designated as a core CS/IA rating, IT personnel should visit the NETWARCOM Web site, at https://www.portal.navy.mil/netwarcom/ia/default.aspx, for the most up-to-date information on all issues related to IAWF management news. CHIPS

Mary Purdy facilitates the DON Cybersecurity/IA Workforce Management Oversight and Compliance Council.

While stationed at NMCI Det Norfolk,Va, IT2(SW/AW) Mujeeb B. Jimoh, attained the following commercial certifications: CompTIA's A+, Network+, and Security+, and Microsoft Certified Systems Engineer (MCSE).

Welcome to the *Virtual Life*, where we can tailor reality to suit our tastes. Applications like Second Life can give us the illusion of the dream job or perfect relationship we cannot achieve in the real world. Games like World of Warcraft allow us to channel our inner swashbuckler. Social networking sites like Facebook can manage our relationships, and Twitter lets us conduct mass conversations with many people regardless of distance.

Yes, we can live la vita virtual, accompanied by our favorite musical soundtrack and enhanced by whatever means we choose to employ to craft our online image. In this issue, we will look at some of the ways the virtual world has become an extension of our personal space, and for some, a second home. But, as with any new medium, living virtually affects and is affected by human behavior.

Virtually Zippy

It has been a while since we have visited our old friend Zippy and his family. Time and distance can take a toll on relationships, so this year I made a resolution to do more than just e-mail and signed up with a social networking site to see if I could revive relationships with old friends. Of course, the first person who popped up on my friends list was Zippy and, through the modern miracle of webcams, we sat with our laptops at our respective dining room tables and shared a virtual meal together while 600 miles apart.

We have not seen Zippy's twins, Paul and Cassie, for a few years. They are eight years-old now and totally wired (or wireless, as the case may be). Instead of yelling upstairs to tell them it was time for dinner, Zippette texted them, explaining: "They always answer a text message." Both kids arrived shortly thereafter, smartphones in hand, followed by a reminder from Zippette to shut their phones off during dinner. We ate, we talked, we watched the latest JibJab videos together. After making sure we were all properly "friended" on Facebook, we said goodnight and sat back to consider the brave new world of computer-mediated relationships.

The more things change in the world of technology, the more they seem to stay the same as far as the underlying concepts of communication. Before we discuss how computer mediation is affecting relationships, we should review some basic definitions and history. First, communication is a process by which information is exchanged between individuals through a common system of symbols, signs or behavior. Communication may be further defined by two other factors: time and interactivity.

In terms of time, communication may be synchronous or asynchronous. Synchronous communication occurs simultaneously between participants. Asynchronous communication involves a sender recording communications in some form for later retrieval by one or more receivers. Some types of communication may qualify for both categories, for example, a live television broadcast or a recording. Interactivity also has two variables: monologue: one-way with no immediate opportunity for a receiver to respond; or dialogue: equal opportunity for exchange of information between participants. For examples, we will start with some easily categorized forms of communication.

Making a telephone call is a form of synchronous dialogue because all participants are in direct communication with equal opportunity to participate. Leaving voice mail, however, is asynchronous monologue that can become asynchronous dialogue if it becomes a full-fledged game of phone tag.

Radio and television broadcasts have traditionally been asynchronous monologues. However, shows like "American Idol" that allow viewers to vote during the show break that paradigm somewhat. In cyberspace, e-mail, instant messages and bulletin board systems are asynchronous, and chat rooms are synchronous. There are, of course, exceptions to any general classification. Though both participants may meet a technical definition of synchronicity by being in the same place at the same time, any recruit who has been chewed out by a drill instructor would be unlikely to describe the experience as a dialogue with an equal opportunity to participate.

Here is one, last, crucial reference before we move into modern social networking: bulletin board systems. Traditionally, Internet bulletin boards and blogs have a hierarchical, topical structure. Messages are posted within topics and only appear within that topic. Readers must go to each topic to read the messages. As we will discuss shortly, social networking sites like Facebook and MySpace represent a radical shift from this model.

With these concepts in mind we can move on to figuring out where modern social networking methods fit into our communications schemes. In the last issue of CHIPS, we briefly looked at two new disruptive social networking applications: Facebook and Twitter. Given their effects and contributions to virtual communities, it is time to take a closer look at each.

Welcome to My Wall

Facebook or MySpace? Both serve essentially the same purpose: manage relationships online. Because I do not have the space to properly discuss both, I flipped a coin, and Facebook won the toss. Facebook is a privately owned, globally available social networking Web site. Members set up home pages called "Walls" and link their accounts with "friends" to share information. Linked users can see each others' messages, personal profiles, photos and other information. An update to your personal page is posted simultaneously to all your friends' pages and vice versa. Facebook users can also join networks organized by city, workplace, school, region or common interest.

As of September, Facebook reportedly has more than 300 million members worldwide which means that about 22 percent of the world's population has a Facebook Wall. Facebook is primarily asynchronous, though there is some opportunity for chat. It

generally follows a bulletin board structure, though unlike traditional bulletin board systems, posts to individual Walls are published simultaneously on the Walls of friends, including those made by friends. So, if you have 20 friends, and your friends have 20 friends, you could potentially see messages from 400 other people on your Wall.

Facebook users seem to fall into four behavioral categories: static, casual, serious and obsessive. Static users broadcast but do not universally allow messages from all their friends. Quite a few celebrity users fall into this category, preferring to have fans subscribe to their Walls and limiting the messages they accept to a small circle of friends. Casual users have a manageable number of friends with whom they freely exchange information. They check Facebook periodically, treating it as an asynchronous way of keeping up with friends.

Serious Facebook users post messages daily. Hard-core users have Web-enabled smartphones that alert them to a new post, and they respond at every opportunity. No post is unworthy of notice, and if they cannot maintain constant contact, they will exhibit withdrawal symptoms. I am doing my best to resist the siren song of hard-core obsession, but I have pretty much given up, adding "Recovering Facebook Addict" beneath "Recovering PowerPoint Addict" on my personal resume. Having something that lets me maintain relationships with distant friends is incredibly attractive from a *Lazy Person* perspective.

However, sites like Facebook are not without issues. Facebook has been banned in many workplaces, and there are privacy issues associated with posting personal information online. The system has also allegedly been compromised by hackers more than once. Too, there are many stories of people who have encountered difficulties from self-inflicted, embarrassing photos or posts. Facebook has also been blocked intermittently in several countries including Syria, China and Iran, where the exchange of free information and the interests of the government are sometimes at odds.

If you want to use Facebook at home to keep up with friends, be aware of the security risks of sharing personal information. With that in mind, here are my personal rules for Web-based social networking. As always, your mileage may vary, but these work for me:

✓ Keep your friends close and everyone else at bay. I only accept friend requests from people I know, and I do not send friend requests to everyone who has a Facebook account.

✓ Do not post anything you would not want to see on the front page of your local newspaper, The New York Times or the National Enquirer. People who post their spring break pictures really only have themselves to blame. Your online privacy is your responsibility.

✓ Be relevant and concise. People will judge you by what you post.

✓ Set a schedule and stick to it. If you find yourself on the computer at 2:00 a.m. to check Facebook, you have gone beyond serious on the user scale.

✓ Make sure you actually talk to your friends once in a while. Text-based relationships can work, but periodic synchronous interaction, even if it is just over the phone, is a big part of being real friends and not just Facebook friends.

Here's a case in point about how social networking can influence behavior. In early September, two Australian girls aged 10 and 12 went exploring in Adelaide's storm drains and got lost. Fortunately, they had a cell phone. However, instead of calling emergency services, they updated their Facebook status and then waited for rescue, according to ABC News. There may be any number of reasons why they did not call for help. Maybe they did not know the number for emergency services, which in Australia is 000. Maybe they wanted to avoid calling a total stranger and admitting they were lost. Whatever the reason, it shows how ingrained computer-mediated social networking can become in human behavior if we are not careful.

The 800-Pound Canary

Twitter is another popular social networking application that has behavioral implications. It is a "micro-blogging" service that lets users send and read short (140 characters or less) text messages known as "tweets." Tweets are displayed on the author's profile page and authors can decide whether to limit them to a particular circle of friends or make them available to anyone who subscribes. Tweets can be sent through the Twitter Web site, Short Message Service (SMS) or external applications. While Twitter is free, accessing it through SMS may incur provider fees.

Last issue I stated that I had trouble taking Twitter seriously. While I still think the vast majority of what passes through Twitter has about the same density of useful information as a cubic light-year of interstellar space has of breathable oxygen, I have revised my opinion of the system overall since its use in the aftermath of certain elections overseas. Twitter became a way for people to bypass strict information controls, exchange information freely and organize resistance under restrictive conditions. For that, I can forgive any other ether it consumes with fluff messages from various celebrities.

Popular Tweeters are more like gurus with followers waiting for the beep that announces their latest pronouncement. However, because of the information exchange that Twitter helps enable and the types of exchange that both Facebook and Twitter facilitate, both sites came under distributed denial of service attacks (DDOS) shortly after election season was over. No specific source was identified for the attacks, but there is some discussion that the attacks did not follow the pattern usually followed by cyber criminals who try to extort money from businesses by threatening DDOS to their Web sites, according to Wired magazine. Regardless of where the attacks came from, it is clear that someone wanted to shut them down. Thus, we see further demonstration of the power and influence of social media sites.

Web-based social networking will continue to shrink time and space and further accelerate changes in society, business and personal relationships. The scope and effect of these changes are still evolving. CHIPS

Happy Networking!

Long is a retired Air Force communications officer who has written 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.

Enterprise Software Agreements

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 5000.2 on May 12, 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://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

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 Oct 09 (Please call for extension information.)

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

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://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

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://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

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://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

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); (813) 612-7352

Ordering Expires: Upon depletion of Army Small Computer Program (ASCP) inventory.

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.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/

Database Management Tools

Microsoft Products

Microsoft Database Products – See information under Office Systems on page 57.

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); Small Business; (757) 284-6570

TKC Integration Services, LLC (W91QUZ-09-A-0001); Small Business; (571) 323-5584

Ordering Expires:

Oracle: 30 Sep 11
DLT: 1 Apr 13
immixTechnology: 26 Aug 11
Mythics: 18 Dec 11
TKCIS: 29 Jun 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://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Special Note to Navy Users: See the information provided on page 58 concerning the Navy Oracle Database Enterprise License under Department of the Navy Agreements.

Sybase (DEAL-S)

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

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

Ordering Expires: 15 Jan 13

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://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Enterprise Application Integration

Sun Software

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; and 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; (314) 919-1513

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: 31 Oct 09 (Please call for extension information.)

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.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); (703) 709-4610

Ordering Expires: 22 Sep 12

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.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 Oct 09 (Please call for extension information.)

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Microsoft Premier Support Services (MPS-2)

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*** (W91QUZ-09-D-0038); (980) 776-8413

Ordering Expires: 31 Mar 10

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.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 8 to 10 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: 05 May 14

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Planet Associates

Planet Associates Infrastructure Relationship Management (IRM) Software Products – Provides software products including licenses, maintenance and training for an enterprise management tool for documenting and visually managing all enterprise assets, critical infrastructure and interconnectivity including the interdependencies between systems, networks, users, locations and services.

Contractor: ***Planet Associates, Inc.*** (N00104-09-A-ZF36); Small Business; (732) 922-5300

Ordering Expires: 01 Jun 14

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

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.

ProSight has been purchased by Oracle. Products are available from the Oracle (DEAL-O) contract on page 54.

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.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) 708-9127

Ordering Expires:

Quest: 14 Aug 10

DLT: 01 Apr 13

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Enterprise Resource Planning

Oracle

Oracle – *See information provided under Database Management Tools on page 54.*

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); (410) 869-3014

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

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

Carahsoft 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 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 and Army released service-specific DAR guidance for their personnel to follow. Go to the ESI Web site at www.esi.mil for more information.

The DON CIO issued an enterprise solution for Navy users purchasing DAR software. See the information provided on page 58 under Department of the Navy Agreements.

The Department of the Army issued an enterprise solution for Army users purchasing DAR software. See the information provided on the Army CHESS

Web site at https://chess.army.mil/ascp/commerce/contract/FA8771-07-A-0301_bpaorderinginstructions(2)_ARMY.jsp.

As of press time, other DoD users are not authorized to purchase DAR software because service-specific guidance has not been issued.

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)
CREDANT Technologies – ***GTSI Corp.*** – (FA8771-07-A-0309)
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/antivirus_index.htm
SIPRNET site: https://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/antivirus_index.htm
SIPRNET site: http://www.cert.smil.mil/antivirus/av_info.htm

Websense (WFT)

Websense – Provides software and maintenance for Web filtering products.
Contractor: ***Patriot Technologies*** (W91QUZ-06-A-0005)
Authorized Users: This BPA is open for ordering by all DoD components and authorized contractors.
Ordering Expires: 31 Aug 11
Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Xacta - NEW!

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.*** (FA8771-09-A-0301); (703) 724-4555
Ordering Expires: 24 Sep 14
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 for Six Sigma 2007; iGrafx Flowcharter 2007; Enterprise Central; and Enterprise Modeler.
Contractors:
Softchoice Corporation (N00104-09-A-ZF34); (416) 588-9002 ext. 2072
Softmart, Inc. (N00104-09-A-ZF33); (610) 518-4192
SHI (N00104-09-A-ZF35); (732) 564-8333
Authorized Users: These BPAs are co-branded ESI/GSA SmartBUY BPAs and are open for ordering by all Department of Defense (DoD) components, U.S. Coast Guard, NATO, Intelligence Community, authorized DoD contractors and all Federal Agencies.
Ordering Expires: 31 Jan 14
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
SHI
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

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 Desktop Products

Adobe Desktop Products – Provides software licenses (new and upgrade) and maintenance for numerous Adobe desktop products, including Acrobat (Standard and Professional); Photoshop; InDesign; After Effects; Frame; Creative Suites; Illustrator; Flash Professional; Dreamweaver; ColdFusion and other Adobe desktop products.

Contractors:

Dell Marketing L.P. *(formerly ASAP)* (N00104-08-A-ZF33); (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 13

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

Adobe Server Products

Adobe Server Products – Provides software licenses (new and upgrade), maintenance, training and support for numerous Adobe server products including LiveCycle Forms; LiveCycle Reader Extensions; Acrobat Connect; Flex; ColdFusion Enterprise; Flash Media Server and other Adobe server products.

Contractor:

Carahsoft Technology Corp. (N00104-09-A-ZF31); Small Business; (703) 871-8503

Ordering Expires: 14 Jan 14

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

Microsoft Products

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

Contractors:

CDW-G (N00104-02-A-ZE85); (877) 890-1330

Dell (N00104-02-A-ZE83); (800) 727-1100 ext. 7253702 or (512) 725-3702

Dell Marketing L.P. *(formerly ASAP)* (N00104-02-A-ZE78); (800) 248-2727, ext. 5303

GTSI (N00104-02-A-ZE79); Small Business; (800) 999-GTSI ext. 2071

Hewlett-Packard (N00104-02-A-ZE80); (978) 399-9818

Insight Public Sector, Inc. (N00104-02-A-ZE82); (800) 862-8758

SHI (N00104-02-A-ZE86); (732) 868-5926

Softchoice (N00104-02-A-ZE81); Small Business; (877) 333-7638

Softmart (N00104-02-A-ZE84); (800) 628-9091 ext. 6928

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., contractors, 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).

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/gcssj

Contractor: ***August Schell Enterprises*** (www.augustschell.com)

Download Site: http://redhat.augustschell.com

Ordering Expires: 14 Mar 10
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.

Contractors:

Carahsoft Technology Corporation (HC1028-09-A-2004)

DLT Solutions, Inc. (HC1028-09-A-2003)

Ordering Expires:
Carahsoft: 09 Feb 14
DLT Solutions, Inc.: 17 Feb 14

Web Link: http://www.esi.mil

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: 31 Jan 10 (Please call for extension information.)

Web Link: https://chess.army.mil/ascp/commerce/contract/ContractsMatrixView.jsp

Operating Systems

Apple

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

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.disa.mil/contracts/guide/bpa/bpa_sun.html

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

Department of the Navy Agreements

Oracle (DEAL-O) Database Enterprise License for the Navy

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) 605-5659 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 netcentric 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

Data at Rest Solutions BPA - Navy Agreement only

The DON CIO has issued an enterprise solution for Navy users purchasing DAR software. Visit the DON CIO Web site at www.doncio.navy.mil and search for "Data at Rest" to read the new policy. The DON awarded MTM Technologies a BPA for purchase of the DON Mobile Armor software bundle. For Navy users, all purchases of DON enterprise DAR solutions must be executed through the enterprise BPA, which can be found on the DON IT Umbrella Program Web site at www.it-umbrella.navy.mil. Procurement of other DAR solutions for Navy users is prohibited.

Navy Enterprise BPA for DAR Users:

Mobile Armor – ***MTM Technologies, Inc.*** (N00104-09-A-ZF30)

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

Visit our Web sites:

www.it-umbrella.navy.mil

www.itec-direct.navy.mil

Page intentionally left blank

Plan to Be There!

West Coast DON IM/IT Conference

Feb 1-4, 2010

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
SPAWARSYSCEN ATLANTIC
CHIPS MAGAZINE
9456 FOURTH AVE
NORFOLK, VA 23511 - 2110
OFFICIAL BUSINESS

PERIODICAL POSTAGE AND
FEES PAID NORFOLK, VA AND
ADDITIONAL MAILING OFFICE
SSC ATLANTIC
CHIPS MAGAZINE
USPS 757-010
ISSN 1947-3990